Т. И. Голенищева-Кутузова, А. Д. Казанцев,
Ю. Г. Кудряшов, А. А. Кустарёв,
Г. А. Мерзон, И. В. Ященко

Элементы математики в задачах

с решениями
и комментариями

Часть 1

Издательство МЦНМО
2010

УДК 51(07)
ББК 74.262.21
Э45

Авторы:
Т. И. Голенищева-Кутузова, А. Д. Казанцев, Ю. Г. Кудряшов,
А. А. Кустарёв, Г. А. Мерзон, И. В. Ященко

Э45 **Элементы математики в задачах** (с решениями и комментариями). Ч. I / Т. И. Голенищева-Кутузова, А. Д. Казанцев, Ю. Г. Кудряшов и др. — М.: МЦНМО, 2010. — 248 с.

ISBN 978-5-94057-579-5

Книга содержит один из курсов математики в задачах, на протяжении ряда лет используемых в 57 школе города Москвы. В представленном виде курс преподавался классу «В» 2008 года выпуска. Часть 1 состоит из тем, изучавшихся в 8 классе.

Задания снабжены решениями и комментариями. Многие сюжеты (листки) могут изучаться независимо.

Книга адресована учителям математики, работающим в математических классах, руководителям кружков и факультативов и всем, кто интересуется обучением старшеклассников математике вне школьной программы.

ББК 74.262.21

ISBN 978-5-94057-579-5

Оглавление

Задачи / Разбор

Введение

В математических классах 57 школы кроме алгебры и геометрии (на которых проходится более-менее обычная школьная программа) имеется еще предмет, который традиционно называется «математический анализ». В отличие от других предметов на уроках анализа практически нет рассказов у доски. Вместо этого ученикам регулярно выдаются *листочки* — наборы задач по какой-либо теме вместе с необходимыми определениями.

Школьники самостоятельно решают и кратко записывают эти задачи — каждый в своем темпе, ни формальных домашних заданий, ни текущих оценок нет (хотя примерно раз в полгода проводится зачет с отметкой), — а на уроке обсуждают их один на один с преподавателями. Для этого на каждом уроке присутствует команда из 4–6 преподавателей. Они же составляют листки.

Из таких листков (выдававшихся нами классу «В» 2008 года выпуска), снабженных решениями задач и комментариями, и состоит эта книга. В часть 1 вошли листки 8 класса. Дополнительные задачи отмечены звездочкой, дополнительные листки имеют букву «д» в номере.

Об этом предисловии.

— Ты, — попросила она, — пока не досказывай до конца. Сначала вспомни какие-нибудь подробности.

Г. Остер. Сказка с подробностями

Длинных предисловий никто обычно не читает. Поэтому мы решили ограничиться кратким описанием учебного процесса выше и довольно разрозненным набором подробностей, среди которых читатель, возможно, найдет ответы на интересующие его вопросы.

О разнообразии подходов. Сразу предупредим, что разные команды преподавателей учат совершенно по-разному. Поэтому подробно говорить об «обучении в матклассах вообще» не имеет особого смысла, а все сказанное ниже относится лишь к тому, как работали и воспринимали педагогический процесс мы.

Более того, так уж получилось, что и сама наша команда состояла из людей с совершенно разными темпераментами, увлечениями, мировоззрением и отношением к учебе и математике[1]. Вероятно, следы этого можно найти и в данной книге.

[1] И это по-своему здорово — например, для каждого школьника можно было выбрать подходящего преподавателя.

В процессе обучения мы довольно часто бывали не согласны с позициями друг друга и немало времени после уроков провели в жарких спорах. И, несмотря на то что в целом все обычно оставались при своих мнениях, аргументы коллег давали каждому возможность взглянуть на какие-то вещи под другим углом.

О целях

> Откровенно признаюсь, на всем своем долгом веку я никогда не говорил своим ученикам о «смысле» музыки; если таковой и существует, во мне он не нуждается. И напротив, я всегда придавал большое значение тому, чтобы мои ученики умели как следует отсчитывать восьмые и шестнадцатые. Будешь ли ты учителем, ученым или музыкантом — благоговей перед «смыслом», но не воображай, будто его можно преподать.
>
> Г. Гессе. Игра в бисер

Скажем сразу, что не ставим единственной (и даже, вероятно, основной) целью выращивание профессиональных математиков (хотя стараемся дать тем, кто хочет и может стать математиком, такой шанс).

То, чему мы хотели бы научить школьников, делится на две группы. С одной стороны (как бы это пафосно ни звучало) — умению мыслить, самостоятельно получать новые результаты; дать опыт математического открытия. И даже если кто-то, закончив маткласс, никогда больше не будет заниматься математикой, этот опыт проявится как-то еще.

С другой стороны, поскольку это вещи сложные, творческие, не вполне ясно, как можно было бы учить непосредственно им. Поэтому на уроках мы занимаемся вещами (по крайней мере внешне) много более скромными. Можно сказать, что мы учим всего четырем вещам: читать, писать, говорить и слушать (школьник *читает* определения и задачи из листка, *записывает* решения, *рассказывает* их преподавателю, *слушает* его комментарии — и всему этому мы стараемся научить; а вот собственно задачи школьнику приходится учиться решать самому).

Мы надеемся, что такие занятия математикой способствуют, по крайней мере, выработке трех умений, полезных и вне ее: «первое — это умение отличать истину от лжи (понимаемой в … объективном математическом смысле, то есть без ссылки на намерение обмануть); второе — это умение отличать смысл от бессмыслицы; третье — это умение отличать понятное от непонятного» (В. А. Успенский).

Кроме того, хотелось бы, чтобы выпускники имели какое-то представление о том, что такое математика и как ей занимаются. Это полезно не только для выпускников, которые дальше будут заниматься математикой, но и для тех, кто дальше никакой математикой заниматься не будет — как минимум для того, чтобы последние смогли вовремя это понять.

Наконец, просто в классе собираются, с одной стороны, ребята, которые хотят заниматься математикой, а с другой стороны — преподаватели, любящие ее и желающие поделиться своими знаниями. И, может быть, такое общение и есть главная цель всего процесса — так же как в музыкальном клубе или кружке макраме. По крайней мере, наверняка это главная его причина.

О системе листков

О листках. Математика — творческое занятие; *технология* получения нового математического знания отсутствует. Единственный способ научиться плавать — так или иначе пробовать это делать; просто смотреть на то, как это делают другие, недостаточно. Так и единственный способ обучения математическому открытию — практика: решение задач, представляющее для школьника открытие *нового знания*.

Конечно, человечеству это знание уже давно известно, но школьнику это мало помогает (только психологически: чтобы что-то сделать, полезно знать, что в принципе это возможно).

Впрочем, в последнем утверждении присутствует некоторое лукавство. Сам набор задач, на которые преподавателями разбит каждый сюжет, позволяет школьникам подниматься, как по ступенькам лестницы. Для этого ступеньки сделаны достаточно высокими, чтобы представлять интерес, но достаточно низкими, чтобы каждый шаг был доступен для школьника[2]. И такое построение листка, конечно, опирается на то, что сами преподаватели хорошо понимают, как эти задачи решать.

В то же время, мы вставляем в листки сложные (а иногда даже нерешенные) задачи. Школьники могут увидеть, что внешне эти задачи ничем не отличаются от других задач листка, и попробовать их

[2]И здесь нельзя не отметить, что самостоятельный поиск/выбор правильных задач и определений — важная часть работы математика (да и не только математика), которой система листков не учит. И даже сама необходимость такой работы от людей, обучающихся по системе листков, скрыта — что может создать искаженное представление о работе математика.

решить. И приятно отметить, что некоторые ребята, работающие по такой системе, уже в школе получают результаты, которые заслуживают настоящей научной публикации[3].

Кроме того, листок представляет собой нечто вроде плана математической статьи в стиле определение-теорема-доказательство, в котором школьникам предлагается заполнить опущенные доказательства. Таким образом, листок передает принятый способ структурирования математического знания[4].

Об индивидуальном подходе. Идея учить по одной программе целый класс кажется нам малопродуктивной.

Поэтому кроме общей для всех обязательной программы имеются дополнительные листки на разные (часто уходящие довольно далеко в сторону от основного курса) темы, которые школьники берут по желанию. Эти листки (вместе с дополнительными задачами из обязательных листков) также компенсируют разницу в темпе разных школьников.

Кроме того, к разным школьникам предъявляются разные требования, им задают разные наводящие — или, наоборот, дополнительные — вопросы. Эти вопросы, вместе с комментариями преподавателя, заполняют пробелы между задачами и определениями листка, создавая (по крайней мере, в идеале) индивидуальный курс для каждого школьника.

Эффективно работать в таком режиме один преподаватель может только с небольшим количеством школьников, которых он достаточно хорошо знает. Соответственно, на класс необходимо несколько преподавателей, каждый из которых работает с 3–5 фиксированными школьниками. В течение урока преподаватель перемещается по классу, подсаживаясь за парты к своим школьникам и обсуждая с ними задачи.

Примерно раз в полгода происходит некоторое перераспределение школьников между преподавателями. Кроме того, тоже примерно раз в полгода проходит зачет, который школьники никогда не сдают своему преподавателю.

---

[3]Например, Yu. Makarychev. A short proof of Kuratowski's graph planarity criterion // J. of Graph Theory, 1997. Vol. 25. P. 129–131; А. А. Кустарев. Ограничения конечных векторных сумм и доказательство теоремы Леви—Штейница // Математическое просвещение, сер. 3, вып. 7.

[4]В том, что этот способ не единственно возможный, нетрудно убедиться, сравнив математическую и физическую статьи, посвященные одному и тому же вопросу.

О традиционных методах. Главное отличие как от традиционной классно-урочной, так и от лекционно-семинарской системы состоит в том, что мы пытаемся научить именно открывать что-то самим, а не действовать по шаблону или пользоваться рассказаными идеями. Именно поэтому мы не заставляем школьников заучивать факты и готовые схемы, а подталкиваем их к изобретению новых (для них) методов решения.

Сразу оговоримся, что на более позднем этапе полезны (и даже необходимы) и изложения в готовом виде: в книгах, лекциях и т. д. Во-первых, изучение какой-либо темы с помощью решения задач требует очень много времени. Во-вторых, даже если предположить, что любая тема может быть изложена в виде набора задач (что неочевидно), то для большинства тем это все равно не сделано (как минимум потому, что для этого требуется серьезная работа кого-то уже разобравшегося в теме). Так что получить достаточный (например, для серьезных занятий математикой) объем знаний при помощи одной только системы листков малореально. Поэтому начиная с 10 класса мы выдаем школьникам математические книги для чтения (и обсуждаем их), организуем лекции по некоторым темам.

Но, по крайней мере в начале обучения, для школьников важно почувствовать крепкую почву под ногами, обрести фундамент из задач и теорем, которые они действительно хорошо понимают, потому что доказали самостоятельно.

При всем том стоит учитывать, что кроме курса анализа в 57 школе всегда присутствуют построенные более-менее по традиционной системе курсы школьной алгебры и геометрии[5].

О рассказах у доски. В 8–9 классах мы рассказывали что-то у доски только в двух случаях.

Во-первых, перед выдачей нового обязательного листка — о соответствующих идеях и мотивировках — неформально, не доказывая точных теорем и не вдаваясь в технические детали определений; этот комментарий ложился на нулевые знания по теме.

Во-вторых, на консультациях, проводившихся перед каждым зачетом, мы рассказывали решения задач, и там, в основном, наоборот, обсуждались детали и технические тонкости. К этому моменту школьники уже довольно давно работали с данной темой и узнавали

[5]И мы рекомендуем ознакомиться с блестящим курсом геометрии Р. К. Гордина (который не только вел в нашем классе обычную математику, но и был его классным руководителем).

решения задач, над которыми (скорее всего) они уже довольно долго размышляли.

О зачетах.

> — ...А яма для сдачи экзамена по математике была?
> — Была, — глаза Змейка блеснули. — Девять локтей глубиной.
> — Один к одному! У нас сажали в яму, давали задачи и тех, кто не решал, наверх уже не вытаскивали. Должен сказать, что вид побелевших костей твоих предшественников чрезвычайно способствует мыслительному процессу.
>
> А. Коростелева. Школа в Кармартене

Проведение зачета преследует несколько целей.

С одной стороны, это способ самому школьнику выяснить, что же он в действительности знает, а что нет, — причем происходит это не только на самом зачете, но и при подготовке к нему.

Вообще, подготовка к зачету, возможно, даже полезнее его самого. Предстоящий зачет очень мобилизует (и это еще одна причина, по которой мы его проводим). В обычное время у детей много разных дел — от прогулок в парке до домашних заданий по другим предметам. А перед зачетом школьники концентрируются на математике: подготовка к зачету — хороший повод вспомнить пройденное и както систематизировать свои знания, а также разобраться наконец в разных тонких местах и пропущенных задачах из старых листков.

Работать в таком режиме постоянно невозможно — и поэтому мы проводим зачет не чаще чем раз в полгода, — но делать это иногда очень полезно (на ледяную горку нельзя взойти пешком, а можно только взбежать; так же и интенсивные занятия способны дать качественный прорыв, которого не получается добиться размеренными занятиями).

С другой стороны, нам и самим интересно, чему же мы научили школьников. При этом нам важно не только и не столько то, насколько хорошо они «усвоили материал», и даже не то, насколько хорошо они научились решать задачи, — в целом это обычно понятно и так (хотя независимая проверка и полезна — особенно для обнаружения отдельных лакун в самых неожиданных местах). Скорее нас интересуют их навыки математического общения (преподавателю, постоянно общающемуся со школьником, через некоторое время становится трудно объективно оценить, насколько внятно последний выражает свои мысли).

Наконец, на зачеты (особенно в старших классах) мы приглашаем профессиональных математиков, общение с которыми интересно и полезно школьникам.

О содержании листков

О выборе тем. Мы не считаем главной целью передачу как можно большего объема знаний; конкретный материал в большинстве случаев для нас лишь средство, повод для математического общения учеников и преподавателей во время урока. Поэтому набор тем во многом определяется математическими вкусами команды: всегда важно учить только тому, что сам любишь.

При этом мы старались использовать сюжеты, которые не требуют слишком больших предварительных знаний — причем понимая под требованиями не только формально используемые определения и теоремы, но и знания, необходимые для мотивировки изучаемых вопросов; недостаточно мотивированные и слишком абстрактные сюжеты плохо усваиваются в 8–9 классах.

При этом темы должны быть достаточно содержательны, чтобы занятия не свелись к формальной игре с определениями. Иначе возникает — не столь редкая, увы — ситуация, когда выпускник матклассa знает много умных слов, но не способен не то что доказать, но даже разобраться в доказательстве сколь-нибудь нетривиальных теорем.

Кроме того, мы старались сделать так, чтобы курс не был разрозненным набором никак не связанных тем, но — хотя бы частично — складывался в какой-то сюжет, дающий при изучении эффект *восхождения*[6]. В нашем курсе в 8–9 классах таким сюжетом является построение действительных чисел: от начал теории множеств через целые и рациональные числа к упорядоченным полям и анализу.

Наконец, хотя объем получаемых знаний для нас и вторичен (по отношению к приобретению навыков математического исследования), мы стараемся включить в программу некоторый минимум, без которого невозможны занятия содержательной математикой. Поэтому время от времени мы даем листки, предназначенные для ликвидации пробелов в образовании. Особенно актуально это в начале обучения, когда в класс приходят ученики с совершенно разными знаниями.

[6]При этом большая часть обязательных листков образует более-менее линейный маршрут, а дополнительные листки предоставляют возможности для радиальных выходов в самых разных направлениях.

О составлении листков. На первый взгляд, нет ничего проще, чем написать листок: достаточно взять какой-нибудь относительно замкнутый математический текст (статью или главу из книги) и выписать из него определения и формулировки лемм и теорем (быть может, добавив некоторые промежуточные леммы). Но нетрудно заметить, что при этом безвозвратно пропадают все комментарии, которые формально не необходимы для доказательства основных результатов. Так что, как минимум, необходимо еще изложить в виде задач (на худой конец, совсем легких — чтобы просто зафиксировать утверждение) примеры к определениям, контрпримеры, демонстрирующие существенность условий теорем, следствия теорем, демонстрирующие важность последних и т. п. А то, что таким образом изложить не получается — например, неформальные идеи и аналогии, — должен иметь в виду преподаватель, обсуждая задачи со школьниками; это, конечно, налагает определенные требования на его математическую квалификацию.

Скажем несколько слов и о композиции листка. Как писал Р. Фейнман, «понять — значит привыкнуть и научиться использовать». Поэтому в начале каждого листка имеются достаточно простые задачи, решая которые школьник может разобраться в базовых понятиях[7]. Но, конечно, математике нельзя научиться, решая только простые задачи, и ближе к концу листка сложность задач возрастает (а в большом листке таких пиков два — где-то в середине и в конце).

Такая напоминающая лестницу композиция, позволяет «самостоятельно» получать доказательства содержательных теорем. Соответственно (в отличие от решения технических упражнений) учащийся может увидеть убедительный результат своей деятельности: например, «я доказал основную теорему арифметики». Причем (в отличие от большинства олимпиадных задач) этот полученный результат не только интересен сам по себе, но и существенен для дальнейшего.

Конечно, такая схема построения листков налагает некоторые ограничения на изучаемый материал: так как объем листка ограничен[8], а каждый следующий листок снова начинается с простых задач, возникает эффект «короткого дыхания»: до действительно сложных

[7]Случается, что сильные преподаватели (особенно работающие с сильными школьниками) торопятся побыстрее проскочить такие — слишком простые и недостаточно содержательные, казалось бы, — задачи. Ничем хорошим это обычно не заканчивается.

[8]Математическая статья в 10 страниц считается очень короткой, а до конца листка в 4 страницы уже доберется не каждый школьник (а некоторые наши коллеги вообще считают, что каждый листок должен умещаться на страницу — на то он и *листок*).

вещей такая лестница регулярным образом не дотягивается (причем ни за какое количество листков). Эту проблему (для сильных школьников) призваны решать дополнительные задачи и дополнительные листки (которые бывали длиннее и существенно сложнее обязательных), а также общение с преподавателем.

В заключение разговора о составлении листков мы хотели бы предостеречь от буквального копирования нашего курса: он, с одной стороны, был построен для конкретных детей (и несет отпечаток разных конкретных обстоятельств), а с другой — отражает математические вкусы конкретных преподавателей. Тем не менее, мы надеемся, что эта книга будет полезна при подборе материалов для занятий.

Об аксиоматическом методе и теории множеств. На крутую гору приходится иногда подниматься не по прямой дороге, а по серпантину. То же бывает полезно и в математике: приступая к изучению курса, мы забываем всю математику, которую знали (курс анализа в 8–9 классах формально полностью замкнут: ссылки на материал школьных курсов отсутствуют в листках, а известные из них факты не разрешается использовать без доказательства), и начинаем все заново, но уже на другом уровне[9]. В частности, на другом уровне строгости: в курсе принят (неформальный) аксиоматический метод. И фундамент, на котором строится здание курса, — неопределяемые понятия множества и целых чисел. С введения в (наивную) теорию множеств и начинается наш курс «математического анализа».

В чем-то это следствие традиции, но для нее есть причины: эта тема обычно незнакома школьникам, что позволяет четко провести черту в начале курса (что более чем уместно в ситуации, когда и цели, и форма, и содержание занятий полностью меняются); на понятном по существу, но новом материале можно зафиксировать требования к строгости[10] решений, к их записи. Видимо, это самое неоднозначное из решений, принятых нами при построении курса, и мы не советуем копировать его, не взвесив тщательно все «за» и «против». И если все же начинать курс таким образом, то делать это нужно очень аккуратно и дифференцированно: школьник, до этого уже занимав-

[9]Причем амплитуда нарастает: по сравнению с предшествующим школьным курсом мы и глубже спускаемся — до теории множеств, и (снова пройдя путь от целых чисел до действительных) значительно выше поднимаемся.

[10]Имеется и противоположная точка зрения, состоящая в том, что, во-первых, решение проблемы (каковым является аксиоматический метод) не может быть адекватно воспринято до знакомства с самой проблемой, а во-вторых, любой метод следует изучать на достаточно содержательных (а не на самых простых) примерах.

шийся, например, на кружке, может быть готов к большему уровню формализма, чем другой, у которого таким образом легко вообще отбить желание заниматься математикой.

О сотрудничестве и принуждении

О математическом общении. С первых уроков (а зачастую и раньше — на кружке) мы стараемся показать школьнику, что мы относимся к нему как к коллеге, создать атмосферу общения равных, совместной научной деятельности. Эта деятельность обычно состоит в том, что школьник вместе с преподавателем совместно пытаются разобраться в предложенном школьником решении какой-либо задачи.

Для того чтобы такое общение было плодотворным, с самого начала занятий мы прививаем *навыки математического общения* (которые, впрочем, ценны и сами по себе): понимать, что дано, а что надо доказать и чем при этом можно пользоваться; отличать доказанное от недоказанного; строить схему доказательства; связно излагать свои мысли (устно и письменно); формулировать отрицание утверждения; исправлять указанные ошибки и пробелы в рассуждениях. На первых уроках основное время и силы уходят именно на такие — казалось бы, простые, но на самом деле фундаментальные — вещи.

О записи решений. Нам приходится работать со школьниками, которые достаточно быстро соображают. Это по-своему здорово и интересно, но ребята обычно соображают гораздо быстрее чем говорят, а тем более пишут. И много сил (и авторитета) уходит на то, чтобы не только научить их умению излагать свои мысли на бумаге, но и просто убедить их в необходимости этого.

Главная причина, по которой мы на этом настаиваем, состоит в том, что только начав записывать решение, можно увидеть полностью ход рассуждения, понять, что ты на самом деле сказал. Типичная в начале обучения ситуация: восьмиклассник говорит нечто и никак не соглашается это записывать, утверждая, что все и так *очевидно*. Преподаватель берется записать то, что говорит ученик; ученик убеждается, что все это действительно аккуратно записано за ним, но перечитав получившийся текст целиком — изумляется: «Вроде я говорил правильное решение, а тут написана какая-то ерунда с кучей ошибок и вообще неверная по сути». Объяснить же школьнику, почему неверно его решение, при чисто устном обсуждении бывает намного сложнее. В частности, потому, что устно при любом указании

на конкретную ошибку можно «менять показания» (причем совершенно искренне — в середине длинного рассказа тяжело вспомнить, что говорил в начале); кроме того, устно легче (сознательно или бессознательно) маскировать недостаток аргументов риторикой.

Записанное на бумаге решение помогает самому школьнику структурировать свои мысли, лучше понять логику (придуманного им же) доказательства, проследить всю цепочку рассуждений. В частности, нередко при записи решения школьник может сам найти в нем ошибки.

О приеме задач. При всем том важно не переусердствовать с наведением строгости в ущерб содержательности. В реальности в сдаче задач всегда присутствует некоторый элемент соревновательности: школьник пытается убедить преподавателя в правильности своего решения, а преподаватель — найти в нем ошибку; если «выигрывает» преподаватель, то школьник дорабатывает решение и снова пытается его сдать. Но не стоит забывать, что главная цель преподавателя все же не в том, чтобы найти в решении школьника как можно больше формальных недочетов, а в том, чтобы постепенно разобраться вместе со школьником в сути происходящего. Мы хотели бы, чтобы урок оставался сотрудничеством, а не поединком.

В противном случае, — даже если не говорить о психологических аспектах ситуации, когда на каждом занятии школьник вынужден бороться с человеком, который его старше и лучше разбирается в теме — к концу обучения у учеников может возникнуть уверенность в том, что математика сводится к формальным манипуляциям с символами по заданным правилам, чего нам (отнюдь не разделяющим такую точку зрения) не хотелось бы.

О принуждении. По нашему убеждению никакое обучение невозможно без определенного принуждения. Те, кто считают, что возможно научить ребенка математике (да и многим другим вещам) просто в атмосфере счастья и любви, сильно заблуждаются. Однако творить из под палки не получится, поэтому приходится тонко совмещать разные формы принуждения, стараясь минимизировать негативные.

Главное — это создать атмосферу, в которой должно быть *принято* (и престижно) учиться и решать задачи. Кроме того, важно сделать так, чтобы школьник, придя на урок и не принеся ни одной задачи, чувствовал неудобство перед преподавателем как перед коллегой, с которым он собирался вместе поработать, обсудить что-то, но пришел ни с чем, и тот пришел зря, попусту потратив свое время.

При этом мы стараемся минимизировать роль школьных отметок — давая почувствовать ребенку, что он работает не за формальную оценку (что, к сожалению, развивается к 8 классу даже у сильных ребят), а ради решения задачи, постижения красоты математики; и высшей наградой является удовольствие от решения задачи и оценка коллег (учителей и одноклассников) этого решения. Причем на первом месте должно стоять именно собственное удовольствие от решения задачи.

Ясно, что обучение по такой системе неэффективно (да и просто невозможно) в ситуации, когда ребенок не любит математику и не хочет ей заниматься. Кстати, поэтому нам достаточно просто экранировать просьбы о взятии ребенка в класс «по блату или звонку» — мы просто честно объясняем, что как раз по знакомству мы можем помочь ребенку избавиться от такой каторги, как обучение в матклассе.

О списывании. Проблема списывания во многом решается, если хватает терпения и педагогического умения освободить ребенка от психологического гнета двойки: нужно добиваться, чтобы ребята не сачковали, но не карать за несделанные задачи, считая формально их количество, — иначе в этом возрасте очень тяжело удержаться от списывания (а о творчестве в таком режиме вообще речи быть не может). Мы стараемся объяснить ученику (и его родителям), что оценка результата обучения происходит не по формальному количеству решенных задач и что списанная задача ничего не дает для достижения описанных выше целей.

О темпе. В силу разного исходного уровня математической подготовки и разного стиля мышления, школьники решают задачи в разном темпе, и мы стараемся не устраивать соревнования по формальным параметрам. И сразу говорим, что оцениваем (как формально, так и неформально) именно индивидуально работу каждого, его отдачу — относительно его возможностей в данный момент, а не относительно какой-то общей планки.

При таком подходе итоговые отметки школьников основываются главным образом на субъективной оценке преподавателя и не претендуют на объективность. Но в нашей практике обычно оказывалось, что оценка школьника ни для кого не является сюрпризом — школьники и сами согласны с тем, как их оценивают преподаватели.

Как уже было сказано, формальных домашних заданий обычно нет, однако преподаватель указывает школьнику (явно или неявно),

когда пора закрывать очередной листок (то есть сдать из него все обязательные задачи). Мы стараемся сделать так, чтобы у школьников не накапливались незакрытые обязательные листки — не выдавая новых листков, пока большинство не справилось со старыми, и мягко помогая отстающим.

О преподавателях

О студентах. Преподавателю в матклассе не обязательно быть математиком, но важно, чтобы он интересовался математикой и разбирался в ней. На самом деле, быть может, лучшие преподаватели — это студенты и аспиранты математических факультетов, сами не так давно закончившие маткласс.

Они лучше чувствуют ребенка — между ними нет психологического барьера (и потому неудивительно, что общение школьников и студентов не ограничивается рамками школьных уроков — это и походы, песни под гитару, обсуждение книг и фильмов; причем все это часто продолжается и после выпуска). У них огромное желание поделиться тем, чему их самих научили в школе и в вузе. Наконец, они еще помнят, *как* их учили; причем не только то, что получалось, но и то, что преподаватели по их (выпускников) мнению делали неудачно. Поэтому им практически и не нужно специальное педагогическое образование — они сразу готовы учить по данной системе, разумеется, при чутком руководстве.

Такие студенты и аспиранты и составляют обычно большую часть команды (именно поэтому система матшкол достаточно стабильна[11] и пережила разные времена). Так было и у нас.

О руководителе команды. Когда обстановка в классе очень неформальная, дисциплину поддерживать гораздо сложнее. Очень тонка грань между творческой обстановкой и абсолютным хаосом. А когда образуется критическая масса учеников, которые ничего не делают, класс рассыпается: либо ребята открыто перестают что-либо делать, либо начинается имитация деятельности (у нас, к счастью, такого ни разу не было).

[11]Как это обычно и бывает с достаточно хорошо работающими системами, основывается эта стабильность во многом на инерции: приходящие в школу студенты обычно считают то, как учили их, самым правильным и естественным (по модулю, быть может, мелких деталей), даже не задумываясь над причинами выбраных когда-то путей и возможными альтернативами. Вероятно, не вполне свободны от такого обмана зрения и мы.

Роль руководителя (кроме приема задач) — это, в первую очередь, чувствовать, что происходит в классе вообще и с каждым учеником в частности, и аккуратно регулировать ситуацию: кого-то похвалить, кого-то поругать (стараясь при этом не потерять психологический контакт), где-то даже поменять преподавателя. Кроме того, он должен оценивать уровень материала, выбирать темы.

Конечно, такие решения принимаются коллективно (не обязательно в результате обсуждения — по некоторым вопросам в команде должно быть согласие), и почти всегда оказывается, что руководитель согласен с общим мнением. И вообще, пока все идет хорошо, руководитель почти и не виден — работает как обычный преподаватель (и может показаться, что он вообще не особенно нужен), но как только начинаются проблемы — решать их прежде всего ему.

И последнее (но, может быть, и главное). Руководитель, как режиссер в театре, должен заражать всех — и учеников, и команду — позитивной энергией. И приходя на урок, он все свои проблемы и дела должен оставить за дверями класса.

Благодарности

Курс сформировался в нынешнем виде (и книга смогла быть написана) благодаря многим замечательным людям:

— Н. Н. Константинову, впервые применившему систему листков в математических классах, и Б. М. Давидовичу (учителю одного из нас), курс которого оказал на нас большое влияние;

— нашим друзьям и коллегам, работавшим (вместе с одним из нас) в классах «В» 57 школы 1996 и 2002 года выпуска и участвовавшим в создании предыдущих версий этого курса: Д. В. Ботину, С. А. Дориченко, В. В. Крюкову, С. В. Маркелову, В. В. Питербаргу, А. Б. Скопенкову, Р. М. Фёдорову, С. Е. Шалунову и другим;

— всем, кто вел вместе с нами «анализ» у v08 (класса «В» 57 школы 2008 года выпуска), обсуждал и писал листки: Е. В. Корицкой, П. И. Митричеву и В. М. Рычеву;

— ребятам из v08, которые удивительным образом смогли это все учить и получать вместе с нами удовольствие от математики, вдохновляя нас на создание курса и на написание этой книги.

Количество ошибок в тексте книги существенно уменьшилось благодаря внимательному чтению А. С. Бохенеком, С. М. Львовским, А. В. Каплиевым, А. В. Семёновым. Отдельная благодарность В. Ю. Радионову, который не только сверстал книгу, но и исправил ряд оши-

бок и дал ряд ценных советов. Наконец, мы благодарны В. Д. Арнольду и М. А. Берштейну за ценные советы по написанию этого предисловия.

Мы будем признательны читателям за сообщения об ошибках и опечатках (e-mail: merzon@mccme.ru, Григорий Мерзон).

Теория множеств 1

листок 1 / сентябрь 2004

Множество — одно из основных неопределяемых понятий в математике. Задать множество — значит определить, из каких элементов оно состоит. Один из способов задать множество — просто перечислить в фигурных скобках его элементы.

«Элемент x принадлежит множеству M» записывают как «$x \in M$», «элемент x не принадлежит множеству M» записывают как «$x \notin M$».

Задача 1. Сколько элементов в множестве:

а) $\{1\}$, $\{1, 2, 3\}$, {Вася}; б) $\{\{1\}\}$; в) $\{1, \{2, 3\}\}$;

г) букв слова «крокодил»; д) $\{\{1\}, 1\}$;

е) имен учеников вашего класса?

Определение 1. Множества A и B называются *равными*, если каждый элемент множества A принадлежит множеству B, а каждый элемент множества B принадлежит множеству A. Обозначение: $A = B$.

Определение 2. Множество A называется *подмножеством* множества B, если каждый элемент множества A принадлежит множеству B. Обозначение: $A \subset B$. Один из способов задать подмножество — задать свойство, которым обладают все его элементы: $\{x \in A \mid x$ обладает свойством …$\}$.

Задача 2. а) Пусть A — множество однозначных натуральных чисел. Запишите указанным в определении 2 способом его подмножество $\{2, 4, 6, 8\}$.

б) Пусть A — множество городов России. Перечислите элементы его подмножества $\{x \in A \mid$ число жителей города x на 1 января 2003 года более 1 000 000 человек$\}$.

Задача 3. Для каждых двух из следующих множеств указать, является ли одно из них подмножеством другого: $\{1\}$, $\{1, 2\}$, $\{1, 2, 3\}$, $\{\{1\}, 2, 3\}$, $\{\{1, 2\}, 3\}$, $\{3, 2, 1\}$, $\{\{2, 1\}\}$.

Задача 4. Докажите, что множество A тогда и только тогда является подмножеством множества B, когда каждый элемент, не принадлежащий B, не принадлежит A.

Задача 5. Докажите, что для произвольных множеств A, B и C:

а) $A \subset A$; б) $A \subset B$ и $B \subset C \Rightarrow A \subset C$; в) $A = B \Leftrightarrow A \subset B$ и $B \subset A$.

Определение 3. Множество называется *пустым*, если оно не содержит ни одного элемента. Обозначение: $\varnothing$.

Задача 6. а) Докажите, что пустое множество является подмножеством любого множества.

б) Докажите, что пустое множество единственно.

Задача 7. Сколько элементов у каждого из следующих множеств: $\varnothing$, $\{1\}$, $\{1, 2\}$, $\{1, 2, 3\}$, $\{\{1\}, 2, 3\}$, $\{\{1, 2\}, 3\}$, $\{\varnothing\}$, $\{\{2, 1\}\}$?

Задача 8. а) Для множеств из предыдущей задачи выпишите все их подмножества.

б) Сколько подмножеств у множества из одного элемента? из двух элементов? трех элементов?

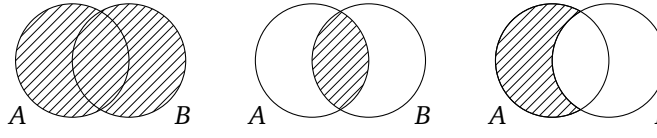
Задача 9. Верно ли, что множество летающих крокодилов является подмножеством множества учеников 8 «В» класса 57-й школы? Верно ли, что множество учеников 8 «В» класса 57-й школы является подмножеством множества классов 57-й школы?

Задача 10. Может ли у множества быть ровно: а) 0; б) 7; в) 16 подмножеств?

Определение 4. *Объединением* множеств A и B называется множество, состоящее из всех таких x, что $x \in A$ или $x \in B$. Обозначение: $A \cup B$.

Пересечением множеств A и B называется множество, состоящее из всех таких x, что $x \in A$ и $x \in B$. Обозначение: $A \cap B$.

Разностью множеств A и B называется множество, состоящее из всех таких x, что $x \in A$ и $x \notin B$. Обозначение: $A \setminus B$.



Задача 11. Пусть даны множества $A = \{1, 3, 7, 137\}$, $B = \{3, 7, 23\}$, $C = \{0, 1, 3, 23\}$, $D = \{0, 7, 23, 2004\}$. Найдите множества:

а) $A \cup B$; б) $A \cap B$; в) $(A \cap B) \cup D$; г) $C \cap (D \cap B)$;

д) $(A \cup B) \cap (C \cup D)$; е) $(A \cup (B \cap C)) \cap D$;

ж) $(C \cap A) \cup ((A \cup (C \cap D)) \cap B)$; з) $(A \cup B) \setminus (C \cap D)$;

и) $A \setminus (B \setminus (C \setminus D))$; к) $((A \setminus (B \cup D)) \setminus C) \cup B$.

Задача 12. Пусть A — множество четных чисел, а B — множество чисел, делящихся на три. Найдите $A \cap B$.

Задача 13. Докажите, что для любых множеств A, B, C:

а) $A \cup B = B \cup A$; $A \cap B = B \cap A$;

б) $A\cup(B\cup C)=(A\cup B)\cup C$; $A\cap(B\cap C)=(A\cap B)\cap C$;
в) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$; $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$;
г) $A\setminus(B\cup C)=(A\setminus B)\cap(A\setminus C)$; $A\setminus(B\cap C)=(A\setminus B)\cup(A\setminus C)$.

Задача 14. Верно ли, что для любых множеств A, B, C:
а) $A\cap\varnothing=\varnothing$; $A\cup\varnothing=A$; б) $A\cup A=A$; $A\cap A=A$;
в) $A\cap B=A\Leftrightarrow A\subset B$; г) $(A\setminus B)\cup B=A$; д) $A\setminus(A\setminus B)=A\cap B$;
е) $A\setminus(B\setminus C)=(A\setminus B)\cup(A\cap C)$; ж) $(A\setminus B)\cup(B\setminus A)=A\cup B$?

Задача 15. а) Внутри фигуры площади 6 расположено три многоугольника площадью не менее 3 каждый. Докажите, что существует два многоугольника, площадь пересечения которых не менее 1.

б*) Внутри фигуры площади 4 расположено 7 многоугольников площадью не менее 1 каждый. Докажите, что существует два многоугольника, площадь пересечения которых не менее $1/7$.

Задача 16*. а) Можно ли записать пересечение двух множеств, используя только разность и объединение?

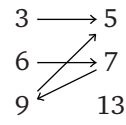
б) Можно ли записать разность двух множеств, используя только объединение и пересечение?

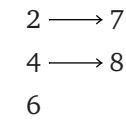
Теория множеств 2. Отображения множеств

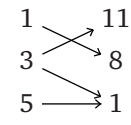
листок 2 / сентябрь 2004

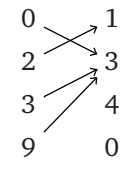
Определение 1. Если каждому элементу x множества X поставлен в соответствие ровно один элемент $f(x)$ множества Y, то говорят, что задано *отображение* f из множества X в множество Y. При этом, если $f(x)=y$, то элемент y называется *образом* элемента x при отображении f, а элемент x называется *прообразом* элемента y при отображении f. Обозначение: $f\colon X\to Y$.

Задача 1. Какие из следующих картинок задают отображения?

а) 

б) 

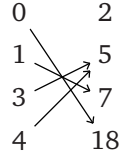
в) 

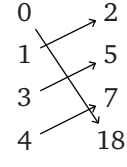
г) 

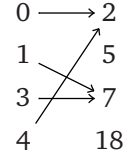
Задача 2. Нарисуйте все возможные отображения из множества $\{7,8,9\}$ в множество $\{0,1\}$.

Определение 2. Пусть $f\colon X\to Y$, $y\in Y$, $A\subset X$, $B\subset Y$. *Полным прообразом элемента* y при отображении f называется множество $\{x\in X\mid f(x)=y\}$. Обозначение: $f^{-1}(y)$. *Образом множества* $A\subset X$ при отображении f называется множество $\{f(x)\mid x\in A\}$. Обозначение: $f[A]$. *Прообразом множества* $B\subset Y$ называется множество $\{x\in X\mid f(x)\in B\}$. Обозначение: $f^{-1}[B]$.

Задача 3. Для отображения $f\colon\{0,1,3,4\}\to\{2,5,7,18\}$, заданного картинкой, найдите $f[\{0,3\}]$, $f[\{1,3,4\}]$, $f^{-1}(2)$, $f^{-1}[\{2,5\}]$, $f^{-1}[\{5,18\}]$.

а) 

б) 

в) 

Задача 4. Пусть $f\colon X\to Y$, $A_1, A_2\subset X$, $B_1, B_2\subset Y$. Всегда ли верно, что:

а) $f[X]=Y$; б) $f^{-1}[Y]=X$; в) $f[A_1\cup A_2]=f[A_1]\cup f[A_2]$;

г) $f[A_1\cap A_2]=f[A_1]\cap f[A_2]$; д) $f^{-1}[B_1\cup B_2]=f^{-1}[B_1]\cup f^{-1}[B_2]$;

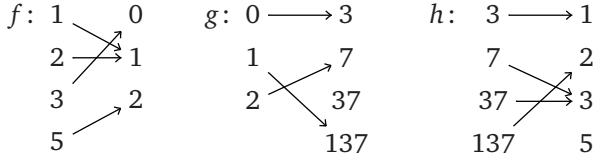
е) $f^{-1}[B_1\cap B_2]=f^{-1}[B_1]\cap f^{-1}[B_2]$; ж) $f[A_1]\subset f[A_2]\Rightarrow A_1\subset A_2$;

з) $f^{-1}[B_1]\subset f^{-1}[B_2]\Rightarrow B_1\subset B_2$?

Определение 3. *Композицией отображений* $f\colon X \to Y$ и $g\colon Y \to Z$ называется отображение, сопоставляющее элементу x множества X элемент $g(f(x))$ множества Z. Обозначение: $g \circ f$. (То есть композиция $g \circ f$ состоит в последовательном применении отображений f и g.)

Задача 5. Докажите, что для произвольных отображений $f\colon X \to Y$, $g\colon Y \to Z$ и $h\colon Z \to W$ выполняется следующее: $h \circ (g \circ f) = (h \circ g) \circ f$ (то есть скобки в выражении $h \circ g \circ f$ можно не писать).

Задача 6. Пусть $f\colon \{1, 2, 3, 5\} \to \{0, 1, 2\}$, $g\colon \{0, 1, 2\} \to \{3, 7, 37, 137\}$, $h\colon \{3, 7, 37, 137\} \to \{1, 2, 3, 5\}$ — отображения, показанные на рисунке:

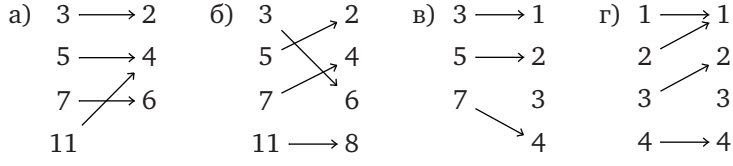


Нарисуйте картинки для следующих отображений:

а) $g \circ f$; б) $h \circ g$; в) $f \circ h \circ g$; г) $g \circ h \circ f$.

Определение 4. Отображение $f\colon X \to Y$ называется *биективным*, если для каждого $y \in Y$ найдется ровно один $x \in X$ такой, что $f(x) = y$.

Задача 7. Про каждое из отображений, изображенных на рисунке, выясните, является ли оно биективным:



Задача 8. Нарисуйте все биективные отображения а) из множества $\{1, 2\}$ в множество $\{3, 4, 5, 6\}$; б) из множества $\{1, 2, 3\}$ в множество $\{4, 5, 6\}$.

Задача 9. Пусть $f\colon X \to Y$, $g\colon Y \to Z$. Верно ли, что если f и g биективны, то и $g \circ f$ биективно?

Определение 5. Отображение f называется *инъективным*, если оно разные элементы переводит в разные, т. е. если из $f(x) = f(x')$ следует, что $x = x'$.

Отображение $f\colon X \to Y$ называется *сюръективным*, если каждый элемент $y \in Y$ имеет хотя бы один прообраз, т. е. $f^{-1}(y) \neq \varnothing$ для любого $y \in Y$.

Задача 10. Докажите, что следующие свойства отображения $f\colon X \to Y$ эквивалентны:

1) f — биекция;

2) f сюръективно и инъективно;

3) f *обратимо*, то есть существует такое отображение[12] $g\colon Y \to X$, что $gf = \mathrm{Id}_X$, $fg = \mathrm{Id}_Y$, где $\mathrm{Id}_M\colon M \to M$, $m \mapsto m$ — *тождественное отображение*.

Задача 11. Про каждые два из следующих множеств выясните, существует ли между ними биекция:

а) множество натуральных чисел;

б) множество четных натуральных чисел;

в) множество натуральных чисел без числа 3;

г) множество целых чисел.

[12] Говорят, что g — обратное к f и пишут $g = f^{-1}$.

Комбинаторика 1

листок 3 / сентябрь 2004

Задача 1. Сколько существует «слов»[13]: а) из двух; б) из трех букв русского языка?

Задача 2. Сколько существует различных ожерелий: а) из трех разноцветных; б) из двух красных и двух синих; в) из трех красных и двух синих бусинок?

Задача 3. Сколькими способами можно выбрать из десяти человек двух дежурных и одного старшего дежурного?

Задача 4. Сколькими способами можно выбрать: а) из пяти; б) из семи; в) из десяти человек трех дежурных?

Задача 5. Сколькими способами можно рассадить пять человек в автобусе, если в автобусе: а) 4; б) 5; в) 6; г) 7 свободных мест?

Задача 6. Семь учеников 8 «В» класса решили вместе покататься

а) на аттракционе «поезд», состоящем из семи одноместных вагончиков;

б) на карусели, у которой ровно семь мест;

в) на «поезде» из десяти вагончиков;

г) на карусели, у которой ровно десять мест.

Сколькими способами они смогут это сделать?

Задача 7. Сколькими способами можно пройти из левого нижнего угла квадрата: а) 2×2; б) 3×3; в*) 5×5, двигаясь только вверх или вправо по сторонам клеток?

Задача 8. Сколькими способами можно представить числа 5, 10, 20 в виде суммы: а) двух; б) трех натуральных чисел?

Задача 9. Сколькими способами можно расставить скобки в выражении $a + b - c \cdot d$?

Задача 10. а) Докажите, что подмножеств в множестве $\{a, b, c, d, e\}$ столько же, сколько отображений этого множества в множество $\{0, 1\}$. б) Докажите, что это число равно числу последовательностей нулей и единиц длины пять.

Задача 11*. Сколько существует различных наборов бусинок, из которых можно составить ровно два различных ожерелья?

[13] В этой задаче, конечно, имеются в виду не те слова, которые можно встретить в словаре, а произвольные сочетания букв русского языка.

Задача 12*. В городе Энск номера автобусных билетов четырехзначные. Жители этого города считают, что билеты, у которых сумма первых двух цифр равна сумме последних двух цифр, счастливые. Сколько счастливых билетов в Энске?

Задача 13*. Сколькими способами можно раскрасить колесо обозрения: а) с 7 кабинками в 3 цвета; б) с 10 кабинками в 2 цвета? При раскраске не обязательно использовать все цвета.

Задача 14. Кто-то режет правильный: а) шестиугольник; б*) семиугольник; в*) восьмиугольник на треугольники, проводя разрезы по непересекающимся диагоналям. Сколько разных наборов треугольников может получиться?

Задача 15. Сколько существует различных игральных кубиков (на гранях кубика расставлены числа от 1 до 6)?

Подстановки 1. Ходим по циклу

листок 1д / октябрь 2004

Определение 1. *Подстановкой из n элементов* называется биективное отображение из множества $\{1, 2, \ldots, n\}$ в себя. Запись вида

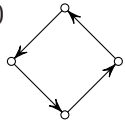
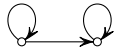
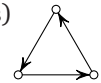
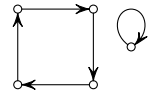
$$\begin{pmatrix} i_1 i_2 \ldots i_n \\ j_1 j_2 \ldots j_n \end{pmatrix},$$

где $i_1, i_2, \ldots, i_n$ — различные элементы множества $\{1, 2, \ldots, n\}$ и $j_1, j_2, \ldots, j_n$ — различные элементы множества $\{1, 2, \ldots, n\}$, обозначает подстановку a, для которой $a(i_k) = j_k$ при всех $k \in \{1, 2, \ldots, n\}$. Множество подстановок из n элементов обозначается S_n. Подстановку можно графически изобразить следующим образом. Расположим на плоскости элементы множества $\{1, 2, \ldots, n\}$ и для каждого i проведем стрелку из элемента i в элемент $a(i)$. То, что получилось, называется *графом подстановки*.

Задача 1. Какие из следующих таблиц являются записями подстановок: а) $\binom{1}{1}$; б) $\binom{123}{123}$; в) $\binom{2}{2}$; г) $\binom{123}{234}$; д) $\binom{123}{333}$; е) $\binom{514632}{164253}$; ж) $\binom{4321}{1234}$; з) $\binom{5321}{5321}$; и) $\binom{1327}{7231}$; к) $\binom{123}{112}$?

Задача 2. Выпишите и изобразите графически все элементы множеств S_1, S_2 и S_3.

Задача 3. Какие из следующих изображений являются графами подстановок?

а)  б)  в)  г) 

Задача 4. а) Сколько элементов в множестве S_n?

б) Сколькими способами можно записать подстановку из n элементов?

Определение 2. *Произведением* подстановок $a, b \in S_n$ называется их композиция как отображений: $a \circ b$. Обозначение: ab.

Задача 5. Найдите произведения: а) $\binom{123}{312}\binom{312}{123}$; б) $\binom{1234}{4321}\binom{1234}{2143}$; в) $\binom{124536}{123456}\binom{642351}{123456}$; г) $\binom{12345}{24531}\binom{12345}{35124}$; д) $\binom{123456}{561423}\binom{123456}{345261}$.

Задача 6. Верно ли, что для любых подстановок $a, b \in S_n$ выполняется равенство $ab = ba$?

Определение 3. Подстановка $e = \binom{12\ldots n}{12\ldots n}$ называется *тождественной*.

Задача 7. Докажите следующие утверждения:

а) для любой подстановки $a \in S_n$ $ae = ea = a$;

б) для любых подстановок $a, b, c \in S_n$ $(ab)c = a(bc)$;

в) для любой подстановки $a \in S_n$ существует и при том единственная подстановка $b \in S_n$ такая, что $ab = ba = e$.

Определение 4. Пусть $1 \leqslant i, j \leqslant n$, $i \neq j$. Подстановка a такая, что $a(i) = j$, $a(j) = i$, $a(k) = k$ при $k \neq i, j$, называется *транспозицией*. Обозначение: $(i\ j)$.

Определение 5. Пусть $i_1, i_2, \ldots, i_k$ — различные элементы множества $\{1, 2, \ldots, n\}$. Подстановка a, сдвигающая элементы $i_1, i_2, \ldots, i_k$, то есть такая, что $a(i_j) = i_{j+1}$ для любого $j \in \{1, 2, \ldots, k-1\}$, $a(i_k) = i_1$ и $a(s) = s$ при $s \notin \{i_1, i_2, \ldots, i_k\}$, называется *циклом длины* k. Обозначение: $(i_1\ i_2 \ldots i_k)$. Множество $\{i_1, \ldots, i_k\}$ называется *носителем* цикла, а число k — *длиной* цикла.

Задача 8. а) Какие из подстановок задач 1 и 2 являются циклами, а какие — транспозициями?

б) Сколько циклов длины 57 в S_{57}?

в) Сколько циклов и сколько транспозиций в S_5?

г) При каких условиях произведение двух транспозиций является циклом?

д*) При каких условиях произведение двух циклов является циклом?

Определение 6. Циклы с непересекающимися носителями называются *независимыми*.

Задача 9*. а) Докажите, что любая подстановка представляется в виде произведения независимых циклов.

б) Докажите, что любая подстановка представляется в виде произведения транспозиций.

в) Докажите, что любая подстановка из S_n представляется в виде произведения не более чем $n - 1$ транспозиции.

г) Верно ли, что любая подстановка из S_n представляется в виде произведения независимых транспозиций?

Метод математической индукции

листок 4 / октябрь 2004

Соглашение. В этом листочке буквами m, n и k обозначены натуральные числа.

Аксиома наименьшего элемента. Каждое непустое подмножество множества натуральных чисел имеет наименьший элемент, т. е. элемент, который меньше любого другого элемента этого подмножества.

Задача 1. а) Останется ли предыдущее утверждение верным, если «множество натуральных чисел» заменить на «множество целых чисел»?

б) Останется ли предыдущее утверждение верным, если «наименьший элемент» заменить на «наибольший элемент»?

Задача 2. На острове Буяне все страны треугольной формы. Если две страны граничат, то по целой стороне. Докажите, что страны можно раскрасить в 3 цвета так, что соседние по стороне страны будут окрашены в разные цвета.

Принцип математической индукции. Пусть задана последовательность утверждений $A_1, A_2, \ldots, A_k, \ldots$, в которой:

1) (база индукции) первое утверждение истинно,

2) (шаг индукции) из истинности утверждения A_n следует истинность утверждения A_{n+1}.

Тогда все утверждения A_n истинны.

(Данным утверждением разрешается пользоваться без доказательства. Иногда это утверждение принимают за аксиому.)

Задача 3*. Докажите принцип математической индукции.

Задача 4. На острове Буяне каждые два города соединены напрямую автомобильной либо железной дорогой. Докажите, что или из любого города в любой другой можно добраться на автомобиле, или из любого города в любой другой можно добраться на поезде.

Задача 5. Докажите, что части, на которые n прямых делят плоскость, всегда можно раскрасить в два цвета так, чтобы соседние части (то есть части, имеющие общий отрезок или луч) были окрашены в разные цвета.

Задача 6. Докажите по индукции, что:

а) $1+\ldots+n=\frac{n(n+1)}{2}$; б) $1+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}$;

в) $1+\ldots+n^3=\frac{n^2(n+1)^2}{4}$.

Задача 7. Найдите ошибку в следующих доказательствах.

а) Докажем, что $n>n+1$.

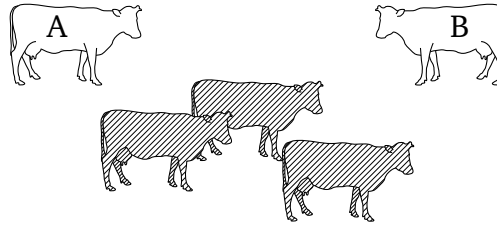
Действительно, пусть это утверждение верно для n, то есть $n>n+1$. Прибавив к обеим частям равенства единицу, мы получаем, что $(n+1)>(n+1)+1$, то есть верно утверждение для $n+1$.

б) Докажем, что в произвольном стаде из N коров все коровы одного цвета.

База индукции. В любом стаде из одной коровы все коровы, очевидно, одного цвета.

Шаг индукции. Предположим, что в любом стаде из N коров все коровы одного цвета. Докажем, что в любом стаде из $N+1$ коровы все коровы одного цвета.

Рассмотрим произвольное стадо из $N+1$ коровы. Возьмем в нем произвольную корову A. Оставшиеся N коров одного цвета. Теперь возьмем другую корову B. Оставшиеся N коров также одного цвета. В частности, A одного цвета со всеми коровами, кроме A и B, и B одного (того же!) цвета со всеми коровами, кроме A и B (см. рисунок). Значит, A, B, и вообще все коровы в стаде одного цвета.



в) В стране несколько городов, некоторые пары которых соединены дорогами, причем каждый город соединен хотя бы с одним другим. Докажем, что из любого города можно проехать в любой другой по дорогам. Будем доказывать индукцией по числу городов. База индукции для стран, состоящих из одного города, очевидна. Докажем шаг индукции. Возьмем какую-нибудь страну из n городов и добавим к ней еще один город. Между старыми городами можно проехать по старым дорогам, так что достаточно доказать, что из нового города можно проехать в любой из старых. По условию задачи из этого города ведет дорога в один из старых городов. Следовательно, из него можно доехать в один из старых городов, а оттуда уже добраться до любого другого. Итак, в новой стране тоже можно из любого города доехать до любого другого, и шаг индукции доказан.

Задача 8. На сколько частей делят плоскость n прямых в общем положении? (Говорят, что прямые находятся *в общем положении*, если никакие две из них не параллельны и никакие три не пересекаются в одной точке.)

Задача 9. Докажите, что:
а) $2^{5n+3}+5^n\cdot 3^{n+2}$ делится на 17; б) $n^{2m-1}+1$ делится на $n+1$;
в*) $2^{3^n}+1$ делится на 3^{n+1}.

Задача 10 (неравенство Бернулли). Докажите, что если $a>-1$, то

$$(1+a)^n \geqslant 1+na.$$

Задача 11. Докажите, что:
а) $2^n>n$; б) $2^n>n^2$ при $n>4$; в) $n!>2^n$ при $n>3$;
г*) существует такое k, что $2^n>n^{2004}$ при всех $n>k$.

Задача 12. Вершины выпуклого многоугольника раскрашены ровно в три цвета так, что никакие две соседние вершины не окрашены в один цвет. Докажите, что многоугольник можно разбить диагоналями на треугольники так, чтобы у каждого треугольника вершины были трех разных цветов.

Обобщенный принцип математической индукции. Пусть задана последовательность утверждений $A_1, A_2, \ldots, A_k, \ldots$ Известно, что:
1) (база индукции) первое утверждение истинно,
2) (шаг индукции) из истинности утверждений $A_1, A_2, \ldots, A_n$ следует истинность утверждения A_{n+1}.
Тогда все утверждения истинны.

Задача 13*. Докажите обобщенный принцип математической индукции.

Задача 14. Докажите, что если $a+\frac{1}{a}$ целое, то $a^k+\frac{1}{a^k}$ целое при любом k.

Задача 15*. В классе каждый болтун дружит хотя бы с одним молчуном. При этом болтун молчит, если в кабинете находится нечетное число его друзей-молчунов. Докажите, что учитель может выгнать из класса не более половины учеников так, чтобы все болтуны молчали.

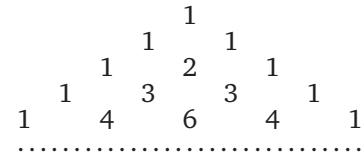
Задача 16* (Задача Сильвестра). На плоскости взяты несколько точек так, что на каждой прямой, соединяющей любые две из них, лежит по крайней мере еще одна точка. Докажите, что все точки лежат на одной прямой.

Задача 17*. Докажите, что $n^{n+1}>(n+1)^n$ при $n>2$.

Комбинаторика 2. Бином Ньютона

листок 5 / октябрь 2004

Определение 1. *Треугольником Паскаля* называется треугольная таблица, составленная из чисел по следующему правилу: строка с номером n состоит из n чисел, первое и последнее числа каждой строки равны единице, а каждое из остальных чисел равно сумме двух ближайших к нему чисел предыдущей строки. Число, стоящее на $(k+1)$-м месте $(n+1)$-й строки, обозначается $\binom{n}{k}$.



Задача 1. Запишите в виде $\binom{a}{b}$ числа предыдущей строки, ближайшие к числу $\binom{n}{m}$.

Задача 2. Выпишите первые 11 строк треугольника Паскаля.

Задача 3. Докажите, что $\binom{n}{k} = \binom{n}{n-k}$.

Задача 4. Докажите, что число способов пройти из левого нижнего угла прямоугольника $m \times n$ в правый верхний, двигаясь только вверх или вправо по границам клеток, равно $\binom{n+m}{m}$.

Задача 5. В каких строках треугольника Паскаля все числа нечётные?

Определение 2. *Числом сочетаний из n по m* называется количество m-элементных подмножеств множества из n элементов. Обозначение: C_n^m.

Задача 6. Найдите: а) C_{100}^1, б) C_4^2, в) C_5^2, г) C_6^4.

Задача 7. Докажите, что: а) $C_n^k = C_n^{n-k}$; б) $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$.

Задача 8. Докажите, что $\binom{n}{k} = C_n^k$.

Задача 9. Раскройте скобки в выражении: а) $(a+b)^3$; б) $(a+b)^4$; в) $(2a+3b)^4$.

Задача 10 (бином Ньютона). а) Раскройте скобки в выражениях $(a+b)$, $(a+b)^2$, $(a+b)^3$, $(a+b)^4$ и выпишите результаты друг под другом. Заметьте, что коэффициенты образуют треугольник Паскаля.

б) Докажите, что

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}b^n.$$

Задача 11. Докажите, что:

а) $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$;

б) $\binom{n}{0} - \binom{n}{1} + \ldots + (-1)^n\binom{n}{n} = 0$.

Задача 12. Докажите, что $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Задача 13. Докажите, что:

а) $\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}$;

б) $\binom{n}{0} + \binom{n+1}{1} + \ldots + \binom{n+k-1}{k-1} + \binom{n+k}{k} = \binom{n+k+1}{k}$;

в) $\binom{n}{1} + 2\binom{n}{2} + \ldots + n\binom{n}{n} = n \cdot 2^{n-1}$;

г) $\binom{n}{k} \cdot \binom{n-k}{m-k} = \binom{m}{k} \cdot \binom{n}{m}$.

Задача 14. Каких подмножеств в множестве из 16 элементов больше: состоящих из более чем 8 элементов, из менее чем 8 элементов, из ровно 8 элементов?

Задача 15. Найдите число таких последовательностей длины 16 из нулей и единиц, в которых не менее чем три единицы.

Задача 16. Решите указанные преподавателем задачи из листка «Комбинаторика 1» для произвольных n и k.

Задача 17*. Сколькими способами можно выбрать неотрицательные целые числа $x_1, x_2, \ldots, x_m$ такие, что $x_1 + x_2 + \ldots + x_m = n$?

Теория графов 1

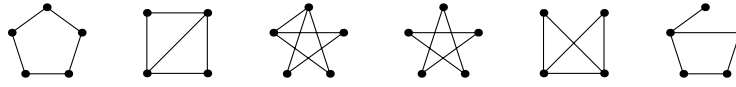
листок 6 / ноябрь 2004

Определение 1. *Графом*[14] называется пара $\Gamma = (V, E)$ из конечного множества *вершин* V и множества *ребер* E, элементами которого являются (неупорядоченные) пары вершин графа Γ.

Граф можно представлять себе как множество точек, некоторые пары которых соединены линиями.

Определение 2. Графы Γ_1 и Γ_2 называются *изоморфными*, если существует такая биекция $f\colon V(\Gamma_1) \to V(\Gamma_2)$, что вершины A и B графа Γ_1 соединены ребром тогда и только тогда, когда вершины $f(A)$ и $f(B)$ соединены ребром в графе Γ_2.

Задача 1. Какие из следующих графов изоморфны?



Задача 2. Нарисуйте все неизоморфные друг другу графы с не более чем четырьмя вершинами.

Задача 3. а) Нарисуйте граф, вершинами которого являются страны СНГ, а ребрами соединены граничащие страны.

б) Нарисуйте граф, вершинами которого являются натуральные числа от 2 до 15, а ребрами соединены различные числа, одно из которых делится на другое.

Задача 4. а) Постройте граф с пятью вершинами, в котором нет ни трех попарно соединенных, ни трех попарно несоединенных вершин.

б) Докажите, что в каждой компании из шести человек найдутся либо три попарно знакомых, либо три попарно незнакомых человека.

Задача 5. Пусть в некоторой компании среди любых трех человек найдутся два друга. Обязательно ли эту компанию можно разбить на две группы, так что всякие два человека из одной группы — друзья?

Задача 6. Найти наибольшее возможное количество ребер в графе с n вершинами, если известно, что среди произвольных трех его вершин есть две, не соединенные ребром.

Определение 3. *Степенью* (или *валентностью*) *вершины* A называется число выходящих из нее ребер. Обозначение: $\deg A$.

[14] Точнее, *неориентированным графом без петель и кратных ребер.*

Задача 7. Укажите степени всех вершин графов из задач 1, 2 и 3.

Задача 8. Докажите, что в графе с более чем одной вершиной есть две вершины одинаковой степени.

Задача 9. Докажите, что сумма степеней вершин произвольного графа равна удвоенному количеству его ребер.

Определение 4. *Путем* в графе называется конечная последовательность вершин и соединяющих их ребер, то есть последовательность вида $v_0e_1v_1e_2v_2\ldots e_nv_n$, где v_i — вершины графа, а ребро e_i соединяет вершины v_{i-1} и v_i. Число n называется *длиной пути*. *Циклом* называется путь, в котором первая и последняя вершины совпадают.

В графе без кратных ребер (а в этом листке изучаются только такие графы) путь однозначно восстанавливается по последовательности своих вершин, поэтому обычно выписывают именно эту последовательность. Однако технически удобнее включать ребра в определение.

Определение 5. Граф Г называется *гамильтоновым*, если в нем существует путь, содержащий каждую вершину ровно один раз.

Задача 10. Докажите, что графы додекаэдра и икосаэдра гамильтоновы.

Определение 6. Граф называется *связным*, если для любых двух различных его вершин существует путь, начинающийся в первой из них и заканчивающийся во второй.

Задача 11. Какие из графов задач 1, 2 и 3 связны?

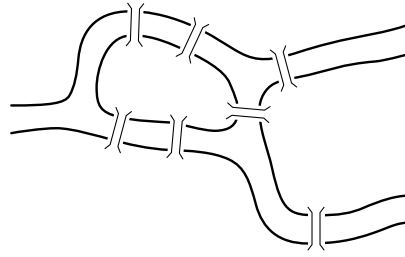
Задача 12. Докажите, что если граф, число вершин которого больше 1, связен, то степень любой его вершины положительна. Верно ли обратное?

Определение 7. Связный граф называется *деревом*, если в нем не существует цикла (т. е. пути, конец которого совпадает с началом), все ребра которого различны.

Задача 13. Докажите, что в любом дереве есть: а) хотя бы одна; б) хотя бы две вершины степени 1.

Задача 14. Докажите, что в дереве число вершин на 1 больше числа ребер.

Задача 15. На рисунке изображена схема расположения мостов в городе Кёнигсберге XVIII века. Можно ли совершить прогулку так, чтобы пройти по каждому мосту ровно один раз?



Определение 8. Граф называется *эйлеровым*, если в нем существует цикл, проходящий по каждому ребру ровно один раз.

Задача 16. Какие из следующих графов эйлеровы?

Задача 17. Докажите, что граф эйлеров тогда и только тогда, когда он связен и степень каждой его вершины четна.

Задача 18*. В турнире без ничьих участвовало n команд. Каждая команда сыграла с каждой ровно по одному разу. Докажите, что можно так занумеровать команды числами $1, \ldots, n$, что $(i+1)$-я команда выиграла у i-й (для произвольного $i = 1, \ldots, n-1$).

Задача 19* (теорема Рамсея). а) Докажите, что для произвольных натуральных m, n существует натуральное k такое, что в произвольном графе с k вершинами найдется либо m попарно соединенных ребрами вершин, либо n попарно несоединенных. Наименьшее такое k обозначается $R(m, n)$.

б) Найдите $R(3, 4)$.

Определение 9. Назовем *расстоянием* между вершинами связного графа наименьшую длину пути, соединяющего эти вершины (длина каждого ребра считается равной 1). *Диаметром графа* называется наибольшее расстояние между его вершинами.

Определение 10. Граф называется *регулярным* графом *валентности* k, если степень каждой его вершины равна k.

Определение 11. *Графом Мура* называется регулярный граф валентности k, диаметр которого не превосходит двух, а число вершин равно $k^2 + 1$.

Задача 20*. а) Докажите, что в регулярном графе валентности k и диаметра 2 не может быть больше k^2+1 вершины.

б) Приведите примеры графов Мура при $k=1, 2, 3$.

в) Существует ли граф Мура при $k=7$?

г**) Существует ли граф Мура при $k=57$?

д) Докажите, что ни при каких других значениях k не существует графов Мура.

Задача 21*. Дан правильный 50-угольник. В одной из его вершин стоит доктор Фауст. У него есть три возможности: 1) бесплатно перейти в диаметрально противоположную точку; 2) заплатив Мефистофелю 1 рубль 5 копеек, перейти на соседнюю вершину против часовой стрелки; 3) получив от Мефистофеля 1 рубль 5 копеек перейти на соседнюю вершину по часовой стрелке. Известно, что доктор Фауст везде побывал (хотя бы один раз). Докажите, что на каком-то отрезке пути кто-то кому-то заплатил не меньше 25 рублей.

Подстановки 2

листок 2д / декабрь 2004

Определение 1. Пусть дана подстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$. *Беспорядком* называется пара (k, l), $1 \leqslant k < l \leqslant n$, такая что $j_k > j_l$. Подстановка называется *четной*, если число беспорядков в ней четно, и *нечетной* в противном случае.

Задача 0. Определим четность подстановки, записанной в произвольной форме, как четность суммы беспорядков в верхней и нижней строках. Докажите, что тем самым получится эквивалентное определение (т. е. все подстановки, являющиеся четными (нечетными) по определению 1, будут также являться четными (нечетными) по новому определению и наоборот).

Задача 1. Найдите четности подстановок из задач 1, 2 предыдущего листка.

Задача 2. Пусть a и b — подстановки на множестве из четырех элементов, $a = (1, 2, 3, 4)$, $b = (1, 4, 3)$. Какие из следующих подстановок четны, а какие нечетны: а) e; б) a; в) b; г) $b^2 = b \cdot b$; д) $b^3 = b \cdot b \cdot b$; е) ab; ж) ba?

Задача 3. Докажите, что а) при умножении на транспозицию (справа или слева) четность меняется; б) четность произведения k транспозиций равна четности числа k.

Задача 4. а) Как выражается четность ab через четность a и четность b?

б) Как выражается четность a^n через четность a?

Задача 5. Каких подстановок в S_n больше: четных или нечетных?

Задача 6*. Докажите, что если в игре «пятнашки» поменять местами фишки с номерами «14» и «15», то, играя в эту игру, невозможно получить первоначальное расположение фишек.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Задача 7*. Докажите, что из любого расположения фишек можно, соблюдая правила игры, получить либо начальное расположение, либо расположение, описанное в предыдущей задаче.

Определение 2. Подстановкой, *обратной* к подстановке $a \in S_n$, называется такая подстановка $b \in S_n$, что $ab = ba = e$. Обозначение: a^{-1}.

Задача 8. Докажите, что для любых двух подстановок a и b имеет место равенство $(ab)^{-1} = b^{-1}a^{-1}$.

Задача 9. Найдите все $a \in S_n$, такие что для любой подстановки $b \in S_n$ выполняются равенства: а) $ba = b$; б) $ba = ab$; в*) $ba = ab^{-1}$.

Задача 10* (замена переменных). Пусть даны подстановки $a, c \in S_n$, и пусть $b = c^{-1}ac$.

а) Докажите, что если подстановка a задана таблицей $a = \binom{i_1 \dots i_n}{j_1 \dots j_n}$, то $b = \binom{c(i_1) \dots c(i_n)}{c(j_1) \dots c(j_n)}$.

б) Докажите, что если подстановка a задана в виде произведения независимых циклов $a = (i_1 \dots i_k) \cdot (j_1 \dots j_l) \cdot \dots$, то $b = (c(i_1) \dots c(i_k)) \cdot (c(j_1) \dots c(j_l)) \cdot \dots$

Задача 11. Дайте определение *степени подстановки* a^k для любого целого k.

Задача 12. Докажите, что для любых $a, b \in S_n$ и любых целых k и l выполняется следующее: а) $a^0 = e$; $a^1 = a$; $a^{k+l} = a^k a^l$; $a^{kl} = (a^k)^l$; б) если $ab = ba$, то $(ab)^k = a^k b^k$.

Задача 13. а) Докажите, что для любых $a, b \in S_n$ существуют и при том единственные $x, y \in S_n$, такие что $ax = b$, $ya = b$. Обязательно ли $x = y$?

б) Докажите, что для любых $a, b, c \in S_n$

$$(a = b) \iff (ac = bc) \iff (ca = cb).$$

Задача 14. Докажите, что для любой подстановки $a \in S_n$ существует натуральное k, такое что $a^k = e$.

Определение 3. Наименьшее натуральное k, такое что для подстановки $a \in S_n$ выполняется равенство $a^k = e$, называется *порядком подстановки* a.

Задача 15. Пусть подстановка σ представлена в виде произведения независимых циклов $c_1, \dots, c_n$. Докажите, что порядок подстановки σ равен НОК($|c_1|, \dots, |c_n|$) (где $|c_i|$ есть длина цикла c_i).

Задача 16. Если k — порядок подстановки a, то $a^n = e$ тогда и только тогда, когда n делится на k.

Задача 17. Вычислите: а) $\binom{123}{321}^{100}$; б) $\binom{1234}{2341}^{1000}$; в) $\binom{12345}{35214}^{-2007}$; г) $\binom{12345}{45213}^{500}$; д) $\binom{123456}{452631}^{-127}$; е) $\binom{1234567}{7651234}^{1001}$.

Целые числа 1. Делимость целых чисел

листок 7 / декабрь 2004

Соглашение. Все числа в этом листке предполагаются целыми.

Определение 1. Целое число a *делится* на ненулевое целое число b, если существует такое целое число k, что $a = kb$. В этом случае b называется *делителем* a. Говорят также, что b *делит* a.

Обозначения: $a \vdots b$ или $b \mid a$.

Задача 1. Докажите, что для любого a:

а) если $a \neq 0$, то $a \vdots a$; б) $a \vdots 1$; в) если $a \neq 0$, то $0 \vdots a$.

Задача 2. Докажите, что для любых a, b, c, x, y:

а) если $a \vdots b$ и $b \vdots c$, то $a \vdots c$;
б) если $a \vdots b$ и $a \neq 0$, то $|a| \geqslant |b|$;
в) если $c \neq 0$, то $a \vdots b \iff ac \vdots bc$;
г) если $a \vdots b$ и $c \vdots b$, то $(a \pm c) \vdots b$;
д) если $a \vdots b$ и $c \vdots b$, то $ax + cy \vdots b$;
е) если $a \vdots b$ и $b \vdots a$, то $a = b$ или $a = -b$;
ж) если $a \vdots b$, то $ac \vdots b$;
з) если $a \vdots b$ и $c \not\vdots b$, то $(a + c) \not\vdots b$;
и) если $ab = cd$ и $a \vdots c$, то $d \vdots b$.

Задача 3. Верно ли, что для любых a, b, c, d:

а) если $b \mid a$ и $c \not\mid b$, то $c \mid a$;
б) если $b \mid a$ и $c \mid a$, то $bc \mid a$;
в) если $c \mid ab$, то $c \mid a$ или $c \mid b$?

Задача 4. Сформулируйте признаки делимости (натурального числа): а) на 2; б) на 3; в) на 4; г) на 5; д) на 9; е) на 11.

Задача 5. Может ли число, сумма цифр которого равна 2004, быть полным квадратом?

Задача 6*. Число a в три раза больше суммы своих цифр. Докажите, что число a делится на 27.

Задача 7. Докажите, что: а) если $a^2 \vdots (a + b)$, то $b^2 \vdots (a + b)$; б*) если $x + y + z \neq 0$, то $(x^3 + y^3 + z^3 - 3xyz) \vdots (x + y + z)$.

Задача 8. У каких натуральных чисел количество положительных делителей нечетно?

Определение 2. Число $p > 1$ называется *простым*, когда оно делится лишь на $1, -1, p$ и $-p$. Остальные натуральные числа, кроме единицы, называются *составными*.

Задача 9. Докажите, что простых чисел бесконечно много.

Задача 10. Докажите, что для любого n найдутся n подряд идущих составных чисел.

Задача 11*. Обозначим через $n?$ произведение всех простых чисел, меньших n. Докажите, что при $n > 3$ выполняется неравенство $n? > n$.

Задача 12. а) Найдите все простые p такие, что $p+2$ и $p+4$ также простые.

б**) Докажите, что существует бесконечно много таких простых чисел p, что число $p+2$ также простое.

Задача 13 (решето Эратосфена). На доске написаны все числа от 2 до 1000. Эратосфен обводит число 2 в кружочек и стирает все числа, отличные от 2, которые делятся на 2. Затем он повторяет этот процесс, а именно обводит в кружочек наименьшее необведенное число и стирает все остальные числа, которые делятся на это число. Процесс заканчивается, когда на доске остаются только обведенные числа. Какие числа останутся на доске? (Их не нужно выписывать.)

Задача 14. Выпишите все простые числа, меньшие 100.

Задача 15. Докажите, что число a — составное, если и только если a делится на какое-нибудь простое число, не превосходящее $\sqrt{a}$.

Задача 16. Докажите, что:

а) любое целое число, большее 1, можно представить в виде произведения простых чисел;

б) каждое целое число x, большее 1, можно представить в виде

$$x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n},$$

где $p_1 < p_2 < \dots < p_n$ — простые числа, $a_1, a_2, \dots, a_n$ — положительные целые числа;

в*) (*Основная теорема арифметики*) если число x представлено двумя способами в таком виде, а точнее

$$x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} = q_1^{b_1} q_2^{b_2} \dots q_m^{b_m},$$

то эти разложения совпадают, то есть $m = n$ и при любом $1 \leqslant i \leqslant n$ $p_i = q_i$, $a_i = b_i$;

г) если в этом разложении все a_i четны, то x есть точный квадрат, то есть найдется такое целое y, что $x = y^2$.

Задача 17. Разложите на простые множители числа 1024, 57, 84, 91, 391, 101, 1000, 1001, 1543.

Целые числа 2. Алгоритм Евклида

листок 8 / декабрь 2004

Соглашение. Все числа в этом листке предполагаются целыми.

Задача 1. Докажите, что для любых a и $b \neq 0$ существуют и единственны q и r такие, что: 1) $a = qb + r$; 2) $0 \leqslant r < |b|$.

Определение 1. Такие q и r называются, соответственно, *частным* и *остатком* при делении a на b.

Задача 2. Найдите частное и остаток при делении: а) -17 на 4; б) 23 на -7; в) -1 на -5.

Задача 3. Какие частные могут получиться при делении числа 59?

Задача 4. Найдите частное и остаток при делении: а) n^2 на $n+1$; б) n^2+n+2 на $n-1$; в) $2^{100}-1$ на 2^7-1; г*) 2^m-1 на 2^n-1.

Задача 5*. а) Покажите, что $a^{2k+1}+1$ всегда делится на $a+1$ без остатка.

б) Найдите остаток от деления $a^{2k}+1$ на $a+1$.

Определение 2. *Наибольшим общим делителем* чисел a и b называется наибольшее из таких чисел d, что $a \vdots d$, $b \vdots d$.

Обозначение: НОД(a, b).

Задача 6. Докажите, что для любых a и b ($a \neq 0$ или $b \neq 0$) НОД(a, b) существует и единственен.

Задача 7. Докажите, что для любых a, b и c ($a \neq 0$ или $b \neq 0$):

а) НОД$(a, b) \geqslant 1$; б) НОД$(a, b) = |a| \Leftrightarrow b \vdots a$;

в) НОД$(a, ca+b) =$ НОД(a, b).

Задача 8 (алгоритм Евклида). Рассмотрим следующий процесс. Пусть (a, b) — пара положительных чисел такая, что $a \geqslant b$. Она заменяется на пару (b, r), где r — остаток от деления a на b. Пара (b, r) заменяется по тому же правилу и так далее. Процесс завершается, когда получается пара вида $(d, 0)$. Покажите, что:

а) процесс всегда завершается;

б) $d =$ НОД(a, b).

Задача 9. Вычислите при помощи алгоритма Евклида:

а) НОД$(91, 147)$; б) НОД$(-144, -233)$.

Задача 10. Пусть $0 < a < 1000$, $0 < b < 1000$. Верно ли, что алгоритм Евклида закончится после не более, чем: а) 14; б) 13 шагов?

Задача 11. Покажите, как при помощи алгоритма Евклида можно по произвольным a и b найти такие k и l, что $ak+bl=\text{НОД}(a,b)$.

Задача 12. Докажите, что уравнение $ax+by=d$ имеет решение в целых числах тогда и только тогда, когда $d\vdots\text{НОД}(a,b)$. В частности, $\text{НОД}(a,b)$ — это наименьшее натуральное число, представимое в виде $ax+by$.

Задача 13. Даны углы в 32° и 25°. Постройте угол в 1°.

Задача 14. Докажите, что если p — простое, то либо a делится на p, либо найдутся такие x и y, что $ax+py=1$.

Задача 15. Пусть p — простое число. Докажите, что если $ab\vdots p$, то $a\vdots p$ или $b\vdots p$.

Задача 16. Докажите основную теорему арифметики (задача 16в листка «Целые числа 1»).

Определение 3. *Наименьшим общим кратным* чисел a и b называется наименьшее из таких положительных чисел d, что $d\vdots a$, $d\vdots b$.

Обозначение: $\text{НОК}(a,b)$.

Задача 17. Докажите, что для любых a и b $(ab\neq 0)$:

а) $\text{НОК}(a,b)$ существует и единственен;

б) $\text{НОК}(a,b)\cdot\text{НОД}(a,b)=ab$.

Задача 18. Найдите $\text{НОК}(12,15)$, $\text{НОК}(120,45)$.

Задача 19. Пусть (x_0,y_0) — решение уравнения

$$ax+by=d.$$

Пусть a_0 и b_0 — такие числа, что $\text{НОД}(a,b)a_0=a$, $\text{НОД}(a,b)b_0=b$. Покажите, что каждое решение уравнения $ax+by=d$ имеет вид

$$x=x_0+b_0t,\quad y=y_0-a_0t,$$

где $t\in\mathbb{Z}$.

Задача 20. Решите уравнения: а) $121x+91y=1$; б) $-343x+119y=42$; в) $111x-740y=11$.

Задача 21*. Есть шоколадка в форме равностороннего треугольника со стороной n, разделенная бороздками на равносторонние треугольники со стороной 1. Играют двое. За ход можно отломить от шоколадки треугольный кусок вдоль бороздки, съесть его, а остаток передать противнику. Тот, кто получит последний кусок — треугольник со стороной 1, — победитель. Тот, кто не может сделать ход, досрочно проигрывает. Кто выигрывает при правильной игре?

Отношения эквивалентности

листок 9 / январь 2005

Определение 1. Пусть M — множество. Произвольное множество $R \subset \{(a, b) \mid a, b \in M\}$ упорядоченных пар элементов M называется (*бинарным*) *отношением* на M. Если $(a, b) \in R$, то пишут $a \sim_R b$, или просто $a \sim b$.

Задача 0. Изобразите в виде таблицы и в виде графа отношения:

а) $a \sim_R b$, если $a \equiv b \pmod 2$ на $X = \{0, \ldots, 9\}$.

б) $a \sim_R b$, если $b \mid a$ на $X = \{2, \ldots, 15\}$ (в этом пункте таблицу рисовать не надо).

в) $A \sim_R B$, если $A \subset B$ на множестве всех подмножеств множества $\{0, 1, 2\}$.

г) $a \sim_R b$, если $a = b$ на $X = \{0, \ldots, 5\}$.

д) $a \sim_R b$, если $a \geqslant b$ на $X = \{0, \ldots, 5\}$.

Определение 2. Отношение $\sim$ на M называется:

1) рефлексивным, если из $a \in M$ следует $a \sim a$;

2) симметричным, если для любых $a, b \in M$ из $a \sim b$ следует $b \sim a$;

3) транзитивным, если для любых $a, b, c \in M$ из $a \sim b$ и $b \sim c$ следует $a \sim c$.

Задача 1. Сколько существует отношений на множестве из n элементов? Сколько существует симметричных отношений на множестве из n элементов?

Задача 2. Приведите примеры отношений, которые удовлетворяют ровно одному, ровно двум свойствам из определения 2.

Определение 3. Отношение $\sim$ на M называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Задача 3. Укажите, какие из следующих отношений являются рефлексивными, симметричными, транзитивными, отношениями эквивалентности (в кавычках указано условие, при котором $a \sim b$):

а) $a \sim b$ для всех $a, b \in M$, на множестве M;

б) $\varnothing$ на множестве M;

в) «$a \mid b$» на множестве натуральных чисел;

г) «a и b можно соединить путем» на множестве вершин графа;

д) «$A \subset B$» на множестве всех подмножеств данного множества;

е) «a и b имеют один и тот же остаток при делении на 2» на множестве натуральных чисел;

ж) «a и b имеют одну и ту же последнюю цифру» на множестве натуральных чисел;

з) «a и b учатся в одном классе» на множестве учеников 57 школы;

и) «a и b родились в одном месяце» на множестве учеников 8 «в» класса 57 школы;

к) «между a и b существует биекция» на множестве всех подмножеств множества натуральных чисел;

л) «$a > b$» на множестве натуральных чисел;

м) фиксируем $X \subset M$. Отношение на множестве M зададим правилом «$a \sim a$ и, если $a \neq b$, то $a \sim b$, если и только если $a, b \in X$»;

н) фиксируем $f\colon X \to Y$. Отношение на множестве X зададим правилом «$a \sim b$ если и только если $f(a) = f(b)$;

о) «a и b являются гражданами одного государства» на множестве людей на Земле;

п) «три стороны одного треугольника равны трем сторонам второго треугольника» на множестве всех треугольников на плоскости;

р) выбранное вами отношение на множестве натуральных чисел;

с) выбранное вами отношение на множестве учеников 57 школы.

Задача 4. Докажите, что отношение эквивалентности на множестве задает отношение эквивалентности на каждом его подмножестве.

Определение 4. Пусть $\sim$ — отношение эквивалентности на M, $a \in M$. Множество $N_a = \{x \in M \mid a \sim x\}$ называется *классом эквивалентности* элемента a.

Задача 5. Докажите, что для любого отношения эквивалентности классы эквивалентности либо не пересекаются, либо совпадают. Докажите, что каждое отношение эквивалентности на M задает разбиение множества M на непересекающиеся классы эквивалентности.

Определение 5. Пусть $\sim$ — отношение эквивалентности на M. Множество классов эквивалентности называется *фактормножеством* и обозначается $M/\sim$.

Задача 6. Опишите классы эквивалентности и фактормножества для отношений эквивалентности задачи 3.

Задача 7. Рассмотрим следующее отношение на множестве S_n: $a \sim b$, если существует такая подстановка c, что $c^{-1}ac = b$.

а) Докажите, что это отношение является отношением эквивалентности (такие подстановки называются *сопряженными*, а отношение — и иногда операция — называется *сопряжением*).

б*) Придумайте простой способ проверки, эквивалентны ли подстановки a и b, и выясните, какие из указанных преподавателем подстановок эквивалентны.

Целые числа 3. Сравнения

листок 10 / февраль 2005

Определение 1. Числа a и b *сравнимы* по модулю $m \neq 0$, если $a - b \vdots m$.
Обозначение: $a \equiv b \pmod{m}$.

Задача 1. Докажите, что a сравнимо с b по модулю m тогда и только тогда, когда остаток от деления a на m равен остатку от деления b на m.

Задача 2. Докажите, что сравнимость по модулю m является отношением эквивалентности.

Задача 3. Докажите, что для любых a_1, a_2, b_1, b_2, c, m:
а) $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$;
б) $a_1 \equiv b_1 \pmod{m} \Rightarrow ca_1 \equiv cb_1 \pmod{m}$;
в) $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Задача 4. Докажите, что если $a \equiv b \pmod{m}$, то:
а) $a^n \equiv b^n \pmod{m}$ для любого неотрицательного n;
б*) для любого многочлена $f(x)$ с целыми коэффициентами $f(a) \equiv f(b) \pmod{m}$.

Задача 5. Верно ли, что если $a \equiv b \pmod{m}$ и $a, b \geqslant 0$, то $2^a \equiv 2^b \pmod{m}$?

Задача 6. Пусть $\overline{a_n a_{n-1} \ldots a_1 a_0}$ — десятичная запись числа x. Докажите, что:
а) $x \equiv a_0 + \ldots + a_n \pmod{3}$, $x \equiv a_0 + \ldots + a_n \pmod{9}$;
б) $x \equiv a_0 \pmod{2}$, $x \equiv a_0 \pmod{5}$;
в) $x \equiv a_0 - a_1 + \ldots + (-1)^n a_n \pmod{11}$.

Задача 7. Докажите, что если x нечетно, то $x^2 \equiv 1 \pmod{8}$.

Задача 8*. Докажите, что следующие уравнения не имеют ненулевых решений в целых числах: а) $x^2 + y^2 = 3z^2$; б) $x^2 + y^2 + z^2 = 4t^2$.

Задача 9*. Докажите, что существует бесконечно много натуральных чисел, не представимых в виде суммы трех а) квадратов; б) кубов натуральных чисел.

Задача 10. Решите сравнения: а) $3x \equiv 1 \pmod{7}$; б) $6x \equiv 5 \pmod{9}$; в) $4x \equiv 2 \pmod{10}$.

Задача 11. Сравнение $ax \equiv b \pmod{m}$ имеет решение тогда и только тогда, когда $b \vdots \text{НОД}(a, m)$.

Задача 12. Пусть p — простое число, $a \not\equiv 0 \pmod{p}$, тогда сравнение $ax \equiv b \pmod{p}$ имеет решение, причем любые два решения этого сравнения сравнимы по модулю p.

Задача 13* (китайская теорема об остатках). Пусть числа $a_1, a_2, \ldots, a_n$ попарно взаимно просты. Тогда для любых $b_1, b_2, \ldots, b_n$ найдется x такое, что

$$x \equiv b_i \pmod{a_i}, \quad i = 1, \ldots, n,$$

причем любые два числа, удовлетворяющие этому условию, сравнимы по модулю $a_1 \ldots a_n$.

Задача 14*. Найдите все решения системы сравнений

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{7} \\ x \equiv 4 \pmod{9}. \end{cases}$$

Задача 15. Пусть p — простое число. Докажите, что:
а) $C_p^k \vdots p$ при $0 < k < p$;
б) $(a+b)^p \equiv a^p + b^p \pmod{p}$;
в) (*малая теорема Ферма*) $a^p - a \vdots p$.

Задача 16* (теорема Вильсона). Пусть p — простое число, тогда $(p-1)! \equiv -1 \pmod{p}$.

Задача 17. Какими правильными многоугольниками можно замостить плоскость?

Задача 18. Докажите, что имеется бесконечное количество простых чисел вида: а) $4n+3$; б*) $4n+1$; в**) $an+b$, где НОД$(a, b) = 1$.

Задача 19*. Найдите количество решений сравнения $x^2 \equiv 1 \pmod{n}$: а) при простом n; б) при произвольном n.

Целые числа 4. Практические задачи

листок 11 / март 2005

Задача 1. Верно ли, что для любого $n>1$ выполняется:
а) $n^3+5n \vdots 6$; б) $2n^3+3n^2+7n \vdots 6$; в) $n^5-n \vdots 30$; г) $2^{2n}-1 \vdots 6$;
д) $11^{6n+3}+1 \vdots 148$?

Задача 2. Дайте определение: а) НОД; б) НОК чисел $a_1, a_2, \ldots, a_n$ $(n>2)$.

Определение 1. *Наибольшим общим делителем* чисел $a_1, a_2 \ldots, a_n$ называется наибольшее из таких чисел d, что $a_1 \vdots d$, $a_2 \vdots d$, $\ldots$, $a_n \vdots d$.

Определение 2. *Наименьшим общим кратным* чисел $a_1, a_2, \ldots, a_n$ называется наименьшее из таких положительных чисел d, что $d \vdots a_1$, $d \vdots a_2$, $\ldots$, $d \vdots a_n$.

Задача 3. Докажите, что для любых a, b и c, таких что $a \cdot b \cdot c \neq 0$:
а) $\text{НОД}(a,b,c) = \text{НОД}(a, \text{НОД}(b,c)) = \text{НОД}(\text{НОД}(a,b),c)$;
б) $\text{НОК}(a,b,c) = \dfrac{|abc| \cdot \text{НОД}(a,b,c)}{\text{НОД}(a,b) \cdot \text{НОД}(b,c) \cdot \text{НОД}(a,c)}$.

Задача 4. Существует ли число, которое при делении на числа 2, 3, 4, 5 и 6 дает в остатке соответственно:
а) 1, 2, 3, 4, 5; б) 0, 1, 2, 3, 4; в) 0, 1, 2, 3, 2?

Задача 5. Вычислите НОД чисел:
а) 923 и 1207; б) 279 и -589; в) -693 и 2475;
г) -697 и -1377; д) 1517 и 1591; е) 1134, 2268 и 1575.

Задача 6. Вычислите НОК чисел:
а) 16 и 84; б) 819 и 504; в) 30, 56 и 72;
г) 340, 990 и 46; д) 41, 85 и 36; е) 2, 5, 7, 9 и 11.

Задача 7. Для $n>0$ найдите значения следующих выражений:
а) $1 \cdot 2 + 2 \cdot 3 + \ldots + (n-1) \cdot n$;
б) $\dfrac{1}{4 \cdot 5} + \dfrac{1}{5 \cdot 6} + \ldots + \dfrac{1}{(n+3)(n+4)}$;
в*) $1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \ldots + n \cdot (n+1) \cdot (n+2)$.

Задача 8. Докажите тождества:
а) $(n+1) \cdot (n+2) \cdot \ldots \cdot (n+n) = 2^n \cdot 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)$;
б) $1 - \dfrac{1}{2} + \dfrac{1}{3} - \ldots + \dfrac{1}{2n-1} - \dfrac{1}{2n} = \dfrac{1}{n+1} + \dfrac{1}{n+2} + \ldots + \dfrac{1}{2n}$;
в) $\left(1 - \dfrac{1}{4}\right) \cdot \left(1 - \dfrac{1}{9}\right) \cdot \ldots \cdot \left(1 - \dfrac{1}{(n+1)^2}\right) = \dfrac{n+2}{2n+2}$.

Задача 9. Решите в целых числах уравнения:
а) $7x+5y=1$; б) $27x-24y=1$; в) $12x-33y=9$;
г) $-56x+91y=21$; д) $344x-215y=86$; е) $3x+5y+7z=1$.

Задача 10. Верно ли, что для любого натурального n числа $10n+7$ и $10n+5$ взаимно просты?

Задача 11. Найдите такие числа a и b, что $ax+by=1$ при:
а) $x=7$, $y=9$; б) $x=17$, $y=19$; в) $x=27$, $y=29$;
г) $x=37$, $y=39$; д) $x=47$, $y=49$.

Задача 12. Определим последовательность чисел $u(n)$ по правилу: $u(0)=0$, $u(1)=1$, $u(n)=u(n-1)+u(n-2)$ (*числа Фибоначчи*).
а) Докажите, что $u(1)+\ldots+u(n)=u(n+2)-1$.
б) Докажите, что $(u(1))^2+\ldots+(u(n))^2=u(n)\cdot u(n+1)$.
в) (*формула Бине*) Как связаны числа $u(n)$ и

$$\delta(n)=\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n-\frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n?$$

Теория групп

листок 12 / март 2005

Соглашение. Все числа в этом листке предполагаются целыми, а число p — простым.

Определение 1. *Бинарной операцией* $\cdot$ на множестве M называется отображение из множества упорядоченных пар $M^2 = \{(a, b) \mid a \in M, b \in M\}$ в множество M, то есть способ поставить каждой паре элементов множества M единственный элемент этого множества. Образ пары (a, b) обозначается $a \cdot b$.

Определение 2. Пара $(G, \cdot)$, состоящая из множества G и бинарной операции $\cdot$ на нем, называется *группой*, если выполнены следующие свойства:

1) $\forall a, b, c \in G\colon a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ассоциативность);

2) $\exists e \in G\ \forall a \in G\colon e \cdot a = a \cdot e = a$ (существование единицы);

3) $\forall a \in G\ \exists a^{-1} \in G\colon a^{-1} \cdot a = a \cdot a^{-1} = e$ (существование обратного).

Если в G содержится конечное число элементов, то G называется *конечной группой*. Число элементов конечной группы G называется *порядком* группы G и обозначается $|G|$.

Соглашение. Условие ассоциативности означает, что в произведении нескольких сомножителей расстановка скобок не влияет на ответ. Поэтому впоследствии скобки в произведении нескольких сомножителей не ставятся.

Задача 1. Является ли группой:

а) $(\mathbb{Z}, +)$; б) $(\mathbb{Z}, -)$; в) $(\mathbb{N}, \cdot)$; г) $(S_n, \cdot)$;

д) множество четных чисел с операцией сложения;

е) множество нечетных чисел с операцией сложения;

ж) множество отображений $f\colon X \to X$ с операцией взятия композиции;

з) множество $P(A)$ всех подмножеств множества A с операцией $\cup$;

и) $(P(A), \cap)$; к) $(P(A), \setminus)$;

л) $(P(A), \triangle)$, где $A \triangle B = (A \cup B) \setminus (A \cap B)$;

м) $(\mathbb{Z}/n\mathbb{Z}, +_n)$, где $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$, $a +_n b$ — остаток от деления числа $a + b$ на число n;

н) $(\mathbb{Z}/n\mathbb{Z}, \cdot_n)$, где $a \cdot_n b$ — остаток от деления числа ab на число n;

о) $(\mathbb{N}, \cdot)$, где $a \cdot b = a^b$;

п) $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \cdot_n)$;

р) $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot_n)$, где $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \text{НОД}(a, n) = 1\}$?

Определение 3. Группа G называется *коммутативной* (или *абелевой*), если для любых $a, b \in G$ выполнено $ab = ba$.

Задача 2. Какие из групп задачи 1 коммутативны?

Задача 3. Докажите, что:
а) единица единственна; б) обратный элемент единственен;
в) $ba = e \Rightarrow b = a^{-1}$; г) $ba = a \Rightarrow b = e$; д) $(a^{-1})^{-1} = a$.

Задача 4*. Докажите, что если в определении 2 свойства существования единицы и существования обратного заменить на свойства:
1°) $\exists e \in G\ \forall a \in G\colon ea = a$ (левая единица);
2°) $\forall a\ \exists a^{-1}\colon a^{-1}a = e$ (левый обратный),
то получится определение группы, эквивалентное определению 2.

Определение 4. Отображение $f\colon G \to H$ из группы G в группу H называется изоморфизмом, если оно взаимно однозначно и сохраняет операцию, то есть $\forall x, y \in G\ f(x * y) = f(x) * f(y)$. Если такое отображение существует, то группы G и H называются изоморфными.

Задача 5. Выпишите все попарно неизоморфные группы из: а) 1, 2, 3; б) 4; в*) 13 элементов.

Определение 5. Непустое подмножество H группы G, замкнутое относительно операций $\cdot$ и взятия обратного элемента, называется *подгруппой*.

Задача 6. Верно ли, что:
а) если H — подгруппа G, то $e \in H$;
б) если H — подгруппа G, то H — группа;
в) если K — подгруппа H, а H — подгруппа G, то K — подгруппа G;
г) объединение двух подгрупп — подгруппа;
д) пересечение двух подгрупп — подгруппа?

Задача 7. Верно ли, что:
а) $\mathbb{N}$ — подгруппа $\mathbb{Z}$;
б) A_n — подгруппа S_n, где A_n — множество четных подстановок на множестве из n элементов;
в) $S_n \setminus A_n$ — подгруппа S_n?

Задача 8. Перечислите все подгруппы: а) S_3; б) $\mathbb{Z}$.

Определение 6. Наименьшее натуральное k, такое что для элемента $a \in G$ выполняется равенство $a^k = e$, называется *порядком элемента* a. Обозначение: $\operatorname{ord} a$. Если такого числа не существует, то говорят, что $\operatorname{ord} a = 0$.

Задача 9. Докажите, что в конечной группе $\operatorname{ord} a > 0$ для любого элемента a.

Задача 10. Докажите, что $a^n = e$ тогда и только тогда, когда $\operatorname{ord} a \mid n$.

Определение 7. *Левым (правым) смежным классом* группы G относительно подгруппы H называется множество вида $aH = \{ax \mid x \in H\}$ (соответственно вида $Ha = \{xa \mid x \in H\}$).

Задача 11. Докажите, что левые (правые) смежные классы между собой либо не пересекаются, либо совпадают.

Задача 12. Найдите разбиение на левые и правые смежные классы группы по подгруппе: а) $\mathbb{Z}/2\mathbb{Z}$; б) S_4/A_4; в) $S_3/\langle(12)\rangle$.

Задача 13 (теорема Лагранжа). Докажите, что для любой конечной группы G подрядок любой ее подгруппы H делит порядок группы G ($|G| \vdots |H|$).

Задача 14. Докажите, что порядок любого элемента конечной группы G делит порядок группы G ($|G| \vdots \operatorname{ord} a$).

Определение 8. Обозначим через $\varphi(n)$ число натуральных чисел, не превосходящих n и взаимно простых с n. Функция $\varphi(n)$ называется *функцией Эйлера*.

Задача 15. Найдите: а) $\varphi(2)$, $\varphi(6)$, $\varphi(30)$; б) $\varphi(p)$; в) $\varphi(p^n)$.

Задача 16. Докажите, что для любых взаимно простых чисел m и n выполнено равенство $\varphi(mn) = \varphi(m)\varphi(n)$.

Задача 17. Найдите $\varphi(p_1^{k_1} \cdot \ldots \cdot p_n^{k_n})$.

Задача 18 (теорема Эйлера). Докажите, что для любого числа a, взаимно простого с n, выполнено равенство $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Задача 19*. Опишите группы симметрий: а) правильного треугольника; б) квадрата; в) правильного n-угольника (*группа диэдра* D_n).

Теория графов 2

листок 3д / март 2005

Задача 1. В турнире по олимпийской системе участвовали n команд. Сколько всего было сыграно матчей?

Задача 2. Докажите, что граф с n вершинами, степень каждой из которых не менее $\frac{n-1}{2}$, связен.

Задача 3. В связном графе все вершины имеют степень 100. Докажите, что после удаления любого из ребер он остается связным.

Задача 4. Докажите, что в любом связном графе есть подграф, являющийся деревом и содержащий все вершины (максимальное поддерево).

Задача 5. Докажите, что из любого связного графа можно выкинуть вершину и выходящие из нее ребра так, чтобы он остался связным.

Задача 6*. В кубической коробке $n \times n \times n$ лежало n^3 единичных кубиков. Кубики высыпали, каждый просверлили по диагонали, затем все плотно нанизали на нить и связали в кольцо (соединили вершину первого кубика с вершиной последнего). При каких n получившееся «ожерелье» можно убрать обратно в коробку?

Задача 7*. Все 28 Петиных одноклассников имеют по различному числу друзей в этом классе. Сколько из них дружат с Петей? А если одноклассников n?

Задача 8* (теорема Кэли). В графе с n вершинами каждая вершина соединена с каждой ребром (такой граф называется *полным*). Докажите, что существует ровно n^{n-2} способов выкинуть несколько ребер так, чтобы оставшийся граф являлся деревом.

Определение 1. *Ориентированным графом* называется граф, на ребрах которого поставлены стрелки. Его ребра называются *дугами*. Более формально, ориентированный граф — это пара $\Gamma = (V, E)$ из конечного множества вершин V и множества дуг E, элементами которого являются упорядоченные пары вершин графа Γ.

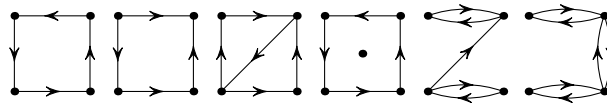
Заметим, что у нас в ориентированном графе разрешаются дуги из вершины в себя саму (*петли*), несколько дуг из одной вершины в другую (*кратные дуги*), «встречные» дуги (из A в B и из B в A).

То, что раньше называлось графом, мы теперь будем называть *неориентированным графом*.

Задача 9. Дайте (формальные!) определения *пути* и *цикла* в ориентированном графе.

Определение 2. Ориентированный граф называется *сильно связным*, если для любых двух его вершин существует путь как из первой во вторую, так и из второй в первую.

Задача 10. Какие из следующих графов сильно связны?



Определение 3. Ориентированный граф называется *связным*, если он окажется связным неориентированным графом после того, как мы сотрем стрелки с его дуг.

Задача 11. а) Приведите пример связного, но не сильно связного ориентированного графа.

б) Приведите пример связного ориентированного графа, в котором для некоторых двух вершин A и B нет пути ни из A в B, ни из B в A.

Задача 12. Докажите, что на ребрах связного неориентированного графа можно так расставить стрелки, чтобы из одной из вершин существовали пути во все остальные.

Задача 13. Можно ли так расставить на ребрах полного неориентированного графа стрелки, чтобы в полученном ориентированном графе не было циклов?

Задача 14. В полном неориентированном графе на ребрах как-то расставили стрелки. Докажите, что найдется вершина, из которой существуют пути во все остальные.

Задача 15* (задача 17* из листка «Теория графов 1»). В полном неориентированном графе на ребрах как-то расставили стрелки. Докажите, что полученный граф гамильтонов (т. е. существует путь, проходящий по каждой вершине ровно по одному разу).

Задача 16*. В полном неориентированном графе с не менее чем тремя вершинами на ребрах как-то расставили стрелки. Докажите, что можно заменить не более одной дуги на противоположную так, чтобы полученный граф стал сильно связным.

Определение 4. Количество дуг, входящих в вершину (ориентированного графа), называется *входной полустепенью* (или *полустепенью захода*) этой вершины. Количество выходящих дуг называется *выходной полустепенью* (или *полустепенью исхода*).

Задача 17. Найдите входные и выходные полустепени каждой вершины для всех графов из задачи 10.

Задача 18. Что можно сказать о сумме всех входных полустепеней и сумме всех выходных полустепеней одного и того же ориентированного графа?

Задача 19. Сформулируйте и докажите критерий эйлеровости ориентированного графа.

Задача 20 (цикл де Брюина). Для того, чтобы открыть кодовый замок (с кнопками от 0 до 9), необходимо набрать код из четырех цифр, причем не важно, что было нажато до набора правильного кода. За какое наименьшее количество нажатий его можно гарантированно открыть?

Задача 21. 20 школьников решали 20 задач. Каждый решил ровно две задачи, и каждую задачу решили ровно двое. Докажите, что можно устроить разбор задач так, чтобы каждый рассказал одну решенную им задачу.

Определение 5. Граф называется *двудольным*, если его вершины можно разбить на две группы (называемые *долями*) так, чтобы все ребра (или дуги) были между различными долями.

Паросочетанием называется такой набор ребер графа, что каждая вершина графа является концом не более одного ребра из набора. Паросочетание называется *совершенным*, если каждая вершина является концом ровно одного ребра паросочетания.

Раскраска вершин графа называется *правильной*, если никакие две вершины одного цвета не соединены ребром. Граф называется *k-дольным*, если правильная раскраска его вершин возможна k цветами и не менее.

Задача 22. Какие графы из задач 1, 2 и 3 первого листка про графы являются двудольными? А сколькодольными являются остальные?

Задача 23. Равносильна ли двудольность неориентированного графа отсутствию циклов нечетной длины?

Задача 24. Любое ли дерево двудольно?

Задача 25* (теорема Холла). В некой компании n юношей. При каждом $k = 1, 2, \ldots, n$ для любых k юношей в этой компании найдется не менее k девушек, знакомых хотя бы с одним из рассматриваемых k юношей. Можно ли просватать всех юношей за знакомых девушек? Является ли это условие необходимым?

Иными словами, верно ли, что в двудольном неориентированном графе (с n вершинами в первой доле) существует паросочетание размера n тогда и только тогда, когда для каждого набора из k вершин первой доли с ними соединены хотя бы k вершин второй доли?

Задача 26* (обобщение задачи 21). Докажите, что в любом регулярном двудольном неориентированном графе есть совершенное паросочетание.

Задача 27*. Верно ли, что при любой правильной раскраске k-дольного неориентированного графа в k цветов найдется путь из k разноцветных вершин?

Определение 6. Граф называется *планарным*, если его можно нарисовать на плоскости, изобразив вершины точками, а ребра (или дуги) — непересекающимися кривыми. Граф, который нарисован на плоскости указанным выше образом, называется *плоским*. Части, на которые плоский граф делит плоскость (включая внешнюю часть) называются его *гранями*.

Задача 28. Какие графы из задач 1, 2 и 3а первого листка про графы являются планарными?

Задача 29 (формула Эйлера). Пусть в неориентированном плоском связном графе B вершин, P ребер и $Г$ граней. Тогда $B + Г - P = 2$.

Задача 30. Чему равно $B + Г - P$ для несвязного неориентированного плоского графа?

Задача 31. Пусть B, P и $Г$ — количества вершин, ребер и граней многогранника соответственно. Чему равно $B + Г - P$?

Задача 32. а) Докажите, что в плоском неориентированном графе $2P \geqslant 3Г$.

б) Докажите, что в плоском двудольном неориентированном графе $P \geqslant 2Г$.

Задача 33. Докажите, что следующие графы не планарны:

а) полный неориентированный граф с 5 вершинами. Этот граф обозначается K_5;

б) двудольный неориентированный граф с 3 вершинами в первой доле и 3 вершинами во второй доле, причем каждая вершина первой доли соединена с каждой вершиной второй (такой граф называется *полным двудольным*). Этот граф обозначается $K_{3,3}$;

в) произвольный неориентированный граф, у которого степени всех вершин не меньше шести.

Определение 7. *Подграфом* данного графа называется граф, который получается из данного выкидыванием некоторых вершин и ребер (дуг).

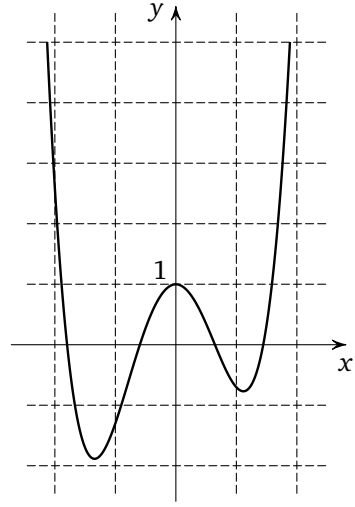
Два неориентированных графа называются *гомеоморфными*, если один можно получить из другого следующими операциями: взять ребро и добавить посередине этого ребра вершину; взять вершину степени 2 и заменить ее и выходящие из нее ребра на одно ребро (заметим, что эти две операции взаимно обратны).

Задача 34* (теорема Понтрягина — Куратовского). Докажите, что неориентированный граф планарен тогда и только тогда, когда у него нет подграфа, гомеоморфного K_5 или $K_{3,3}$.

Графики функций

листок 13 / апрель 2005

Задача 1. Функция f задана графиком. Найдите $f(0)$ и $f(1)$, решите графически уравнения $f(x)=0$, $f(x)=1$ и $f(x)=x$; найдите все c, для которых уравнение $f(x)=c$ имеет ровно одно, ровно два и ровно три решения.



Определение 1. *Целой частью* числа x называется наибольшее целое число, не превосходящее x. Обозначение: $[x]$.

Определение 2. *Дробной частью* числа x называется число $\{x\} = x - [x]$.

Определение 3. $\operatorname{sign} x = \begin{cases} 1, & \text{если } x > 0; \\ 0, & \text{если } x = 0; \\ -1, & \text{если } x < 0. \end{cases}$

Задача 2. а) Найдите [3,5], [−2,2], {1,1}, {−2,7}, [0], {0}, [5], {5}, sign(5,6), sign(−2,4), sign(0).

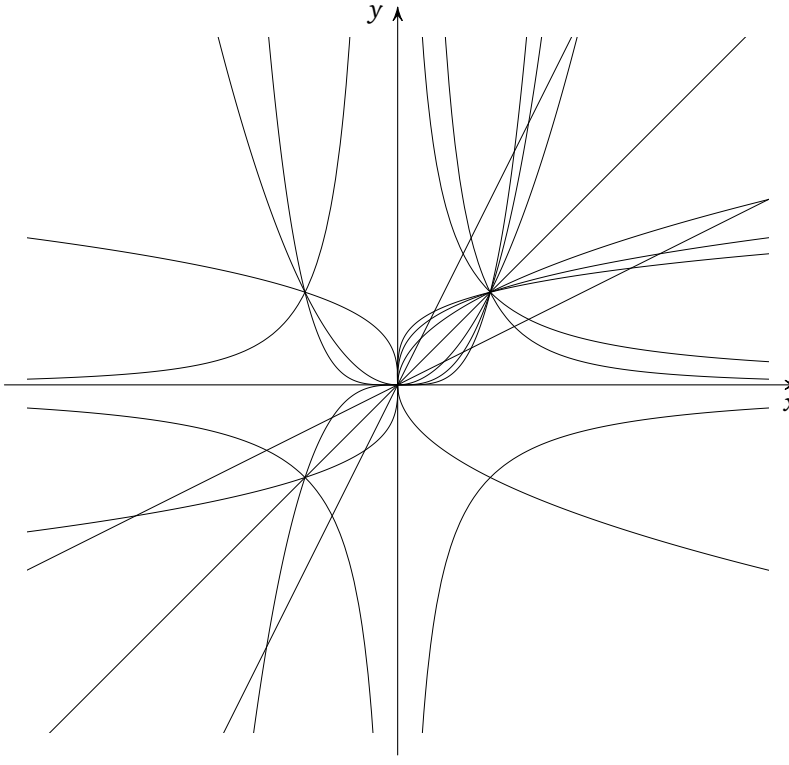
б) Верно ли, что $\operatorname{sign} xy = \operatorname{sign} x \cdot \operatorname{sign} y$, $[xy] = [x][y]$, $\{xy\} = \{x\}\{y\}$?

в) Верно ли, что $\operatorname{sign}(x+y) = \operatorname{sign} x + \operatorname{sign} y$, $[x+y] = [x] + [y]$, $\{x+y\} = \{x\} + \{y\}$?

г) Докажите, что $x = |x| \cdot \operatorname{sign} x$, $x = [x] + \{x\}$.

Задача 3. Постройте графики функций $2x+3$, x^2, $1/x$, $[x]$, $\{x\}$, $\operatorname{sign} x$, $\frac{|x|}{x}$, $|x|$.

Задача 4. На рисунке обведите разными цветами графики функций $x/2$, x, $2x$, x^2, x^3, x^4, x^6, $\sqrt{x}$, $\sqrt[3]{x}$, $\sqrt[4]{x}$, $1/x$, $1/x^2$.

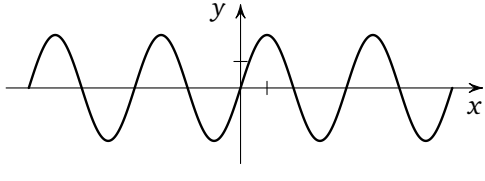


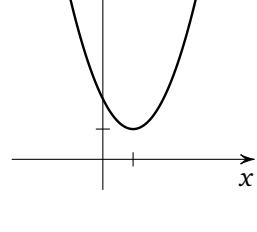
Задача 5. Для указанных преподавателем функций f и g нарисуйте графики функций $f(x)+g(x)$, $f(x)\cdot g(x)$, $f(x)-g(x)$, $\sqrt{f(x)}$, $\frac{1}{f(x)}$.

Задача 6. Нарисуйте графики функций

$f(|x|)$, $|f(x)|$, $f(x+1)$, $f(x-1)$, $f(x)+1$, $f(x)-1$, $f(2x)$, $3f(x)$, $f(x/3)$, $-f(x)$, $f(-x)$, $f([x])$, $f(\{x\})$, $[f(x)]$,

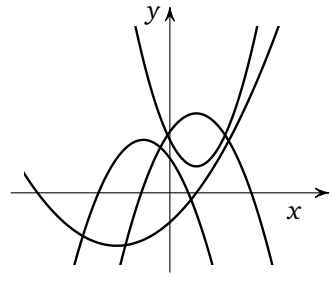
если график функции f изображен на рисунке.



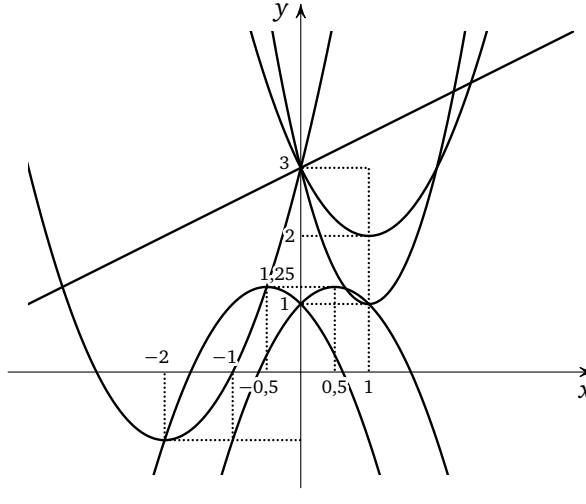


Задача 7. Нарисуйте графики функций:
а) x^2+2x+3; б) $-2x^2+3x-1$; в) $x^2-2|x|+1$.

Задача 8. На рисунке изображены графики квадратичных функций вида $y=ax^2+bx+c$. Найдите sign a, sign b и sign c для каждой из этих функций.



Задача 9. На рисунке изображены графики функций x^2-2x+3, $2x^2-4x+3$, x^2+4x+3, $-x^2+x+1$, $x/2+3$. Определите, какой функции соответствует каждый из графиков.



Задача 10. На координатной плоскости изобразите множество точек (p,q), для которых уравнение $x^2+px+q=0$: а) не имеет корней; б) имеет ровно один корень; в) имеет два корня.

Задача 11*. По изображенному преподавателем графику движения автобуса нарисуйте график скорости этого автобуса.

Теория групп 2. Гомоморфизмы

листок 4д / май 2005

1. гомоморфизмы

Определение 1. Отображение $f\colon G\to H$ группы $(G,*)$ в группу $(H,\circ)$ называется *гомоморфизмом*, если для любых $a,b\in G$ выполнено равенство $f(a*b)=f(a)\circ f(b)$. Множество всех гомоморфизмов из G в H обозначается $\mathrm{Hom}(G,H)$.

Биективный гомоморфизм называется *изоморфизмом*. Изоморфизм на себя называется *автоморфизмом*. Множество всех автоморфизмов группы G обозначается $\mathrm{Aut}(G)$.

Группы G и H называются *изоморфными*, если между ними существует изоморфизм. Обозначение: $G\cong H$. Неформально говоря, изоморфными называются группы, отличающиеся «переобозначением элементов».

Задача 1. Докажите, что отношение «$G\cong H$» является отношением эквивалентности (формально говоря, это верно на любом множестве групп, но множества всех групп не существует).

Задача 2. Какие из следующих отображений являются гомоморфизмами? А какие — изоморфизмами?

а) Тождественное отображение произвольной группы;
б) отображение произвольной группы в единицу;
в) $f\colon\mathbb{Z}\to\mathbb{Z}$, $f(n)=2n$; г) $f\colon\mathbb{Z}\to\mathbb{Z}$, $f(n)=n+1$;
д) $f\colon\mathbb{Z}\to\mathbb{Z}$, $f(n)=n^2$; е) $f\colon\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$, $f(n)=-n$;
ж) $f\colon(\mathbb{Z}/p\mathbb{Z})^\times\to(\mathbb{Z}/p\mathbb{Z})^\times$, $f(n)=n^{-1}$;
з) $f\colon(\mathbb{Z}/p\mathbb{Z})^\times\to(\mathbb{Z}/p\mathbb{Z})^\times$, $f(n)=n^{10}$;
и) $f\colon S_n\to S_n$, $f(x)=ax$; к) $f\colon S_n\to S_n$, $f(x)=x^{-1}$;
л) $f\colon S_n\to S_n$, $f(x)=axa^{-1}$; м) $\mathrm{sign}\colon S_n\to\mathbb{Z}/2\mathbb{Z}$.

Задача 3. Докажите, что для любого гомоморфизма $f\colon G\to H$

а) $f(e_G)=e_H$; б) $f(x^{-1})=f(x)^{-1}$; в) $f(x^n)=f(x)^n$.

Задача 4. Пусть G — произвольная группа, а H — абелева группа. Введите структуру группы: а) на $\mathrm{Hom}(G,H)$, б) на $\mathrm{Aut}(G)$.

Задача 5. Найдите все гомоморфизмы

а) $f\colon\mathbb{Z}\to\mathbb{Z}$; б) $f\colon\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$; в) $f\colon\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$.

Задача 6. а) Найдите все подгруппы в $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$.

б) Докажите, что любая подгруппа группы $\mathbb{Z}/n\mathbb{Z}$ изоморфна группе вида $\mathbb{Z}/m\mathbb{Z}$.

Задача 7*. Сколько существует гомоморфизмов из группы: а) $\mathbb{Z}$; б) $\mathbb{Z}/p\mathbb{Z}$ в группу G?

Задача 8. Какие из следующих групп изоморфны: $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^\times$, S_2, $\mathbb{Z}/6\mathbb{Z}$, S_3, $(\mathbb{Z}/7\mathbb{Z})^\times$?

Определение 2. Множество $f(G)$ называется *образом* гомоморфизма $f\colon G\to H$. Обозначение: $\operatorname{Im} f$.

Множество $f^{-1}(e_H)$ называется *ядром* гомоморфизма $f\colon G\to H$. Обозначение: $\operatorname{Ker} f$.

Задача 9. Найдите ядра и образы всех гомоморфизмов задачи 2.

Задача 10. Докажите, что $\operatorname{Im} f$ и $\operatorname{Ker} f$ — подгруппы в H и G соответственно.

Задача 11. Докажите, что гомоморфизм $f\colon G\to H$ является изоморфизмом тогда и только тогда, когда $\operatorname{Im} f = H$, $\operatorname{Ker} f = \{e_G\}$.

Задача 12. Придумайте гомоморфизм из группы $\mathbb{Z}$, ядром которого является подгруппа четных чисел.

2. смежные классы

Задача 13. Существует ли гомоморфизм из группы S_3, ядром которого является подгруппа $\{e, (12)\}$?

Задача 14. Докажите, что для любого $a\in G$ и любого гомоморфизма $f\colon G\to H$ выполнено равенство $a(\operatorname{Ker} f) = (\operatorname{Ker} f)a$.

Задача 15. а) Докажите, что школьное правило

$$\text{четное}+\text{четное} = \text{нечетное}+\text{нечетное} = \text{четное},$$
$$\text{четное}+\text{нечетное} = \text{нечетное}+\text{четное} = \text{нечетное}$$

задает структуру группы на множестве $\{\{2n \mid n\in\mathbb{Z}\}, \{2n+1 \mid n\in\mathbb{Z}\}\}$.

б) Докажите, что аналогичное правило задает структуру группы на множестве $\{A_n, S_n\backslash A_n\}$.

Определение 3. Напомним, что левым *смежным классом* элемента g группы G относительно подгруппы H называется множество gH. Множество всех левых смежных классов обозначают G/H.

Множество правых смежных классов группы G относительно подгруппы H (множеств вида Hg) обозначают $H\backslash G$. (Не следует путать фактор с разностью множеств.)

Определение 4. Подгруппа H группы G называется *нормальной*, если для любого элемента $a \in G$ выполнено $aH = Ha$ (или, что то же самое, $aHa^{-1} = H$). Обозначение: $H \triangleleft G$).

Задача 16. Докажите, что любая подгруппа коммутативной группы нормальна.

Задача 17. Какие из подгрупп задачи 12 листка «Теория групп 1» нормальны?

Задача 18. Докажите, что подгруппа H группы G нормальна тогда и только тогда, когда разбиение группы G на левые смежные классы относительно группы H совпадает с разбиением на правые смежные классы.

Задача 19. Перечислите все нормальные подгруппы группы S_3.

Задача 20. Докажите, что любая подгруппа H группы G, для которой $2|H| = |G|$, нормальна.

Задача 21. Назовем произведением левых смежных классов aH и bH класс $(ab)H$.

а) Докажите, что это определение корректно тогда и только тогда, когда подгруппа H нормальна.

б) Докажите, что в этом случае множество левых смежных классов образует группу относительно введенной операции.

Определение 5. Пусть H — нормальная подгруппа группы G. Группа, построенная в предыдущей задаче, называется *факторгруппой* (группы G по подгруппе H). Обозначение: G/H.

Задача 22. Докажите, что для любого гомоморфизма $f\colon G \to H$ выполнено $\operatorname{Im} f \cong G/\operatorname{Ker} f$ (в частности, $\operatorname{Ker} f$ — нормальная подгруппа G).

3. действия

Определение 6. Гомоморфизм f группы G в группу преобразований множества A (т. е. биективных отображений множества A в себя) называется *действием* группы G на этом множестве. (Таким образом f ставит в соответствие каждому элементу g группы G некоторую биекцию множества A в себя.) Если понятно, о каком действии идет речь, элемент $f(g)(a)$ обозначается ga.

Задача 23. Какие из следующих отображений являются действиями группы на себе?

а) $f(g)(x) = gx$ (*левый сдвиг*);
б) $f(g)(x) = g^{-1}x$;
в) $f(g)(x) = xg$ (*правый сдвиг*);
г) $f(g)(x) = xg^{-1}$;
д) $f(g)(x) = gxg^{-1}$ (действие сопряжениями).

Задача 24 (теорема Кэли). Докажите, что любая конечная группа изоморфна некоторой подгруппе группы S_n.

Задача 25. Перечислите все действия:
а) группы $\mathbb{Z}$ на множестве из двух элементов (одного элемента);
б) группы $\mathbb{Z}/n\mathbb{Z}$ на множестве из двух элементов (одного элемента);
в) группы $\mathbb{Z}/n\mathbb{Z}$ на множестве из трех элементов;
г) группы $\mathbb{Z}/2\mathbb{Z}$ на группе $\mathbb{Z}$ (на группе $\mathbb{Z}/4\mathbb{Z}$), такие что каждое преобразование $f(g)$ является изоморфизмом;
д) группы $\mathbb{Z}/n\mathbb{Z}$ на множестве вершин квадрата, такие что каждое преобразование $f(g)$ является поворотом.

Определение 7. Множество $Ga = \{ga \mid g \in G\}$ называется *орбитой* точки $a \in A$.

Определение 8. Орбиты действия сопряжениями называются *классами сопряженных элементов*.

Задача 26. Докажите, что отношение «точка a принадлежит орбите точки b» является отношением эквивалентности.

Задача 27. а) Опишите орбиты для действий из задачи 25.
б) Опишите орбиты действия левыми сдвигами.
в) Найдите классы сопряженных элементов в S_3 и A_3.
г) Найдите классы сопряженных элементов в S_n.
д*) Найдите классы сопряженных элементов в A_n.

Определение 9. Множество $\operatorname{stab} a = \{g \in G \mid ga = a\}$ (другое обозначение: G_a) называется *стабилизатором* точки $a \in A$.

Задача 28. Укажите стабилизаторы для действий из предыдущих задач.

Задача 29. Докажите, что $|G_x| \cdot |Gx| = |G|$.

Задача 30. Докажите, что в группе из p^2 элементов (p — простое число) найдется хотя бы два класса сопряженных элементов из одного элемента.

Определение 10. Множество $\operatorname{Fix} g = \{a \in A \mid ga = a\}$ (другое обозначение: A^g) называется *множеством неподвижных точек* элемента g (вообще говоря, это множество зависит от действия, но когда ясно, о каком действии идет речь, наименование действия не указывается).

Задача 31. Укажите множества неподвижных точек всех элементов для действий группы $\mathbb{Z}/4\mathbb{Z}$: а) левыми сдвигами; б) сопряжениями.

Задача 32. Укажите множества неподвижных точек всех элементов для действий группы S_3: а) левыми сдвигами; б) сопряжениями.

Задача 33 (лемма Бернсайда). Группа $|G|$ действует на множестве X. Докажите, что число орбит этого действия равно

$$\frac{1}{|G|} \sum_{g \in G} |\operatorname{Fix} g|.$$

Задача 34. а) Найдите число способов раскрасить n-местную карусель в красный и синий цвета.

б) Найдите число способов раскрасить ожерелье из n бусинок в красный и синий цвета.

Теория множеств 1

листок 1 / сентябрь 2004

Первый листок знакомит с языком теории множеств, на котором далее будет излагаться большинство понятий.

В начале листка фиксируются обозначения для множеств и даются упражнения, призванные научить различать подмножество и элемент множества. Вторая часть листка призвана задать стандарт вполне формального доказательства; естественно, для первых упражнений в формальных доказательствах выбраны содержательно очень простые вопросы теории множеств.

Мы считаем, что сводить математику к аксиоматической теории (тем более в школе) нельзя, однако понимание определённых «правил игры», принятых в математике, необходимо. Поэтому мы учим школьников «наивной теории множеств» — учим работать с множествами, чувствовать тонкости и возможные проблемы, но не вводим формальных аксиом.

> Множество — одно из основных неопределяемых понятий в математике. Задать множество — значит определить, из каких элементов оно состоит. Один из способов задать множество — просто перечислить в фигурных скобках его элементы.
>
> «Элемент x принадлежит множеству M» записывают как «$x \in M$», «элемент x не принадлежит множеству M» записывают как «$x \notin M$».

Важно объяснить школьнику, что множество — это понятие, которое формально не определяется (наоборот, остальные математические понятия обычно определяются через множества). Тем не менее, мы можем с ним работать, считая, что все понимают, о чем идет речь. Привыкнув выполнять операции с множествами, ученики почувствуют, что это такое.

> **Задача 1.** Сколько элементов в множестве:
> а) {1}, {1, 2, 3}, {Вася}; б) {{1}}; в) {1, {2, 3}};
> г) букв слова «крокодил»; д) {{1}, 1};
> е) имен учеников вашего класса?

Решение. а) Один элемент: «1»; три элемента: «1», «2» и «3»; один элемент: «Вася».

б) Один элемент: множество {1}.

В этом месте можно спросить у школьника, поменяется ли ответ, если заменить 1 на 2 или, например, на {1, 2}.

в) Два элемента: число 1 и множество {2, 3}.

г) Шесть элементов: «к», «р», «о», «д», «и», «л».

д) Два элемента: множество {1} и число 1.

Важно понимать, что каждый элемент (например, буква «о») может либо принадлежать, либо не принадлежать множеству, а принадлежать, скажем, два раза не может. Поэтому, зная множество букв слова, можно сказать, какие буквы необходимы, чтобы его составить, но нельзя сказать ни в каком порядке они идут, ни даже сколько раз какие буквы используются.

В этом месте полезно попросить привести пример двух различных (и даже имеющих разную длину) русских слов, множества букв которых совпадают.

Определение 1. Множества A и B называются *равными*, если каждый элемент множества A принадлежит множеству B, а каждый элемент множества B принадлежит множеству A. Обозначение: $A = B$.

Определение 2. Множество A называется *подмножеством* множества B, если каждый элемент множества A принадлежит множеству B. Обозначение: $A \subset B$. Один из способов задать подмножество — задать свойство, которым обладают все его элементы: $\{x \in A \mid x$ обладает свойством …$\}$.

В этом определении и в следующей задаче мы показываем, как использовать важный способ задания множества, как «множества элементов, удовлетворяющих данному свойству».

Отметим, что его следует использовать только для выделения подмножества из уже имеющегося множества. Неограниченное использование аксиомы выделения приводит к парадоксам. Например, так можно построить «множество всех множеств, не содержащих себя в качестве элемента»: $A = \{x \notin x\}$. Заметим, что, с одной стороны, $A \in A$, а с другой, $A \notin A$. Этот вариант «парадокса брадобрея» подробно рассмотрен позже. В этом месте преждевременно заострять на этом внимание, но приучать школьников правильно пользоваться аксиомой выделения надо.

Задача 2. а) Пусть A — множество однозначных натуральных чисел. Запишите указанным в определении 2 способом его подмножество $\{2, 4, 6, 8\}$.

б) Пусть A — множество городов России. Перечислите элементы его подмножества $\{x \in A \mid$ число жителей города x на 1 января 2003 года более 1 000 000 человек$\}$.

Решение. а) Один из способов записи: $\{2, 4, 6, 8\} = \{x \in A \mid x$ чётно$\}$. Есть и другие способы.

б) Города, упомянутые в условии, — это города-миллионеры (их можно найти в атласе или в учебнике географии).

> **Задача 3.** Для каждых двух из следующих множеств указать, является ли одно из них подмножеством другого: $\{1\}$, $\{1, 2\}$, $\{1, 2, 3\}$, $\{\{1\}, 2, 3\}$, $\{\{1, 2\}, 3\}$, $\{3, 2, 1\}$, $\{\{2, 1\}\}$.

Указание. Взяв два множества, аккуратно проверьте, из каких элементов они состоят.

В этой задаче важно понимать, что требуется про *каждую* пару множеств (в том числе совпадающих) ответить на вопрос, является ли одно из них подмножеством другого.

Решение. Для решения задачи нужно для каждой пары множеств (возможно, совпадающих) выяснить, является ли одно из них подмножеством другого. Кроме того, что каждое множество является подмножеством себя, мы получим, что первое множество является подмножеством второго, третьего и шестого; второе — подмножеством третьего и шестого; третье равно шестому (а потому каждое из них является подмножеством другого); четвёртое не является ничьим подмножеством, как и пятое, а седьмое — подмножество пятого.

Отметим, что множество $\{1\}$ является элементом множества $\{\{1\}, 2, 3\}$, но не является его подмножеством, а множество $\{1, 2\}$ является элементом множества $\{\{2, 1\}\}$ и является подмножеством множества $\{1, 2, 3\}$.

> **Задача 4.** Докажите, что множество A тогда и только тогда является подмножеством множества B, когда каждый элемент, не принадлежащий B, не принадлежит A.

Решение. Оборот «тогда и только тогда» означает *два* утверждения:

1) $(A \subset B) \Rightarrow$ (для любого x, не принадлежащего B, x не принадлежит A),

2) (для любого x, не принадлежащего B, x не принадлежит A) $\Rightarrow$ $\Rightarrow (A \subset B)$.

Продемонстрируем на примере этой задачи, как применяется метод доказательства «от противного». Чтобы доказать некоторое утверждение, мы предполагаем, что оно не выполняется и приходим к противоречию[15].

[15]Бывают математические теории, в которых принцип исключённого третьего отсутствует, и любое утверждение требуется доказывать «напрямую». С принципом исключенного третьего тесно связаны вопросы непротиворечивости математики в целом.

1) Докажем первое утверждение. Предположим противное, то есть что $A \subset B$, но существует некоторый элемент x, не принадлежащий B, но принадлежащий A. По определению того, что $A \subset B$ мы знаем, что каждый элемент, принадлежащий A, должен принадлежать B. В частности, $x \in B$. *Возникает противоречие. Значит, наше предположение было неверно, и нет элементов принадлежащих A, но не принадлежащих B.*

2) Теперь перейдём к доказательству второй части утверждения, которое мы тоже проведём от противного. Пусть каждый элемент, не принадлежащий B, не принадлежит A, но $A \not\subset B$. То, что $A \not\subset B$, означает, что для множеств A и B не выполняется условие определения 2. То есть существует некоторый элемент x, принадлежащий A, но не принадлежащий B. *Опять получили противоречие. Значит, и второе наше предположение было неверно.*

Эта внешне несложная задача является одновременно очень важной и достаточно сложной для школьников. Как и в некоторых других задачах этого листка, школьникам неясно, что, собственно, надо доказывать. Мы одновременно демонстрируем метод от противного, учимся писать отрицание к следствию и разбираемся, что значит «тогда и только тогда».

Задача 5. Докажите, что для произвольных множеств A, B и C:
а) $A \subset A$; б) $A \subset B$ и $B \subset C \Rightarrow A \subset C$; в) $A = B \Leftrightarrow A \subset B$ и $B \subset A$.

Решение. а) Применяем определение: каждый элемент x, принадлежащий множеству A, принадлежит множеству A, значит, $A \subset A$.

б) Требуется доказать, что каждый элемент из множества A будет принадлежать множеству C. Возьмём произвольный элемент $x \in A$. Так как $A \subset B$, $x \in B$. Так как $B \subset C$, $x \in C$. Таким образом, мы доказали, что произвольный элемент множества A принадлежит множеству C.

в) Этот пункт содержит в себе *две* задачи. Надо доказать, во-первых, что из $A \subset B$ и $B \subset A$ следует, что $A = B$, а во-вторых, что из $A = B$ следует, что $A \subset B$ и $B \subset A$.

Докажем первое утверждение. Если $A \subset B$, то каждый элемент множества A принадлежит B, а из $B \subset A$ следует, что каждый элемент множества B принадлежит A. Значит, по определению равенства множеств, $A = B$.

Теперь докажем второе утверждение. Действительно, если $A = B$, то, по определению, каждый элемент множества A принадлежит также B, и каждый элемент множества B принадлежит A. Но это и означает, что $A \subset B$ и $B \subset A$.

В этой задаче возникает важный метод доказательства того, что некоторое утверждение верно для всех x, удовлетворяющих некоторому условию. А именно, зафиксировав произвольный x, удовлетворяющий условию, провести рассуждения для «этого конкретного» x.

Определение 3. Множество называется *пустым*, если оно не содержит ни одного элемента. Обозначение: $\varnothing$.

Задача 6. а) Докажите, что пустое множество является подмножеством любого множества.

б) Докажите, что пустое множество единственно.

Здесь впервые приходится доказывать единственность объекта, обладающего некоторыми свойствами. Для этого нужно рассмотреть два таких объекта и доказать, что они равны между собой. В данном случае удобнее всего провести доказательство «от противного».

Решение. а) Пусть имеется некоторое множество A, подмножеством которого пустое множество *не* является. Это означает, что есть некоторый элемент x, который принадлежит пустому множеству, но не принадлежит множеству A. Но такого элемента быть не может, так как в пустом множестве вообще нет элементов. Получили противоречие. Значит, пустое множество является подмножеством любого множества.

б) Убедимся в том, что любые два пустых множества равны между собой. Предположим, что у нас имеется два пустых множества: первое и второе. Но по предыдущему пункту каждое из них является подмножеством другого. А значит, по определению 1 они равны.

Задача 7. Сколько элементов у каждого из следующих множеств: $\varnothing$, $\{1\}$, $\{1, 2\}$, $\{1, 2, 3\}$, $\{\{1\}, 2, 3\}$, $\{\{1, 2\}, 3\}$, $\{\varnothing\}$, $\{\{2, 1\}\}$?

Указание. Обратите особое внимание на множества с шестого по восьмое.

Ответ. 0, 1, 2, 3, 3, 2, 1, 1.

Задача 8. а) Для множеств из предыдущей задачи выпишите все их подмножества.

б) Сколько подмножеств у множества из одного элемента? из двух элементов? трех элементов?

Главное, что здесь нужно понимать — что число подмножеств зависит только от числа элементов (и не зависит от их природы). Точная формула для числа подмножеств появляется позднее, хотя можно ее вывести и сейчас.

Ответ. а) $\varnothing$: $\varnothing$; {1}: $\varnothing$ и {1}; {1, 2}: $\varnothing$, {1}, {2}, {1, 2};
{1, 2, 3}: $\varnothing$, {1}, {2}, {3}, {1, 2}, {1, 3}, {2, 3}, {1, 2, 3};
{{1}, 2, 3}: $\varnothing$, {{1}}, {2}, {3}, {{1}, 2}, {{1}, 3}, {2, 3}, {{1}, 2, 3};
{{1, 2}, 3}: $\varnothing$, {{1, 2}}, {3}, {{1, 2}, 3};
{$\varnothing$}: $\varnothing$ и {$\varnothing$}; {{2, 1}}: $\varnothing$ и {{2, 1}};
б) 2; 4; 8.

Задача 9. Верно ли, что множество летающих крокодилов является подмножеством множества учеников 8 «В» класса 57-й школы? Верно ли, что множество учеников 8 «В» класса 57-й школы является подмножеством множества классов 57-й школы?

Указание. Перво-наперво следует задаться вопросом: какие элементы содержатся во множестве летающих крокодилов? А после понять, не принадлежат ли все элементы этого множества множеству учеников 8 «В» класса 57-й школы.

При ответе на второй вопрос надо обратить внимание на элементы обоих множеств. Какие объекты являются элементами первого множества, а какие — второго?

Решение. Поскольку множество летающих крокодилов пусто, оно является подмножеством множества учеников 8 «В» класса 57-й школы. Если множество учеников 8 «В» класса 57-й школы непусто, то оно не является подмножеством множества классов 57-й школы, поскольку ни один ученик 8 «В» класса не является классом 57-й школы. (Подчеркнём ещё раз разницу между учениками и классом — даже если класс состоит ровно из одного ученика, этот ученик не совпадает со своим классом.)

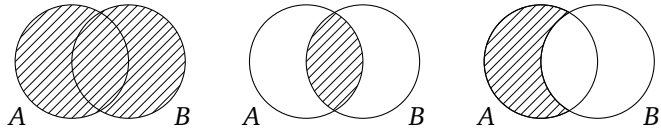
Задача 10. Может ли у множества быть ровно: а) 0; б) 7; в) 16 подмножеств?

Набросок решения. Во-первых, заметим, что число подмножеств множества пустого множества равно 1, число подмножеств множества, состоящего из одного элемента, равно 2, из двух — 4, из трех — 8, из четырех — 16. Второе важное наблюдение — монотонность: если у одного множества больше элементов, чем у другого, то и подмножеств у него больше.

Определение 4. *Объединением* множеств A и B называется множество, состоящее из всех таких x, что $x \in A$ или $x \in B$. Обозначение: $A \cup B$.

Пересечением множеств A и B называется множество, состоящее из всех таких x, что $x \in A$ и $x \in B$. Обозначение: $A \cap B$.

Разностью множеств A и B называется множество, состоящее из всех таких x, что $x \in A$ и $x \notin B$. Обозначение: $A \setminus B$.



Операция $\cap$ соответствует логическому И, а $\cup$ — логическому ИЛИ.

Задача 11. Пусть даны множества $A = \{1, 3, 7, 137\}$, $B = \{3, 7, 23\}$, $C = \{0, 1, 3, 23\}$, $D = \{0, 7, 23, 2004\}$. Найдите множества:
а) $A \cup B$; б) $A \cap B$; в) $(A \cap B) \cup D$; г) $C \cap (D \cap B)$;
д) $(A \cup B) \cap (C \cup D)$; е) $(A \cup (B \cap C)) \cap D$;
ж) $(C \cap A) \cup ((A \cup (C \cap D)) \cap B)$; з) $(A \cup B) \setminus (C \cap D)$;
и) $A \setminus (B \setminus (C \setminus D))$; к) $((A \setminus (B \cup D)) \setminus C) \cup B$.

Ответ. а) $A \cup B = \{1, 3, 7, 23, 137\}$; б) $A \cap B = \{3, 7\}$;
в) $(A \cap B) \cup D = \{0, 3, 7, 23, 2004\}$; г) $C \cap (D \cap B) = \{23\}$;
д) $(A \cup B) \cap (C \cup D) = \{1, 3, 7, 23\}$; е) $(A \cup (B \cap C)) \cap D = \{7, 23\}$;
ж) $(C \cap A) \cup ((A \cup (C \cap D)) \cap B) = \{1, 3, 7, 23\}$;
з) $(A \cup B) \setminus (C \cap D) = \{1, 3, 7, 137\}$;
и) $A \setminus (B \setminus (C \setminus D)) = \{1, 3, 137\}$;
к) $((A \setminus (B \cup D)) \setminus C) \cup B = \{3, 7, 23, 137\}$.

При решении этой задачи полезно рисовать картинки, а также проговаривать вслух, что происходит с каждым элементом.

Задача 12. Пусть A — множество четных чисел, а B — множество чисел, делящихся на три. Найдите $A \cap B$.

Решение. Это множество чисел, делящихся на 6, так как любое число, которое делится на 6, будет делиться также на 2 и на 3. И наоборот: любое число, делящееся на 2 и на 3, будет делиться также и на 6.

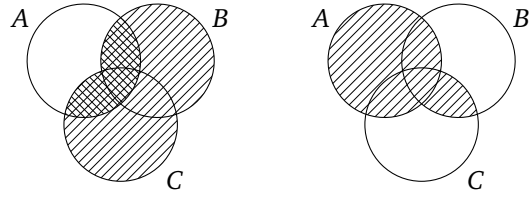
Задача 13. Докажите, что для любых множеств A, B, C:
а) $A \cup B = B \cup A$, $A \cap B = B \cap A$;
б) $A \cup (B \cup C) = (A \cup B) \cup C$, $A \cap (B \cap C) = (A \cap B) \cap C$;
в) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
г) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$, $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

Указание. Чтобы доказать, что одно множество равно другому, нужно воспользоваться определением равенства множеств и показать, что любой элемент первого лежит во втором и любой элемент второго множества лежит в первом.

Во всех пунктах проверка не очень сложна. Надо лишь аккуратно записать, что означает, что x принадлежит левому множеству, и

что означает, что x принадлежит правому множеству. Очень полезно предварительно нарисовать картинки, изобразив разные множества цветами или штриховкой. Такие картинки называют *диаграммами Эйлера—Венна* или *кругами Эйлера*.

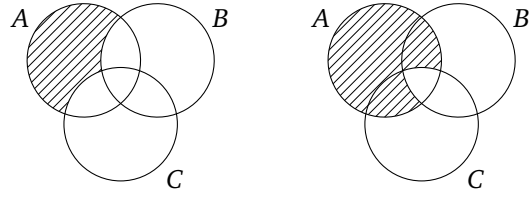
Решение. Разберем для примера доказательства пунктов в) и г).



в) $x \in A \cap (B \cup C)$ означает, что x принадлежит множеству A и по крайней мере одному из множеств B и C. Пусть, для определенности, $x \in C$ (случай $x \in B$ аналогичен). Тогда $x \in A$ и $x \in C$, а значит, $x \in A \cap C$, откуда $x \in (A \cap B) \cup (A \cap C)$.

Если же $x \in (A \cap B) \cup (A \cap C)$, то это означает, что x принадлежит по крайней мере одному из множеств $(A \cap B)$ или $(A \cap C)$. Пусть, для определенности, $x \in (A \cap B)$. Это означает, что $x \in A$ и $x \in B$, следовательно, $x \in A$ и $x \in B \cup C$, откуда $x \in A \cap (B \cup C)$.

Второе равенство доказывается аналогично.



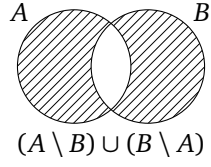
г) $x \in A \setminus (B \cup C)$ означает, что x принадлежит множеству A, но не принадлежит объединению множеств B и C. Поскольку элемент x принадлежит множеству A, но не принадлежит B, элемент x принадлежит множеству $A \setminus B$. Аналогично, $x \in A \setminus C$. Следовательно, $x \in (A \setminus B) \cap (A \setminus C)$.

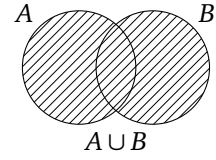
Пусть, наоборот, $x \in (A \setminus B) \cap (A \setminus C)$. Это означает, что x одновременно принадлежит множествам $A \setminus B$ и $A \setminus C$. Следовательно, $x \in A$ и элемент x не принадлежит ни одному из множеств B и C, то есть $x \in A \setminus (B \cup C)$.

Второе равенство доказывается аналогично.

Задача 14. Верно ли, что для любых множеств A, B, C:
а) $A\cap\varnothing=\varnothing$; $A\cup\varnothing=A$; б) $A\cup A=A$; $A\cap A=A$;
в) $A\cap B=A \Leftrightarrow A\subset B$; г) $(A\setminus B)\cup B=A$; д) $A\setminus(A\setminus B)=A\cap B$;
е) $A\setminus(B\setminus C)=(A\setminus B)\cup(A\cap C)$; ж) $(A\setminus B)\cup(B\setminus A)=A\cup B$?

Решение. Объясним на примере пункта ж), как можно решать такие задачи. Сначала надо понять, следует ли доказывать равенство или опровергать его. Для этого нарисуем диаграмму:





Из рисунка видно, что утверждение скорее всего неверно и нужно искать контрпример. Опять-таки, по диаграмме видно, что любой элемент пересечения $A\cap B$ содержится в правом множестве, но не содержится в левом. Поэтому в качестве примера можно взять любые два пересекающихся множества (например, $A=B=\{1\}$).

Формальным решением является доказательство в стиле предыдущей задачи, если равенство истинно, и контрпример, если равенство ложно (кругов Эйлера недостаточно).

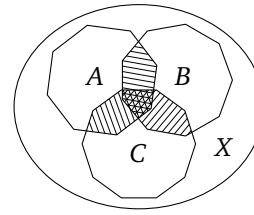
Ответ. Утверждения пунктов а), б), в), д), и е) верны и доказываются аналогично тому, как доказываются утверждения предыдущей задачи. Утверждения пунктов г) и ж) неверны.

Задача 15. а) Внутри фигуры площади 6 расположено три многоугольника площадью не менее 3 каждый. Докажите, что существует два многоугольника, площадь пересечения которых не менее 1.

б*) Внутри фигуры площади 4 расположено 7 многоугольников площадью не менее 1 каждый. Докажите, что существует два многоугольника, площадь пересечения которых не менее 1/7.

Решение. а) Будем доказывать методом от противного. Пусть площадь пересечения любых двух многоугольников менее 1. Обозначим многоугольники буквами A, B и C, а фигуру, внутри которой они находятся, — за X. Кроме того, за $S(P)$ будем обозначать площадь соответствующей фигуры P. Тогда $S(A)+S(B)+S(C)\geqslant 9$. А так как $S(A\cap B)<1$, $S(A\cap C)<1$ и $S(C\cap B)<1$, то

$$S(A)+S(B)+S(C)-S(A\cap B)-S(A\cap C)-S(C\cap B)>6.$$



Из диаграммы видно, что

$$S(A\cup B\cup C)\overset{!}{=}S(A)+S(B)+S(C)-$$
$$-S(A\cap B)-S(A\cap C)-S(B\cap C)+S(A\cap B\cap C).$$

Следовательно, $6<S(A)+S(B)+S(C)-S(A\cap B)-S(A\cap C)-S(C\cap B)=$ $=S(A\cup B\cup C)-S(A\cap B\cap C)\leqslant S(A\cup B\cup C)$. Поскольку все многоугольники расположены внутри фигуры X, $S(A\cup B\cup C)\leqslant S(X)=6$. Возникает противоречие. Значит, существует два многоугольника, площадь пересечения которых не менее 1.

Равенство, отмеченное знаком !, — это ключевой момент доказательства, в котором обязательно надо разобраться.

б) Обозначим многоугольники буквами A_1, …, A_7, а содержащую их фигуру — за X.

Если бы множества не пересекались, площадь их объединения была бы равна $S(A_1)+\ldots+S(A_7)\geqslant 7$. Таким образом, за счёт пересечений площадь объединения данных многоугольников уменьшается хотя бы на 3. Посмотрим теперь, каков смысл суммы $S(A_1)+\ldots+S(A_7)$ для пересекающихся многоугольников A_1, …, A_7. Заметим, что в этой сумме площадь каждой части объединения посчитана столько раз, в скольки многоугольниках она содержится. В частности, попарные пересечения исходных многоугольников посчитаны как минимум по два раза. Вычтем теперь из суммы $S(A_1)+\ldots+S(A_7)$ сумму площадей попарных пересечений. Заметим, что теперь площадь каждой части объединения посчитана не более одного раза (проверьте!). Следовательно, полученная разность не превосходит 4. Но она получена вычитанием из суммы $S(A_1)+\ldots+S(A_7)$ (которая не меньше 7) 21 слагаемого. Следовательно, одно из вычитаемых слагаемых не менее $3/21=1/7$, что и требовалось доказать.

Продолжая рассуждения, можно доказать следующую *формулу включений-исключений*.

Площадь объединения n многоугольников равна сумме площадей минус сумма попарных пересечений плюс сумма площадей тройных

пересечений и т. д.:

$$S(A_1 \cup \ldots \cup A_n) = S(A_1) + \ldots + S(A_n) - \sum_{1 \leqslant i_1 < i_2 \leqslant n} S(A_{i_1} \cap A_{i_2}) +$$

$$+ \sum_{1 \leqslant i_1 < i_2 < i_3 \leqslant n} S(A_{i_1} \cap A_{i_2} \cap A_{i_3}) + \ldots + (-1)^k \sum_{1 \leqslant i_1 < \ldots < i_k \leqslant n} S(A_{i_1} \cap \ldots \cap A_{i_k}),$$

причём, если отбросить слагаемые, начиная со слагаемого, идущего со знаком «+», получится оценка на площадь снизу, а если со знаком «−», то сверху.

Задача 16*. а) Можно ли записать пересечение двух множеств, используя только разность и объединение?

б) Можно ли записать разность двух множеств, используя только объединение и пересечение?

Решение. а) Читателю предлагается проверить следующую формулу: $A \cap B = (A \cup B) \setminus ((A \setminus B) \cup (B \setminus A))$.

б) Нет. Дело в том, что кроме множеств A, B, $A \cap B$ и $A \cup B$ при помощи наших операций ничего получить нельзя. Для доказательства этого факта достаточно проверить, что в результате применения операций $\cap$ и $\cup$ к произвольной паре этих множеств никаких новых множеств мы не получим.

Другой способ решить задачу — заметить, что при помощи операций объединения и пересечения из множеств A и B можно получить лишь множества, содержащие $A \cap B$.

Теория множеств 2. Отображения множеств

листок 2 / сентябрь 2004

В этом листке вводится понятие отображения. В задачах это понятие обсуждается на простых примерах, в которых его можно «потрогать руками».

Отображение (функция, морфизм… — имеется очень много сходных по смыслу терминов) — одно из фундаментальных понятий математики. При помощи отображений можно не только изучать внутренние свойства объектов, но и сравнивать их, изучать связи между объектами. Впоследствии возникнут отображения, сохраняющие те или иные свойства множеств.

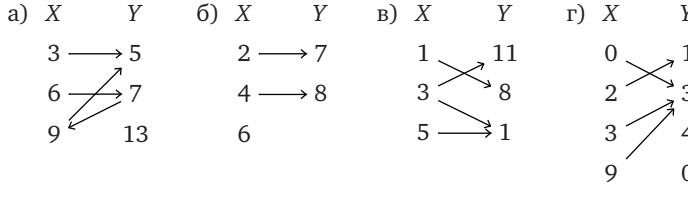
Как и в предыдущем листке, большинство задач здесь представляют собой скорее упражнения для изучения некоторого языка, чем содержательные математические факты. Отметим, однако, задачу 10, хотя и несложную, но исключительно полезную, и задачу 11, в которой впервые возникают нетривиальные эффекты, связанные с бесконечными множествами.

> **Определение 1.** Если каждому элементу x множества X поставлен в соответствие ровно один элемент $f(x)$ множества Y, то говорят, что задано *отображение* f из множества X в множество Y. При этом, если $f(x) = y$, то элемент y называется *образом* элемента x при отображении f, а элемент x называется *прообразом* элемента y при отображении f. Обозначение: $f\colon X \to Y$.

Надо понимать, что это не является формальным определением, потому что, когда мы определяем отображение, мы говорим, что одному элементу «ставится в соответствие» другой. А что такое «поставить в соответствие»? Это как раз и значит отобразить! Получается, что наше «определение» — просто замена одних слов другими.

Формальное определение отображения (в отличии от множества) можно дать (например, определив отображение как множество упорядоченных пар, удовлетворяющее некоторым условиям), однако пока имеющегося определения вполне достаточно.

Задача 1. Какие из следующих картинок задают отображения?



Решение. а) В этом пункте имеется (как и в некоторых других) тонкое место. Картинка, которая здесь предлагается для рассмотрения, действительно *задает* отображение (определение 1 выполняется — мы можем сказать, какой элемент куда переходит), но эта картинка *не является диаграммой отображения*, потому что имеется одна «лишняя» стрелка — из 7 в 9.

б) Диаграмма в этом пункте не задает отображения из X в Y, так как не указано, куда переходит 6. Однако диаграмма задает отображение подмножества множества X в Y.

в) В этом пункте диаграмма также не является диаграммой отображения, потому что элементу 3 множества X поставлено в соответствие целых *два* элемента множества Y.

г) Здесь картинка задает отображение.

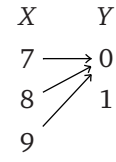
> **Задача 2.** Нарисуйте все возможные отображения из множества $\{7, 8, 9\}$ в множество $\{0, 1\}$.

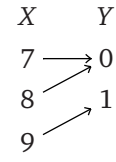
В этом месте следует объяснить школьнику, что когда просят «нарисовать все отображения...» или «перечислить все объекты, которые...», то не стоит перечислять нужные объекты наобум — мы наверняка что-нибудь забудем или назовем несколько раз. Если же придумать некоторое правило перечисления, то можно быть уверенным в том, что перечислено все, что нужно, и ровно по одному разу.

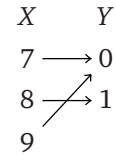
Например, если в задаче просят перечислить все натуральные числа от 1 до 5 включительно, то нелогично перечислять их в таком порядке: 1, 4, 2, 5, 3. При таком перечислении мы не застрахованы от ошибки. А если нужно перечислить сто чисел? Если же мы перечислим их, например, в порядке возрастания, то можно смело утверждать, что перечислены все нужные числа. Ведь в каждый момент в процессе перечисления мы однозначно можем сказать, какое будет следующее число. В процессе обсуждения как раз и всплывет идея о том, что перечислять всегда следует, руководствуясь некоторым правилом. Отметим, что таких правил может быть много (например, в только что разобранной задаче с числами мы могли, скажем, перечислять числа в порядке убывания).

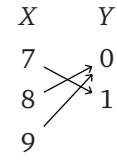
В ответе к задаче 2 отображения расположены в следующем порядке: сначала идет отображение, в котором все элементы переходят в 0, затем те, в которых только два элемента переходят в 0 (а один элемент в 1), затем те, в которых в 0 переходит лишь один элемент, затем отображение, в котором в 0 не переходит ни один элемент. Конечно, в случае, когда нам надо перечислить всего восемь объектов, ошибка маловероятна. Однако учить математической культуре надо как раз

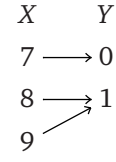
начиная с совсем простых примеров.

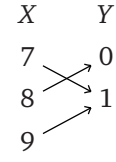
Ответ. 1) 

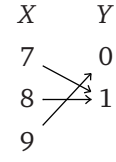
2) 

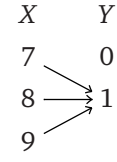
3) 

4) 

5) 

6) 

7) 

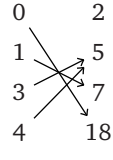
8) 

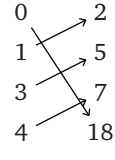
Можно обсудить, почему число отображений в множество $\{0,1\}$ — всегда степень двойки (на самом деле, отображения из множества A в $\{0,1\}$ соответствуют подмножествам множества A), и сколько вообще существует отображений из n-элементного множества в m-элементное (как обычно, полезно начать с разбора разных примеров).

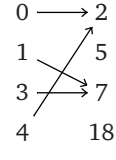
Определение 2. Пусть $f\colon X \to Y$, $y \in Y$, $A \subset X$, $B \subset Y$. *Полным прообразом элемента* y при отображении f называется множество $\{x \in X \mid f(x) = y\}$. Обозначение: $f^{-1}(y)$. *Образом множества* $A \subset X$ при отображении f называется множество $\{f(x) \mid x \in A\}$. Обозначение: $f[A]$. *Прообразом множества* $B \subset Y$ называется множество $\{x \in X \mid f(x) \in B\}$. Обозначение: $f^{-1}[B]$.

Хотя в математических текстах обычно используются только круглые скобки, в этом листочке мы специально используем разные скобки для образа элемента и образа множества, чтобы было проще понять, что происходит. Этот формализм очень важен в начале изучения этих понятий.

Задача 3. Для отображения $f\colon \{0,1,3,4\} \to \{2,5,7,18\}$, заданного картинкой, найдите $f[\{0,3\}]$, $f[\{1,3,4\}]$, $f^{-1}(2)$, $f^{-1}[\{2,5\}]$, $f^{-1}[\{5,18\}]$.

а) 

б) 

в) 

Ответ. а) $f[\{0,3\}] = \{5,18\}$, так как 0 отображается в 18, а 3 — в 5;
$f[\{1,3,4\}] = \{5,7\}$, так как 1 отображается в 7, 3 отображается в 5, 4 тоже отображается в 5;

$f^{-1}(2)=\varnothing$, так как в 2 ничего не отображается;

$f^{-1}[\{2,5\}]=\{3,4\}$, так как в 2 ничего не отображается, а в 5 отображаются элементы 3 и 4;

$f^{-1}[\{5,18\}]=\{0,3,4\}$, так как в 18 отображается 0, а в 5 отображаются 3 и 4.

б) $f[\{0,3\}]=\{5,18\}$, $f[\{1,3,4\}]=\{2,5,7\}$, $f^{-1}(2)=\{1\}$, $f^{-1}[\{2,5\}]=\{1,3\}$, $f^{-1}[\{5,18\}]=\{0,3\}$.

в) $f[\{0,3\}]=\{2,7\}$, $f[\{1,3,4\}]=\{2,7\}$, $f^{-1}(2)=\{0,4\}$, $f^{-1}[\{2,5\}]=\{0,4\}$, $f^{-1}[\{5,18\}]=\varnothing$.

Задача 4. Пусть $f\colon X\to Y$, $A_1, A_2\subset X$, $B_1, B_2\subset Y$. Всегда ли верно, что

а) $f[X]=Y$; б) $f^{-1}[Y]=X$; в) $f[A_1\cup A_2]=f[A_1]\cup f[A_2]$;

г) $f[A_1\cap A_2]=f[A_1]\cap f[A_2]$; д) $f^{-1}[B_1\cup B_2]=f^{-1}[B_1]\cup f^{-1}[B_2]$;

е) $f^{-1}[B_1\cap B_2]=f^{-1}[B_1]\cap f^{-1}[B_2]$; ж) $f[A_1]\subset f[A_2]\Rightarrow A_1\subset A_2$;

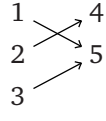
з) $f^{-1}[B_1]\subset f^{-1}[B_2]\Rightarrow B_1\subset B_2$?

Решение. а) Нет. Например, при отображении из пункта а) предыдущей задачи это не так.

б) Да. $f^{-1}[Y]=\{x\in X\mid f(x)\in Y\}$. Так как $f(x)\in Y$ для любого $x\in X$, то $\{x\in X\mid f(x)\in Y\}=X$.

в) Да. $f[A_1\cup A_2]=\{y\in Y\mid \exists x\in A_1\cup A_2\colon f(x)=y\}=\{y\in Y\mid \exists x$ такой, что $x\in A_1$ или $x\in A_2$ и $f(x)=y\}=\{y\in Y\mid \exists x\in A_1\colon f(x)=y\}\cup \cup\{y\in Y\mid \exists x\in A_2\colon f(x)=y\}=f[A_1]\cup f[A_2]$.

г) Нет. Вот пример: X Y $A_1=\{1,2\}$; $A_2=\{2,3\}$.

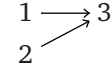


д) Верно. Докажем сначала, что $f^{-1}[B_1\cup B_2]\subset f^{-1}(B_1)\cup f^{-1}(B_2)$. Действительно, для любого $x\in f^{-1}[B_1\cup B_2]$ верно, что $f(x)\in B_1$ или $f(x)\in B_2$, то есть $x\in f^{-1}[B_1]$ или $x\in f^{-1}[B_2]$.

Теперь докажем, что $f^{-1}(B_1)\cup f^{-1}(B_2)\subset f^{-1}[B_1\cup B_2]$. Действительно, для любого $x\in f^{-1}(B_1)\cup f^{-1}(B_2)$ верно, что $f(x)\in B_1$ или $f(x)\in B_2$, то есть $f(x)\in B_1\cup B_2$, что и означает, что $x\in f^{-1}[B_1\cup B_2]$.

е) В этом пункте ответ такой же: верно. Для проверки этого факта надо доказать (по определению равенства множеств из листка 1), что любой элемент, содержащийся в правом множестве, содержится также и в левом, и наоборот.

ж) Нет. Вот пример: X Y $A=\{1\}$, $B=\{2\}$.



з) Верно. В этом пункте также нужно сделать несложную проверку того, что $\forall y \in B_1$ будет также выполняться $y \in B_2$.

Определение 3. *Композицией отображений* $f\colon X \to Y$ и $g\colon Y \to Z$ называется отображение, сопоставляющее элементу x множества X элемент $g(f(x))$ множества Z. Обозначение: $g \circ f$. (То есть композиция $g \circ f$ состоит в последовательном применении отображений f и g.)

Стоит подчеркнуть, что мы пишем $g \circ f$, но применяем *сначала* отображение f к элементу x, а *потом* к элементу $f(x)$ применяем отображение g. В качестве мнемонического правила можно мысленно приписывать к $g \circ f$ справа (x).

Задача 5. Докажите, что для произвольных отображений $f\colon X \to Y$, $g\colon Y \to Z$ и $h\colon Z \to W$ выполняется следующее: $h \circ (g \circ f) = (h \circ g) \circ f$ (то есть скобки в выражении $h \circ g \circ f$ можно не писать).

Обе записи, по сути, означают последовательное применение всех трех отображений.

Решение. Возьмем произвольный $x \in X$. Пусть $f(x) = y$, $g(y) = z$, $h(z) = w$. (Вообще, множества часто обозначают большими буквами, а их элементы — соответствующими маленькими.) Тогда $g \circ f$ переводит x в z, $h \circ g$ переводит y в w. Соответственно, оба отображения $h \circ (g \circ f)$ и $(h \circ g) \circ f$ переводят x в w.

Заметим, что в этой задаче требуется доказательство равенства отображений, хотя нигде не определялось, что это такое. Действительно, что означает, что одно отображение «равно» другому? В этом месте следует навести школьника на мысль о том, что задача не вполне корректна, и попросить придумать *разумное* определение равенства отображений и решить задачу, пользуясь данным определением.

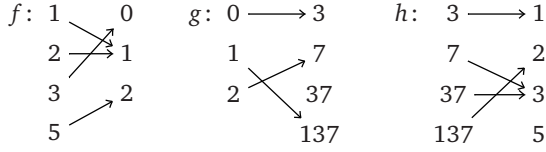
Естественно такое определение: два отображения f и g из X в Y называются равными, если $\forall x \in X \ f(x) = g(x)$, где «=» — это уже равенство (совпадение) элементов одного и того же множества. Согласно этому определению для равенства отображений нам надо показать, что если мы возьмем какой-то элемент $x \in X$, то образы при отображении $h \circ (g \circ f)$ и при отображении $(h \circ g) \circ f$ совпадут.

Действительно, пусть $f(x) = y$, $g(y) = z$, $h(z) = w$, тогда несложно убедиться в том, что образом элемента x при обоих отображениях будет элемент w. Что и требовалось доказать.

Если же пользоваться формальным определением отображения, то равенство отображений будет означать равенство соответствую-

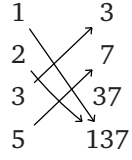
щих множеств пар элементов. А равенство множеств уже определялось в листке 1.

Задача 6. Пусть $f\colon \{1,2,3,5\}\to\{0,1,2\}$, $g\colon \{0,1,2\}\to\{3,7,37,137\}$, $h\colon \{3,7,37,137\}\to\{1,2,3,5\}$ — отображения, показанные на рисунке:

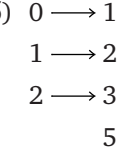


Нарисуйте картинки для следующих отображений:
а) $g\circ f$; б) $h\circ g$; в) $f\circ h\circ g$; г) $g\circ h\circ f$.

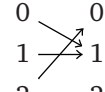
Решение. а)



б)



в)

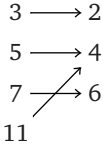


г) Отображение $g\circ h\circ f$ не определено (из-за того, что $h(0)$ не определено).

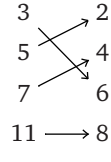
Определение 4. Отображение $f\colon X\to Y$ называется *биективным*, если для каждого $y\in Y$ найдется ровно один $x\in X$ такой, что $f(x)=y$.

Задача 7. Про каждое из отображений, изображенных на рисунке, выясните, является ли оно биективным:

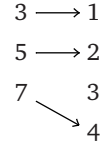
а)



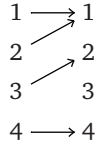
б)



в)



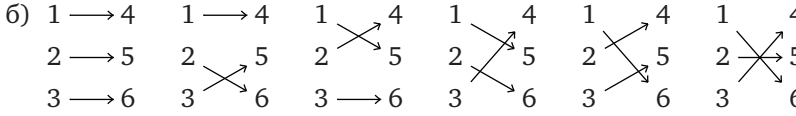
г)



Ответ. а) Нет; б) да; в) нет; г) нет.

Задача 8. Нарисуйте все биективные отображения а) из множества $\{1,2\}$ в множество $\{3,4,5,6\}$; б) из множества $\{1,2,3\}$ в множество $\{4,5,6\}$.

Решение. а) Биективных отображений из множества $\{1,2\}$ в множество $\{3,4,5,6\}$ существовать не может, так как в множестве $\{3,4,5,6\}$ элементов больше, а значит для любого отображения найдется такой элемент множества $\{3,4,5,6\}$, в который ничего не переходит.

б) 

Задача 9. Пусть $f\colon X \to Y$, $g\colon Y \to Z$. Верно ли, что если f и g биективны, то и $g \circ f$ биективно?

Ответ. Да. Доказательство представляет собой тривиальную проверку определения.

Определение 5. Отображение f называется *инъективным*, если оно разные элементы переводит в разные, т. е. если из $f(x) = f(x')$ следует, что $x = x'$.

Отображение $f\colon X \to Y$ называется *сюръективным*, если каждый элемент $y \in Y$ имеет хотя бы один прообраз, т. е. $f^{-1}(y) \neq \varnothing$ для любого $y \in Y$.

Задача 10. Докажите, что следующие свойства отображения $f\colon X \to Y$ эквивалентны:

1) f — биекция;

2) f сюръективно и инъективно;

3) f *обратимо*, то есть существует такое отображение[16] $g\colon Y \to X$, что $gf = \mathrm{Id}_X$, $fg = \mathrm{Id}_Y$, где $\mathrm{Id}_M\colon M \to M$, $m \mapsto m$ — *тождественное отображение*.

Нередко самый простой способ убедиться в биективности какого-либо отображения — построить к нему обратное.

Решение. Докажем сначала, что первые два свойства эквивалентны. Действительно, биективность означает, что у каждого элемента из Y ровно один прообраз, а инъективность и сюръективность — что этих прообразов, соответственно, не больше и не меньше одного.

Докажем теперь, что биективное отображение обратимо. Определим отображение g следующим образом. Пусть $y \in Y$. Так как отображение f биективно $f^{-1}(y)$ состоит из одного элемента — $x \in X$. Положим $g(y) = x$. По построению gf и fg — тождественные отображения.

Наконец, докажем, что обратимое отображение биективно. Пусть $y \in Y$. Тогда у y обязательно есть прообраз — элемент $g(y)$. Кроме того, у y не может быть другого прообраза x, так как $x = Id(x) = g(f(x)) = g(y)$.

[16] Говорят, что g — обратное к f и пишут $g = f^{-1}$.

Задача 11. Про каждые два из следующих множеств выясните, существует ли между ними биекция:

а) множество натуральных чисел;
б) множество четных натуральных чисел;
в) множество натуральных чисел без числа 3;
г) множество целых чисел.

В этой задаче впервые возникает удивительная ситуация, когда множество равномощно собственному подмножеству. Такое возможно только для бесконечных множеств.

Указание. Следует сначала построить биекцию между натуральными числами и натуральными числами без числа 3, а потом оптимально решать задачу, пользуясь задачей 9.

Решение. Формально нам надо проверить 6 утверждений: можно ли установить биекцию между первым и вторым множеством, между первым и третьим, вторым и третьим и т. д. Однако, воспользовавшись утверждением задачи 9, мы можем показать, что между всеми вышеперечисленными множествами можно установить биекцию, построив (явно) лишь три отображения. А именно, построим биективные отображения между множеством натуральных чисел и остальными тремя.

Обозначим множества из пунктов а), б), в) и г) соответственно буквами A, B, C и D и зададим биективные отображения:

$$\begin{array}{cccccccccc}
A & 1 & 2 & 3 & \dots & n & & & & \\
 & \downarrow & \downarrow & \downarrow & & \downarrow & & & & \\
B & 2 & 4 & 6 & \dots & 2n & & & & \\
\end{array}$$

$$\begin{array}{cccccccc}
A & 1 & 2 & 3 & 4 & \dots & n & \\
 & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \\
C & 1 & 2 & 4 & 5 & \dots & n+1 & \\
\end{array}$$

$$\begin{array}{cccccccccccc}
A & 1 & 2 & 3 & 4 & 5 & 6 & \dots & 2n & 2n+1 \\
 & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & & \downarrow & \downarrow \\
D & 0 & -1 & 1 & -1 & 2 & -2 & \dots & -n & n \\
\end{array}$$

Комбинаторика 1

листок 3 / сентябрь 2004

В этом листке обсуждаются простейшие комбианторные задачи на нахождение числа каких-то объектов. Общий метод решения этих задач следующий. Нужно придумать разумный способ перечисления (возможно с повторениями) всех интересующих нас объектов. Например, часто удобно перечислять что-либо в лексикографическом («алфавитном») порядке. Длину получившегося списка часто несложно вычислить.

После этого следует учесть наличие в списке повторений — разных записей, соответствующих одному и тому же (с точки зрения данной задачи) объекту. В простейшем случае все объекты повторяются одно и то же число раз, и достаточно разделить число элементов в списке на количество повторений («число симметрий объекта»). Развитием этой идеи является, например, лемма Бернсайда (простейшие проявления которой можно встретить и в этом листочке).

Соответственно, основные навыки, которые должны получить школьники при решении этого листка, — 1) перечисление всех вариантов в разумном порядке; 2) понимание того, какие «записи» соответствуют одному и тому же объекту (именно поэтому в листке много похожих, но различных задач), и умение это учесть при подсчете.

Другая полезная (отнюдь не только в комбинаторике) идея, которой можно научить на материале этого листка, состоит в том, что, прежде чем решать задачу для произвольного (или очень большого) n, полезно сначала разобраться со случаем небольших n. Замеченные при этом закономерности (даже если они не доказаны) часто существенно упрощают решение задачи.

Задача 1. Сколько существует «слов» [17]: а) из двух; б) из трех букв русского языка?

Решение. а) Попробуем для начала решить ту же задачу, но с алфавитом, состоящим всего из трех букв — а, б, в. Здесь мы можем явно выписать все слова, состоящие из двух букв: аа, аб, ав, ба, бб, бв, ва, вб, вв. Получили $9 = 3 \cdot 3$.

В общем случае подсчет числа таких слов будем вести следующим образом: сначала посчитаем число слов, которые начинаются с буквы «а», затем — число слов, начинающихся с буквы «б» и так далее. Со-

[17] В этой задаче, конечно, имеются в виду не те слова, которые можно встретить в словаре, а произвольные сочетания букв русского языка.

вершенно очевидно, что таким образом мы посчитаем каждое «слово» по разу.

Заметим, что двухбуквенных слов, начинающихся на букву «а», будет ровно столько же, сколько есть букв в алфавите. Слов, начинающихся на букву «б», будет столько же. И так со всеми буквами.

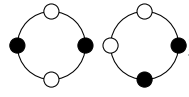
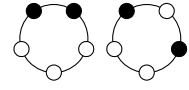
В нашей задаче слов, начинающихся с буквы «а», будет 33. Столько же будет слов, начинающихся с буквы «б», и так далее. Значит, всего слов, состоящих из двух букв, будет $33 \cdot 33 = 1089$.

б) Ответ: $33 \cdot 33 \cdot 33 = 35937$.

На самом деле в пункте а) речь идет о (декартовом) произведении множеств. Произведением множеств называют множество из упорядоченных пар. Число элементов в произведении множеств равно произведению числа элементов исходных множеств.

Задача 2. Сколько существует различных ожерелий: а) из трех разноцветных; б) из двух красных и двух синих; в) из трех красных и двух синих бусинок?

В этой задаче важно понимать, что такое различные ожерелья. Здесь это означает, что одно из них нельзя «совместить» с другим. Считается, что ожерелье можно поворачивать и переворачивать.

Ответ. а) 1:  ; б) 2:  ; в) 2:  .

Задача 3. Сколькими способами можно выбрать из десяти человек двух дежурных и одного старшего дежурного?

Решение. Полезным упражнением является честное выписывание троек дежурных, выбираемых из, скажем, четырех человек (Вася, Коля, Леша, Петя).

При этом первым будем писать старшего дежурного, а остальных дежурных записывать в алфавитном порядке. Удобно при этом сначала выбирать старшим дежурным первого по алфавиту, потом второго по алфавиту и т. д. Так как порядок «обычных» дежурных не важен, выписывая их по алфавиту, мы никакой случай не забудем и не повторим дважды.

(Вася, Коля, Леша),	(Вася, Коля, Петя),	(Вася, Леша, Петя),
(Коля, Вася, Леша),	(Коля, Вася, Петя),	(Коля, Леша, Петя),
(Леша, Вася, Коля),	(Леша, Вася, Петя),	(Леша, Коля, Петя),
(Петя, Вася, Коля),	(Петя, Вася, Леша),	(Петя, Коля, Леша),

Итого 12 вариантов.

Теперь перейдем к решению исходной задачи. Старшего дежурного можно выбрать десятью способами. Когда мы уже выбрали старшего, мы можем выбрать первого дежурного девятью (потому что одного человека мы уже назначили старшим дежурным) способами. После того, как мы выбрали старшего дежурного и еще одного дежурного, второго дежурного мы можем выбрать восемью способами. Итого, вроде бы, по «правилу умножения» должно получаться $10 \cdot 9 \cdot 8 = 720$.

Однако если мы внимательно посмотрим на наше решение, то увидим, что каждую тройку дежурных мы посчитали по два раза. Например, тройку дежурных (Вася — старший дежурный, Леша, Петя) мы посчитали два раза: как тройку (Вася, Петя, Леша) и как тройку (Вася, Леша, Петя). Поэтому правильный ответ в два раза меньше — 360.

Задача 4. Сколькими способами можно выбрать: а) из пяти; б) из семи; в) из десяти человек трех дежурных?

Решение. а) В этой задаче все дежурные одинаковые. Поэтому нам надо число $5 \cdot 4 \cdot 3 = 60$ (это число способов выбрать трех *разных* дежурных из пяти человек) поделить на число повторений. Оно равно шести. Действительно, ведь *каждую* тройку мы повторили шесть раз. Например, группу дежурных, состоящую из Васи, Пети и Леши, мы посчитали как шесть троек дежурных: (Вася, Петя, Леша), (Вася, Леша, Петя), (Петя, Вася, Леша), (Леша, Вася, Петя), (Петя, Леша, Вася), (Леша, Петя, Вася). Ответ: $10 = 60/6$.

б) Аналогично получаем ответ: $7 \cdot 6 \cdot 5/6 = 35$.

в) Ответ: $10 \cdot 9 \cdot 8/6 = 120$.

Задача 5. Сколькими способами можно рассадить пять человек в автобусе, если в автобусе: а) 4; б) 5; в) 6; г) 7 свободных мест?

Решение. а) Попробуем для начала рассадить троих людей в автобусе с двумя местами. В этом простом случае мы можем явно выписать способы рассадки, перечисляя имена людей в скобках. При этом первым будем писать имя того, кто сидит на первом месте, а вторым — имя того, кто сидит на втором месте. Например, так:

(Коля, Вася), (Коля, Петя),
(Вася, Коля), (Вася, Петя),
(Петя, Вася), (Петя, Коля).

Получили $2 \cdot 3 = 6$.

Этот же ответ можно было получить так: на первое место может сесть три человека, тогда на второе — оставшиеся два; всего получается $2 \cdot 3 = 6$ способов.

Аналогично действуем и при решении исходной задачи: на первое место может сесть пять человек, на второе — четыре, на третье — три, и на четвертое — два. Итого получаем $5 \cdot 4 \cdot 3 \cdot 2 = 120$.

б) В этом пункте совершенно аналогично получаем $5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$.

в) Первый человек может сесть на любое из шести мест, второй — на любое из оставшихся пяти, третий — на любое из оставшихся четырех, четвертый — на любое из оставшихся трех, и, наконец, пятый — на любое из оставшихся двух. Всего получаем $6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 720$ вариантов рассадки.

г) Аналогично находим ответ: 2520 способов.

Задача 6. Семь учеников 8 «В» класса решили вместе покататься:

а) на аттракционе «поезд», состоящем из семи одноместных вагончиков;

б) на карусели, у которой ровно семь мест;

в) на «поезде» из десяти вагончиков;

г) на карусели, у которой ровно десять мест.

Сколькими способами они смогут это сделать?

Вопросы в пунктах а) и в) по существу такие же, как и в предыдущей задаче.

Пункты б) и г) отличается от пунктов а) и в) тем, что карусель — это как бы поезд, замкнутый в кольцо. Поэтому для того, чтобы получить правильные ответы в пунктах б) и г), надо ответы в пунктах а) и в) поделить на число мест. Действительно, ведь если мы будем «склеивать» карусель с уже сидящими в кабинках школьниками из поезда с сидящими в вагонах школьниками, то каждая карусель будет получаться из ровно семи рассадок школьников по поезду. Так, например, следующие рассадки школьников в поезде:

(1, 2, 3, 4, 5, 6, 7), (2, 3, 4, 5, 6, 7, 1), (3, 4, 5, 6, 7, 1, 2),
(4, 5, 6, 7, 1, 2, 3), (5, 6, 7, 1, 2, 3, 4), (6, 7, 1, 2, 3, 4, 5),
(7, 1, 2, 3, 4, 5, 6)

«склеятся» в одну и ту же карусель.

Ответ. а) $7! = 5040$ (здесь $n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$); б) $5040/7 = 720$; в) $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 = 604800$; г) $604800/10 = 60480$.

Задача 7. Сколькими способами можно пройти из левого нижнего угла квадрата: а) 2×2; б) 3×3; в*) 5×5, двигаясь только вверх или вправо по сторонам клеток?

Решение. Решать задачу будем следующим образом: будем писать рядом с узлом решетки число, равное числу способов попасть из этой точки в правый верхний угол. Рядом с точками, лежащими на правой или верхней стороне квадрата, мы сразу можем написать единицы, потому что из каждой из них можно пройти в правый верхний угол, очевидно, единственным способом. А далее будем действовать так: если у нас есть такая точка, что правее и выше от нее лежат точки, рядом с которыми уже написаны числа, то рядом с этой точкой мы пишем сумму чисел, стоящих справа и сверху. Вопрос на засыпку: почему именно сумму и почему именно этих чисел? Как сумма этих чисел связана с числом способов пройти в правый верхний угол?

В итоге рано или поздно мы расставим числа рядом со всеми узлами решетки. В частности, рядом с левым нижним углом. Это и будет ответ.

Ответ. а) 6; б) 20; в) 252.

> **Задача 8.** Сколькими способами можно представить числа 5, 10, 20 в виде суммы: а) двух; б) трех натуральных чисел?

Решение. Заметим, что условие задачи можно понимать по-разному. Вопрос в том, считаются ли, например, разложения $3=2+1$ и $3=1+2$ одинаковыми. Разберем оба случая на примере разбиения числа 10 в сумму трех натуральных чисел.

Вариант 1. Разложения, отличающиеся перестановкой слагаемых, считаются одинаковыми.

Выпишем все способы разложения десяти в сумму трех слагаемых: $10=1+1+8=1+2+7=1+3+6=1+4+5=2+2+6=2+3+5=2+4+4=3+3+4$.

Заметим, что для того, чтобы выписать все тройки чисел, дающих в сумме 10, достаточно выписать лишь те наборы чисел, в которых каждое следующее не меньше предыдущего (что мы и сделали). Например, набор (7, 2, 1) у нас представлен как (1, 2, 7). В этом месте возникает вопрос, почему мы выписали все разложения. Для ответа достаточно внимательно посмотреть на способ перечисления.

Ответ. Число 5 раскладывается в сумму двух натуральных чисел двумя способами, а в сумму трех — двумя способами. Число 10 раскладывается в сумму двух натуральных чисел пятью способами, а в сумму трех — восемью способами. Число 20 раскладывается в сумму двух натуральных чисел десятью способами, а в сумму трех — тридцатью тремя способами.

Вариант 2. Разложения, отличающиеся перестановкой слагаемых, считаются разными.

Тогда наша задача будет эквивалентна следующей: перед нами лежат в ряд десять палочек; сколькими способами между ними можно поставить две перегородки так, чтобы и слева и справа от каждой перегородки лежало по палочке.

А задачу с палочками решить совсем не трудно. Всего у нас есть девять мест, куда мы можем ставить перегородки. Поэтому первую перегородку мы можем поставить на девять мест, а вторую — на оставшиеся восемь. Но при этом мы каждый расклад посчитаем по два раза (перегородки-то одинаковые). Поэтому ответ: $(9\cdot 8)/2 = 36$.

Задача 9. Сколькими способами можно расставить скобки в выражении $a+b-c\cdot d$?

Условие этой задачи при первом прочтении не вполне понятно. Вопрос вот в чем: нас интересуют произвольные расстановки скобок или обладающие какими-то разумными свойствами? Например, устроит ли нас такая расстановка скобок: $(((a+b-c\cdot d)))$?

Ясно, что если мы будем расставлять скобки произвольно, то получим бесконечно много вариантов. Поэтому возможное разумное прочтение условия такое:

Будем считать две расстановки скобок в выражении $a+b-c\cdot d$ *одинаковыми*, если при подстановке в них любого набора чисел (a, b, c, d) получается одно и то же число. Сколько существует различных (в этом смысле) расстановок скобок?

Решение. Расставить скобки — это то же самое, что определить порядок выполнения действий. В каком порядке выполнять сложение и вычитание неважно, остается решить, в какой момент выполнять умножение. Получаются 3 выражения:

$$(a+b-c\cdot d), \quad a+(b-c)\cdot d, \quad (a+b-c)\cdot d.$$

Остается убедиться, что при некоторых значениях a, b, c и d все эти выражения принимают попарно различные значения. Для этого подойдут практически любые значения переменных, например, $a=3$, $b=2$, $c=1$, $d=0$.

Задача 10. а) Докажите, что подмножеств в множестве $\{a, b, c, d, e\}$ столько же, сколько отображений этого множества в множество $\{0, 1\}$. б) Докажите, что это число равно числу последовательностей нулей и единиц длины пять.

Решение. Каждому подмножеству M множества $A=\{a, b, c, d, e\}$ мы можем естественным образом сопоставить отображение f из множества A в множество $\{0, 1\}$ по следующему правилу: элемент $x \in A$ отображается в 1 (то есть $f(x)=1$), если x лежит в M, и в 0, если не лежит. Нетрудно заметить (хотя это надо формально и аккуратно проверить), что мы построили биекцию.

В пункте б) действуем аналогично. То есть строим биекцию из множества всех подмножеств множества $A=\{a, b, c, d, e\}$ в множество последовательностей из нулей и единиц. Например, подмножеству $M=\{a, c, e\}$ мы сопоставим последовательность (1, 0, 1, 0, 1); подмножеству $M=\{b, c\}$ сопоставим (0, 1, 1, 0, 0); подмножеству $M=\{a, d, e\}$ сопоставим (1, 0, 0, 1, 1) и так далее. А именно, занумеруем элементы множества, после чего любому подмножеству поставим в соответствие последовательность, у которой на каждом месте стоит 1, если этот элемент принадлежит подмножеству, и 0, если нет.

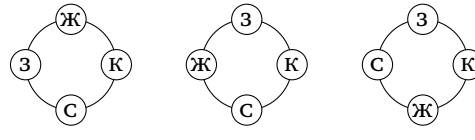
Задача 11*. Сколько существует различных наборов бусинок, из которых можно составить ровно два различных ожерелья?

Во-первых, очень важно разобраться в том, какие наборы считаются различными, а какие — нет. Например, наборы {синий, синий, красный} и {оранжевый, зеленый, зеленый} считаются одинаковыми, а наборы {красный, синий, зеленый} и {голубой, желтый, голубой} — различными. Почему?

Во-вторых, полезно порисовать всевозможные наборы из небольшого числа бусинок и попытаться найти какие-то закономерности.

Решение. Во-первых, наборы бусинок не упорядочены, то есть наборы {синий, синий, красный} и {синий, красный, синий} одинаковы. Во-вторых, наборы, получающиеся друг из друга переименованием цветов, также считаются одинаковыми.

Докажем сначала, что в искомом наборе не может быть слишком много различных цветов, а именно, не может быть более трех различных цветов. Допустим, нашелся набор, содержащий бусинки четырех различных цветов (назовем их красный, желтый, зеленый, синий), из которого можно составить только два различных ожерелья. Рассмотрим следующие ожерелья:



Здесь «К» означает все бусинки красного цвета, «З» — синего и т. д. Видно, что эти ожерелья различны. Следовательно, в искомом наборе не более трех различных цветов. Если все бусинки одноцветны, то можно составить только одно ожерелье. Итак, в искомом наборе бусинок может встречаться или два, или три цвета. Дальше задача является явным перебором. Приведем его для случая двух цветов.

Если бусинок каждого цвета хотя бы три, то можно составить такие три различных ожерелья: (все красные, все синие), (красные кроме одной, синяя, красная, остальные синие), (красные кроме двух, синяя, красная, синяя, красная, остальные синие).

Следовательно, бусинок какого-то цвета (допустим, красного) не больше двух. Если в наборе ровно одна красная бусинка, то из этого набора можно составить только одно ожерелье. Таким образом, в искомом наборе ровно две красные бусинки и сколько-то синих. Заметим, что различные ожерелья отличаются только числом синих бусинок между красными. Теперь уже несложно видеть, что ровно два ожерелья получится, если синих бусинок будет две или три.

Случай наборов из трех цветов разбирается аналогично.

Ответ. Две красных и две синих бусинки; две красных и три синих бусинки; две красных, одна синяя и одна желтая бусинка; три красных, одна синяя и одна желтая бусинка.

Задача 12*. В городе Энск номера автобусных билетов четырехзначные. Жители этого города считают, что билеты, у которых сумма первых двух цифр равна сумме последних двух цифр, счастливые. Сколько счастливых билетов в Энске?

Указание. Здесь надо отдельно посчитать число счастливых билетов, у которых сумма первых двух цифр равна нулю. Затем те, у которых эта сумма будет равна единице. И так далее до случая, когда сумма будет равна $18 = 9 + 9$. Затем найденные числа сложить. Заметим, что мы уже решали похожую задачу, когда разбивали разные числа в сумму двух.

Ответ. 670.

Задача 13*. Сколькими способами можно раскрасить колесо обозрения: а) с 7 кабинками в 3 цвета; б) с 10 кабинками в 2 цвета? При раскраске не обязательно использовать все цвета.

Решение. а) Зафиксируем сначала колесо и раскрасим его. Это можно сделать 3^7 способами. Теперь посчитаем, сколько раз мы учли каждую раскраску вращающегося колеса. Любая раскраска, которая не

переходит в себя ни при каком вращении колеса, посчитана 7 раз. Поскольку число 7 — простое, в себя при вращении колеса переходят только одноцветные раскраски. Итак, все раскраски, кроме трех, посчитаны по 7 раз, а эти три — по одному разу. Отсюда легко находим число раскрасок $\frac{3^7-3}{7}+3$.

б) Будем действовать аналогично предыдущему пункту. При этом возникнет новая трудность: не только одноцветные раскраски переходят в себя при повороте. Посчитаем сначала (кроме одноцветных), сколько раскрасок переходят в себя при хоть каком-нибудь повороте. При повороте на 1, 3, 7 и 9 в себя переходят только одноцветные раскраски. При повороте на 2, 4, 6 и 8 в себя переходят еще и раскраски, в которых цвета чередуются (у зафиксированной карусели есть две такие неодноцветные раскраски). При повороте на 5 в себя переходят симметричные раскраски (кроме одноцветных, их $2^5-2=30$). Следовательно, по 10 раз мы посчитали $2^{10}-2-2-30=990$ раскрасок.

Итак, общее число раскрасок вращающегося колеса равно $\frac{990}{10}+$ $+\frac{30}{5}+\frac{2}{2}+2=99+6+1+2=108$.

Далеким обобщением этого метода подсчета является лемма Бернсайда из листочка «Теория групп 2».

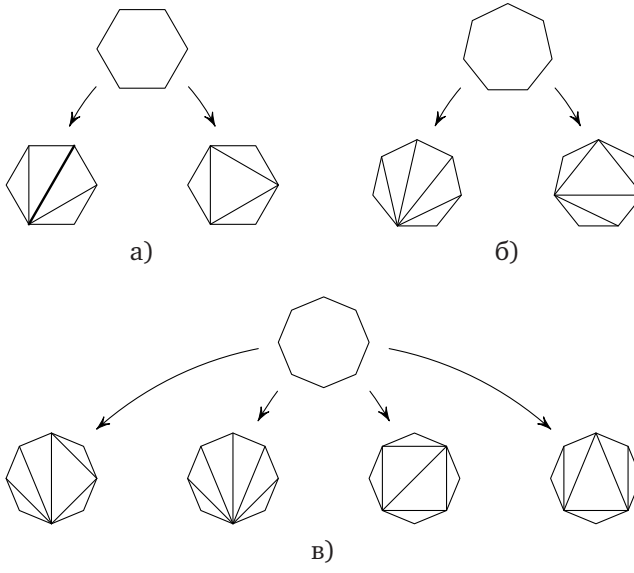
Задача 14. Кто-то режет правильный: а) шестиугольник; б*) семиугольник; в*) восьмиугольник на треугольники, проводя разрезы по непересекающимся диагоналям. Сколько разных наборов треугольников может получиться?

Решение. а) Разрезания шестиугольника мы можем разбить на два класса: те, в которых есть разрез по главной диагонали, и те, в которых его нет. Заметим, что если шестиугольник разрезан по главной диагонали, то как бы мы ни разрезали получившиеся четырехугольники (трапеции), мы будем получать один и тот же набор треугольников.

Если же разреза по главной диагонали нет, то это означает, что мы можем лишь отрезать маленькие треугольнички от шестиугольника, и в этом случае также можем получить лишь один набор треугольников в итоге (см. рис. а).

б) Ответ: два набора (см. рис. б).

в) Ответ: четыре набора (см. рис. в).



Задача 15. Сколько существует различных игральных кубиков (на гранях кубика расставлены числа от 1 до 6)?

Это хорошее упражнение на идею «факторизации»: нужно сначала вычислить число элементов большего множества объектов, а потом разделить это число на число повторений.

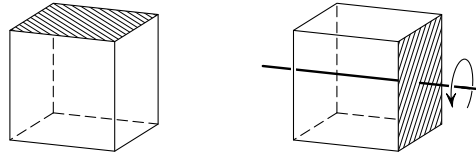
К концу листка до такого плана обычно догадывается каждый, но его реализация связана с некоторыми техническими трудностями. Поэтому не стоит требовать полностью формального решения от всех школьников — вполне достаточно понимания того, что происходит.

Решение. Итак, нас интересует число способов наклеить на грани кубика цифры от 1 до 6, при этом кубики с наклеенными цифрами считаются одинаковыми, если их можно совместить так, чтобы цифры на гранях совпали.

Пусть сначала кубик неподвижно лежит на столе. Число способов наклеить на него цифры от 1 до 6 есть количество способов рассадить 6 человек (наклейки) по 6 местам (грани), т. е. (см. задачу 5) $6! = 720$.

Осталось понять, сколько из получившихся 720 кубиков можно совместить так, чтобы наклейки совпали. Другими словами, пусть все эти 720 кубиков лежат на столе в том положении, в каком на них были наклеены цифры; если разрешить какой-то из кубиков катать по столу, сколько из имеющихся кубиков мы сможем получить?

Ясно, что это число равно числу способов повернуть кубик (числу симметрий куба). Эти способы уже нетрудно подсчитать: при повороте верхняя грань куба может оказаться в одном из 6 положений (сверху, снизу, слева, справа, спереди, сзади), каждому из которых соответствует ровно 4 поворота (действительно, после того, как место одной из граней куба зафиксировано, единственное, что мы можем делать, — вращать его вокруг проходящей через эту грань оси). То есть всего способов $6 \cdot 4 = 24$.



Значит, на нашем столе каждый игральный кубик встречается по 24 раза. Соответственно, число различных игральных кубиков равно $720 : 24 = 30$.

Подстановки 1. Ходим по циклу

листок 1д / октябрь 2004

Это первый листок из серии, в которой изучаются сначала подстановки, а потом и абстрактные группы.

Большинство задач представляют собой несложные упражения на понимание того, что такое произведение подстановок. Содержательные вопросы про подстановки отложены до листка «Подстановки 2» (и, частично, листков по теории групп). Стоит, однако, отметить две важные задачи: задачу 7, в которой (как будет видно позже) доказывается, что подстановки образуют группу, и (дополнительную) задачу 9, что-то объясняющую про то, как могут быть устроены перестановки.

Определение 1. *Подстановкой из n элементов* называется биективное отображение из множества $\{1, 2, \ldots, n\}$ в себя. Запись вида

$$\begin{pmatrix} i_1 i_2 \ldots i_n \\ j_1 j_2 \ldots j_n \end{pmatrix},$$

где $i_1, i_2, \ldots, i_n$ — различные элементы множества $\{1, 2, \ldots, n\}$ и $j_1, j_2, \ldots, j_n$ — различные элементы множества $\{1, 2, \ldots, n\}$, обозначает подстановку a, для которой $a(i_k) = j_k$ при всех $k \in \{1, 2, \ldots, n\}$. Множество подстановок из n элементов обозначается S_n. Подстановку можно графически изобразить следующим образом. Расположим на плоскости элементы множества $\{1, 2, \ldots, n\}$ и для каждого i проведем стрелку из элемента i в элемент $a(i)$. То, что получилось, называется *графом подстановки*.

Проясним несколько моментов, которые могут вызвать трудности после прочтения определения. Несмотря на данное «формальное» определение, подстановка — это очень наглядный объект. При решении задач этого листка следует обязательно «поиграть» с подстановками, проверяя утверждения для небольших n, в том числе, сделав несколько фишек с номерами, и переставляя их.

Запись $\begin{pmatrix} i_1 i_2 \ldots i_n \\ j_1 j_2 \ldots j_n \end{pmatrix}$ означает, что в первой строке стоят числа 1, 2, …, n, как-то перемешанные (то есть не обязательно по порядку), а в нижней строке тоже стоят числа 1, 2, …, n, возможно, перемешанные по-другому. Отметим отдельно, что подстановка — это *биективное* отображение. Запись $a(i_k) = j_k$ означает, что число (i_k) при подстановке (ведь подстановка — это отображение) переходит в число j_k.

Важно понимать, что требование того, чтобы отображение переводило именно множество $\{1, 2, \ldots, n\}$ в себя — это вопрос соглашения. Можно было бы определить подстановку на произвольном

множестве из n элементов. Этой темы мы еще коснемся в следующих листках, когда определим действие группы.

Задача 1. Какие из следующих таблиц являются записями подстановок: а) $\binom{1}{1}$; б) $\binom{123}{123}$; в) $\binom{2}{2}$; г) $\binom{123}{234}$; д) $\binom{123}{333}$; е) $\binom{514632}{164253}$; ж) $\binom{4321}{1234}$; з) $\binom{5321}{5321}$; и) $\binom{1327}{7231}$; к) $\binom{123}{112}$?

Ответ. а) Является.

б) Является.

в) Нет, так как множество $\{2\}$ не имеет вид $\{1, 2, \ldots, n\}$.

г) Нет, так как данное отображение не отображает множество $\{1, 2, 3\}$ в себя.

д) Нет, так как данное отображение не отображает множество $\{1, 2, 3\}$ в себя.

е) Является.

ж) Является.

з) Нет, так как множество $\{1, 2, 3, 5\}$ не имеет вид $\{1, 2, \ldots, n\}$ (пропущено 4).

и) Нет, так как множество $\{1, 2, 3, 7\}$ не имеет вид $\{1, 2, \ldots, n\}$ (пропущены 4, 5 и 6).

к) Нет, так как данное отображение не отображает множество $\{1, 2, 3\}$ в себя.

Задача 2. Выпишите и изобразите графически все элементы множеств S_1, S_2 и S_3.

Решение. а) В S_1 имеется всего один элемент — подстановка $\binom{1}{1}$.

б) В S_2 будет два элемента — подстановки $\binom{12}{12}$ и $\binom{12}{21}$.

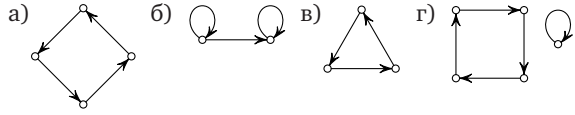
в) В S_3 будет шесть элементов — подстановки $\binom{123}{123}$, $\binom{123}{132}$, $\binom{123}{213}$, $\binom{123}{231}$, $\binom{123}{321}$, $\binom{123}{312}$.

Если в задаче требуется перечислить биективные отображения (или же какие-либо другие объекты), то нужно найти такой способ перечисления, при котором ни один объект не будет пропущен или посчитан два раза. Более подробно вопрос перечисления объектов разобран в листке «Комбинаторика 1».

В последней задаче подстановки перечислялись следующим образом: элемент 1 может перейти в один из n элементов, элемент 2 — в один из $n-1$ элемента (один уже занят), элемент 3 — в один из

$n-2$ элементов (два уже заняты), и так далее. Следовательно, число подстановок из n элементов равно $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$.

Задача 3. Какие из следующих изображений являются графами подстановок?



Решение. а) Картинка является графом подстановки $\begin{pmatrix}1234\\2341\end{pmatrix}$.

б) Картинка не является графом подстановки, так как в одну вершину входят две стрелки.

в) Картинка является графом подстановки $\begin{pmatrix}123\\231\end{pmatrix}$.

г) Картинка является графом подстановки $\begin{pmatrix}12345\\23415\end{pmatrix}$.

Задача 4. а) Сколько элементов в множестве S_n?

б) Сколькими способами можно записать подстановку из n элементов?

Конечно, имеется в виду число различных записей в виде таблицы (а не графиком, в виде таблицы и т. п.).

Решение. а) Заметим, что вопрос о числе биективных отображений из множества, состоящего из n элементов, в себя уже был разобран в задаче 2. Остается лишь вспомнить ответ: $n! = n(n-1)\ldots 1$.

б) Как уже было замечено, одна и та же подстановка может быть записана разными способами. Например, записи $\begin{pmatrix}123\\213\end{pmatrix}$ и $\begin{pmatrix}231\\132\end{pmatrix}$ задают одну и ту же подстановку. Нетрудно понять, что различные записи одной и той же подстановки могут различаться лишь порядком столбцов. Следовательно, всего записей одной перестановки из n элементов столько же, сколько существует способов переставить n столбцов. То есть в точности столько же, сколько существует перестановок из n элементов, а именно $n!$.

Чтобы избежать неоднозначности, обычно используют так называемую *каноническую* запись подстановки, при которой все числа сверху упорядочены по возрастанию. В этом случае вся информация о том, какие элементы куда переходят, содержится в нижней строке. Но иногда, например, при умножении подстановок, оказывается удобнее пользоваться другими записями. Вот примеры подстановок, записанных канонически: $\begin{pmatrix}123\\213\end{pmatrix}$, $\begin{pmatrix}12345\\12345\end{pmatrix}$, $\begin{pmatrix}12345\\21354\end{pmatrix}$, $\begin{pmatrix}1234567\\7654321\end{pmatrix}$.

Определение 2. *Произведением* подстановок $a, b \in S_n$ называется их композиция как отображений: $a \circ b$. Обозначение: ab.

Здесь нужно помнить о том, что подстановки — это отображения из множества $\{1, 2, \ldots, n\}$ в себя (см. листок «Теория множеств 2»). Когда мы записываем композицию двух отображений, они записываются как бы «в обратном порядке». Это удобно запоминать, мысленно приписав справа (x): получится $ab(x)$. При этом, находя образ числа x, мы сначала вычисляем $b(x)$, а потом применяем к результату подстановку a и получаем $a(b(x)) = ab(x)$.

Разберем два способа перемножения подстановок на конкретном примере. Пусть мы хотим вычислить произведение двух перестановок, записаных в канонической форме. Например, вычислим произведение $\binom{12345}{43521}\binom{12345}{23451}$. Мы будем вычислять каноническую форму произведения, постепенно заменяя на цифры значки «$*$» в подстановке-результате $\binom{12345}{*****}$.

Заметим, что в правой подстановке 1 переходит в 2, а затем в левой подстановке 2 переходит в 3. Значит, при их композиции 1 переходит в 3 и мы пишем вместо первой звездочки число 3. Аналогично действуем дальше:

$$\binom{12345}{*****} \to \binom{12345}{3****} \to \binom{12345}{35***} \to \binom{12345}{352**} \to \binom{12345}{3521*} \to \binom{12345}{35214}.$$

Опишем второй способ, позволяющий в ряде случаев сократить вычисления. Допустим, нам надо посчитать произведение подстановок $\binom{12345}{43521}\binom{15342}{21453}$. Приведем первую подстановку к такому виду, чтобы ее первая строка оказалась такой же, как и вторая строка второй подстановки. В данном случае это будет выглядеть так: $\binom{12345}{43521} \to \binom{21453}{34215}$. А теперь запишем подстановки одну под другой (приведенную левую под правой):

$$\binom{15342}{21453}$$
$$\binom{21453}{34215}$$

После этого выкинем две промежуточные строчки (вторую у верхней подстановки и первую у нижней). Получим ответ $\binom{15342}{34215} = \binom{12345}{35214}$.

Задача 5. Найдите произведения: а) $\binom{123}{312}\binom{312}{123}$; б) $\binom{1234}{4321}\binom{1234}{2143}$; в) $\binom{124536}{123456}\binom{642351}{123456}$; г) $\binom{12345}{24531}\binom{12345}{35124}$; д) $\binom{123456}{561423}\binom{123456}{345261}$.

Решение. а) Воспользуемся первым способом. Сперва в правой подстановке 1 переходит в 2, а затем в левой 2 переходит в 1. Значит, в их произведении 1 перейдет в себя. Аналогично устанавливаем, что 2 переходит в 2, а 3 — в 3.

Ответ. а) $\binom{123}{123}$; б) $\binom{1234}{3412}$; в) $\binom{123456}{653241}$; г) $\binom{12345}{51243}$; д) $\binom{123456}{142635}$.

Задача 6. Верно ли, что для любых подстановок $a, b \in S_n$ выполняется равенство $ab = ba$?

Решение. Нет. Например, если $a = \binom{123}{213}$, $b = \binom{123}{132}$, то $ab = \binom{123}{231}$, $ba = \binom{123}{312}$. То есть $ab \neq ba$. Это означает, что операция перемножения подстановок некоммутативна.

Определение 3. Подстановка $e = \binom{12\ldots n}{12\ldots n}$ называется *тождественной*.

Задача 7. Докажите следующие утверждения:
а) для любой подстановки $a \in S_n$ $ae = ea = a$;
б) для любых подстановок $a, b, c \in S_n$ $(ab)c = a(bc)$;
в) для любой подстановки $a \in S_n$ существует и при том единственная подстановка $b \in S_n$ такая, что $ab = ba = e$.

Решение. а) С одной стороны, утверждение этого пункта следует из свойств отображений. С другой стороны, можно записать общий вид произвольной подстановки: $a = \binom{i_1 i_2 \ldots i_n}{j_1 j_2 \ldots j_n}$ и перемножить ее с тождественной — $\binom{12\ldots n}{12\ldots n}$, следуя одному из описанных способов.

б) Решение задачи следует из аналогичного свойства отображений (листок «Теория множеств 2»).

в) Если подстановка a имеет вид $\binom{i_1 i_2 \ldots i_n}{j_1 j_2 \ldots j_n}$, то в качестве b нужно взять подстановку вида $\binom{j_1 j_2 \ldots j_n}{i_1 i_2 \ldots i_n}$. Теперь легко проверить напрямую, что подстановка b удовлетворяет условию задачи.

Полезно понимать, как по графу подстановки построить граф обратной к ней.

Определение 4. Пусть $1 \leqslant i, j \leqslant n$, $i \neq j$. Подстановка a такая, что $a(i) = j$, $a(j) = i$, $a(k) = k$ при $k \neq i, j$, называется *транспозицией*. Обозначение: $(i\ j)$.

Определение 5. Пусть $i_1, i_2, \ldots, i_k$ — различные элементы множества $\{1, 2, \ldots, n\}$. Подстановка a, сдвигающая элементы $i_1, i_2, \ldots, i_k$, то есть такая, что $a(i_j) = i_{j+1}$ для любого $j \in \{1, 2, \ldots, k-1\}$, $a(i_k) = i_1$ и $a(s) = s$ при $s \notin \{i_1, i_2, \ldots, i_k\}$, называется *циклом длины* k. Обозначение: $(i_1\, i_2 \ldots i_k)$. Множество $\{i_1, \ldots, i_k\}$ называется *носителем* цикла, а число k — *длиной* цикла.

Задача 8. а) Какие из подстановок задач 1 и 2 являются циклами, а какие — транспозициями?

б) Сколько циклов длины 57 в S_{57}?

в) Сколько циклов и сколько транспозиций в S_5?

г) При каких условиях произведение двух транспозиций является циклом?

д*) При каких условиях произведение двух циклов является циклом?

Решение. Не будем упоминать в перечислении тождественную подстановку — «цикл длины 1», присутствующую в каждом S_n.

а) Среди подстановок первой задачи лишь один цикл: $\binom{514632}{164253}$. В S_1 циклов нет. В S_2 только один цикл — $\binom{12}{21}$. В S_3 пять циклов: $\binom{123}{213}$, $\binom{123}{132}$, $\binom{123}{321}$, $\binom{123}{231}$, $\binom{123}{312}$.

б) Рассмотрим варианты того, куда может переходить единица в цикле длины 57. Для этого имеется 56 вариантов (все числа кроме самой единицы). Тогда у числа, в которое перешла единица, есть 55 вариантов перехода (все числа, кроме себя и единицы), у следующего будет 54 варианта, и так далее. Значит, ответ 56!.

в) В S_5 имеется $C_5^2 = 10$ транспозиций (т. е. циклов длины 2): (1 2), (1 3), (1 4), (1 5), (2 3), (2 4), (2 5), (3 4), (3 5), (4 5).

Кроме того, в S_5 имеется $(3-1)! \cdot C_5^3 = 2 \cdot 10 = 20$ циклов длины 3: (1 2 3), (3 2 1); (1 2 4), (4 2 1); (1 2 5), (5 2 1); (1 3 4), (4 3 1); (1 3 5), (5 3 1); (1 4 5), (5 4 1); (2 3 4), (4 3 2); (2 3 5), (5 3 2); (2 4 5), (5 4 2); (3 4 5), (5 4 3).

Еще имеется $(4-1)! \cdot C_5^4 = 3! \cdot 5 = 30$ циклов длины 4 (здесь в качестве упражнения их также можно выписать).

И, наконец, циклов длины 5 будет $4! \cdot C_5^5 = 24$. Получаем ответ: $10 + 20 + 30 + 24 = 84$.

г) Несложно проверить, что произведение двух совпадающих транспозиций есть тождественная подстановка («цикл длины 0»),

произведение транспозиций, пересекающихся по одному элементу есть цикл длины 3, а произведение непересекающихся транспозиций циклом не является.

Определение 6. Циклы с непересекающимися носителями называются *независимыми*.

Задача 9*. а) Докажите, что любая подстановка представляется в виде произведения независимых циклов.

б) Докажите, что любая подстановка представляется в виде произведения транспозиций.

в) Докажите, что любая подстановка из S_n представляется в виде произведения не более чем $n-1$ транспозиции.

г) Верно ли, что любая подстановка из S_n представляется в виде произведения независимых транспозиций?

Набросок решения. а) Утверждение этой задачи наглядно очевидно из графической записи подстановки.

Прежде чем переходить к формальному доказательству, следует разобрать несколько примеров, чтобы разобраться в том, что происходит. Рассмотрим, например, подстановку

$$a = \begin{pmatrix} 123456789 \\ 354978261 \end{pmatrix} = (1\,3\,4\,9)\cdot(2\,5\,7)\cdot(6\,8).$$

Теперь ясно как доказывать утверждение задачи в общем случае. Возьмем произвольный элемент (можно начать с единицы), и рассмотрим последовательность $1, a(1), a(a(1)), \ldots$ Эта последовательность обязательно замкнется, так как множество возможных значений конечно.

Тонкий момент: почему последний элемент перейдет в единицу (а не в какой-то другой элемент цепочки)? Это следует из того, что подстановка — *биективное* отображение.

Итак, подстановка a содержит замкнутый цикл $\{1, a(1), \ldots\}$. Возьмем теперь произвольный элемент b, не лежащий в этом цикле и рассмотрим последовательность $b, a(b), a(a(b)), \ldots$, которая даст еще один цикл, и так далее, пока вся подстановка не разобьется на циклы.

б) Нужно воспользоваться утверждением предыдущего пункта, после чего доказать, что любой цикл представим в виде произведения транспозиций (конечно, не являющихся независимыми).

Полезно рассмотреть какой-нибудь пример:

$$\begin{pmatrix} 123456789 \\ 641725938 \end{pmatrix} = (1\,6)\cdot(1\,5)\cdot(1\,2)\cdot(1\,4)\cdot(1\,7)\cdot(1\,9)\cdot(1\,8)\cdot(1\,3).$$

В общем случае $(i_1\,i_2 \ldots i_k) = (i_k\,i_{k-1})\ldots(i_3\,i_2)(i_2\,i_1)$.

в) Утверждение следует из предыдущих пунктов. Из пункта а) следует, что каждая подстановка из S_n представима в виде произведения независимых циклов, суммарная длина которых не превышает n. А каждый цикл длины n, в свою очередь, как следует из пункта б), представим в виде произведения $n-1$ транспозиции.

г) Неверно. Например, такая подстановка непредставима: $\begin{pmatrix}123\\231\end{pmatrix}$ (докажите это).

Метод математической индукции

листок 4 / октябрь 2004

Часто при попытке доказать утверждение для всех натуральных чисел появляются рассуждения, содержащие слова «и так далее». Формализовать такие рассуждения, а также отделить верные рассуждения такого вида от неверных позволяет метод математической индукции. При решении задач этого листка важно научиться применять этот метод и понять несколько тонких мест, возникающих при его применении. Несколько таких мест обсуждаются в задаче 7.

Только достаточно освоившись с использованием индукции, стоит вернуться к доказательству самого утверждения метода математической индукции. Отметим, что довольно часто сам этот принцип принимается без доказательства, как аксиома. Мы предпочитаем пользоваться аксиомой существования наименьшего элемента не столько потому, что она кажется интуитивно более очевидной, но, скорее, чтобы продемонстрировать еще один метод доказательства (по сути, впрочем, аналогичный индукции) — метод наименьшего контрпримера.

Соглашение. В этом листочке буквами m, n и k обозначены натуральные числа.

Аксиома наименьшего элемента. Каждое непустое подмножество множества натуральных чисел имеет наименьший элемент, т. е. элемент, который меньше любого другого элемента этого подмножества.

Задача 1. а) Останется ли предыдущее утверждение верным, если «множество натуральных чисел» заменить на «множество целых чисел»?

б) Останется ли предыдущее утверждение верным, если «наименьший элемент» заменить на «наибольший элемент»?

Решение. а) Ответ: нет. Действительно, рассмотрим множество целых чисел. Оно является своим подмножеством. От противного докажем, что в нем нет наименьшего элемента: пусть во множестве целых чисел есть наименьший элемент n. Но элемент $n-1$ также лежит во множестве целых чисел, и при этом он меньше, чем n. Получили противоречие.

б) Ответ: нет. Доказательство аналогично.

Задача 2. На острове Буяне все страны треугольной формы. Если две страны граничат, то по целой стороне. Докажите, что страны можно раскрасить в 3 цвета так, что соседние по стороне страны будут окрашены в разные цвета.

Решение. Воспользуемся аксиомой наименьшего элемента. Этот метод также носит название «метода наименьшего контрпримера». Пусть существует хотя бы один остров, не удовлетворяющий условию задачи, то есть такой, что его нельзя раскрасить требуемым способом. Выберем из всех таких островов остров B с наименьшим числом стран (если таких несколько — возьмем любой из них). Пусть число стран на B равно $n > 1$. Тогда для любого острова, на котором не больше $n - 1$ страны, утверждение задачи выполняется.

Возьмем страну, имеющую выход к морю, то есть граничащую с ним по крайней мере по одной стороне. Очевидно, у нее не более двух соседей. Теперь рассмотрим «остров», состоящий из всех стран на B, кроме этой страны. На нем меньше n стран, а значит, мы можем раскрасить их в 3 цвета так, что соседние по стороне страны будут окрашены в разные цвета. Остается только выбрать цвет для отброшенной нами страны. Если у нее один сосед, окрашенный в некоторый цвет, то мы просто красим эту страну в любой другой цвет и получаем нужную раскраску. Если соседних стран две, то мы красим нашу страну в оставшийся третий цвет и получаем требуемую раскраску.

Таким образом, предположение о существовании острова, страны которого невозможно раскрасить в 3 цвета, было неверным.

Принцип математической индукции. Пусть задана последовательность утверждений $A_1, A_2, \ldots, A_k, \ldots$, в которой:

1) (база индукции) первое утверждение истинно,

2) (шаг индукции) из истинности утверждения A_n следует истинность утверждения A_{n+1}.

Тогда все утверждения A_n истинны.

(Данным утверждением разрешается пользоваться без доказательства. Иногда это утверждение принимают за аксиому.)

Задача 3*. Докажите принцип математической индукции.

Вообще принцип индукции, будучи достаточно очевидным на первый взгляд, является довольно тонким и нетривиальным утверждением, часто постулируемым в качестве аксиомы. Мы докажем его ниже, используя аксиому о существовании наименьшего элемента.

Отметим, что интуитивно очевидное рассуждение

«Рассмотрим первое утверждение A_1. Оно по условию 1 истинно. Рассмотрим второе утверждение A_2. Его истинность следует из истинности первого утверждения (условие 2). Истинность третьего утверждения следует из истинности второго утверждения. И так далее до бесконечности.»

доказательством не является. Попытки его формализации упираются не только в «как бы» бесконечное время, необходимое для выписывания полного доказательства, но и в «замкнутый круг»: попытку использовать доказываемый принцип индукции, завуалированный словами «и так далее» или спрятанный в определение натуральных чисел.

Решение. От противного. Предположим, что не все утверждения истинны. Это означает, что множество индексов (номеров) ложных утверждений непусто. Заметим, что это подмножество множества натуральных чисел. Значит, по аксиоме (!) в нем есть наименьший элемент. То есть имеется такой номер n, что A_n ложно и ложных утверждений с меньшим номером нет. По условию 1 n не может быть равным 1. Поэтому в нашей последовательности утверждений имеется утверждение A_{n-1}. Так как A_n — самое первое ложное утверждение, A_{n-1} истинно. Но тогда по условию 2 мы получаем, что A_n истинно. Противоречие.

> **Задача 4.** На острове Буяне каждые два города соединены напрямую автомобильной либо железной дорогой. Докажите, что или из любого города в любой другой можно добраться на автомобиле, или из любого города в любой другой можно добраться на поезде.

Решение. База индукции. Если на острове Буяне есть всего один город, то утверждение задачи, очевидно, выполняется.

Шаг индукции. Предположим, что утверждение задачи выполнено для некоторого n. То есть если имеется n городов, то из любого города в любой другой можно добраться на автомобиле, или из любого города в любой другой можно добраться на поезде.

Пусть теперь имеется $n+1$ город. Выкинем из рассмотрения какой-нибудь один из них. По предположению мы знаем, что по оставшимся n городам можно проехать, используя лишь один вид транспорта. Пусть для определенности это автомобиль. Теперь рассмотрим коммуникации, соединяющие выкинутый нами $(n+1)$-й город со всеми остальными. Если все дороги, ведущие из него во все остальные — железные, то мы берем поезд и проезжаем по всей системе из $(n+1)$ города (транзитом через выкинутый нами). Если же есть хоть одна автомобильная дорога, ведущая в выкинутый город, то мы можем смело выбирать автомобиль и кататься по всей стране.

> **Задача 5.** Докажите, что части, на которые n прямых делят плоскость, всегда можно раскрасить в два цвета так, чтобы соседние части (то есть части, имеющие общий отрезок или луч) были окрашены в разные цвета.

Решение. База индукции. Рассмотрим случай $n=1$. Если у нас имеется всего одна прямая, то мы красим одну полуплоскость в один цвет (например, в черный), а другую — в другой (например, в белый).

Шаг индукции. Предположим, что утверждение задачи верно для *любых* n прямых. То есть как бы мы ни провели n прямых, мы можем раскрасить части, на которые они делят плоскость, так, чтобы соседние части были окрашены в разные цвета.

Рассмотрим плоскость, на которой проведена $n+1$ прямая. Выкинем любую из них и покрасим части, на которые делят плоскость оставшиеся прямые, в два цвета так, чтобы соседние части были окрашены в разные цвета (это мы можем сделать по предположению индукции). Теперь дорисуем выкинутую прямую и сделаем следующее: все точки, которые лежат с одной стороны от этой прямой, мы оставляем как есть, а у всех, которые лежат с другой стороны, меняем цвет на противоположный. Нетрудно видеть, что таким образом мы получаем раскраску плоскости с $(n+1)$-й прямой, удовлетворяющую условию задачи.

На примере этой в общем-то несложной задачи мы показываем, как работают с принципом математической индукции:

1) проверяют утверждение задачи для конкретного n (обычно, но не обязательно, для $n=1$),

2) предполагают, что утверждение задачи верно для некоторого n (это называют *предположением индукции*), и, используя его, доказывают утверждение задачи для $n+1$.

Задача 6. Докажите по индукции, что:

а) $1+\ldots+n=\frac{n(n+1)}{2}$; б) $1+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}$;

в) $1+\ldots+n^3=\frac{n^2(n+1)^2}{4}$.

Решение. а) База индукции. Рассмотрим случай $n=1$. Утверждение задачи примет вид $1=1$ — очевидно верное равенство.

Шаг индукции. Предположим, что утверждение задачи выполнено для некоторого n, то есть $1+\ldots+n=\frac{n(n+1)}{2}$. Докажем, что утверждение задачи выполнено для $n+1$, то есть

$$1+2+\ldots+(n+1)=(1+\ldots+n)+(n+1)=\frac{(n+1)((n+1)+1)}{2}. \qquad (1)$$

Действительно, по предположению индукции

$$1+\ldots+n=\frac{n(n+1)}{2}. \qquad (2)$$

Постараемся получить из этого равенства равенство (1). Прибавим к обеим частям (2) число $n+1$. Имеем

$$1+\ldots+n+(n+1)=\frac{n(n+1)}{2}+(n+1)=\frac{n(n+1)+2(n+1)}{2}=$$
$$=\frac{(n+1)(n+2)}{2}=\frac{(n+1)((n+1)+1)}{2}.$$

б) База индукции. $1=\frac{1(1\cdot 1+1)(2\cdot 1+1)}{6}$.

Шаг индукции. Предположим, что $1+\ldots+n^2=\frac{n(n+1)(2n+1)}{6}$. Тогда

$$1+\ldots+(n+1)^2=1+\ldots+n+(n+1)^2=\frac{n(n+1)(2n+1)}{6}+(n+1)^2=$$
$$=\frac{(n+1)(n+2)(2n+3)}{6}=\frac{(n+1)((n+1)+1)(2(n+1)+1)}{6}.$$

в) Доказывается аналогичной проверкой.

Задача 7. Найдите ошибку в следующих доказательствах.

а) Докажем, что $n>n+1$.

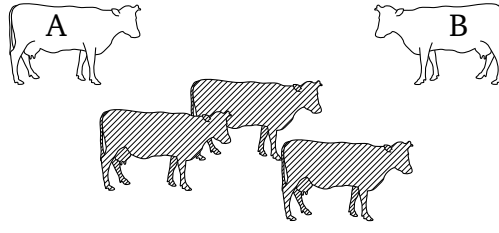
Действительно, пусть это утверждение верно для n, то есть $n>n+1$. Прибавив к обеим частям равенства единицу, мы получаем, что $(n+1)>(n+1)+1$, то есть верно утверждение для $n+1$.

б) Докажем, что в произвольном стаде из N коров все коровы одного цвета.

База индукции. В любом стаде из одной коровы все коровы, очевидно, одного цвета.

Шаг индукции. Предположим, что в любом стаде из N коров все коровы одного цвета. Докажем, что в любом стаде из $N+1$ коровы все коровы одного цвета.

Рассмотрим произвольное стадо из $N+1$ коровы. Возьмем в нем произвольную корову A. Оставшиеся N коров одного цвета. Теперь возьмем другую корову B. Оставшиеся N коров также одного цвета. В частности, A одного цвета со всеми коровами, кроме A и B, и B одного (того же!) цвета со всеми коровами, кроме A и B (см. рисунок). Значит, A, B, и вообще все коровы в стаде одного цвета.



в) В стране несколько городов, некоторые пары которых соединены дорогами, причем каждый город соединен хотя бы с одним другим. Докажем, что из любого города можно проехать в любой другой по дорогам. Будем доказывать индукцией по числу городов. База индукции для стран, состоящих из одного города, очевидна. Докажем шаг индукции. Возьмем какую-нибудь страну из n городов и добавим к ней еще один город. Между старыми городами можно проехать по старым дорогам, так что достаточно доказать, что из нового города можно проехать в любой из старых. По условию задачи из этого города ведет дорога в один из старых городов. Следовательно, из него можно доехать в один из старых городов, а оттуда уже добраться до любого другого. Итак, в новой стране тоже можно из любого города доехать до любого другого, и шаг индукции доказан.

Решение. а) Не проверена база индукции. При $n = 1$ получается очевидно неверное неравенство $1 > 2$.

б) Ошибка в шаге индукции. Приведенное рассуждение «проходит» для всех n, кроме $n = 2$. В этом случае $n - 2$ равно 0, и, убрав коров A и B, мы не оставим в стаде ни одной коровы. С другой стороны, если бы вдруг утверждение оказалось верным для $n = 2$, то несложно было бы показать, что оно верно для любого n.

в) Ошибка в шаге индукции. В приведенном рассуждении берется какая-то страна из n городов, и в ней строится новый город. Но при доказательстве шага индукции требуется доказать утверждение для любой страны из $n + 1$ города, а не только для стран, получающихся описанным выше способом. Например, страна, состоящая из четырех городов, в которой первый город соединен дорогой со вторым, а третий — с четвертым, не может быть получена из страны, удовлетворяющей условиям задачи, добавлением еще одного города.

Вообще, при доказательстве подобных утверждений по индукции следует взять какую-то страну из $n + 1$ города, построить по этой стране другую страну из n городов, применить для нее предположение индукции, и вывести из этого доказываемое утверждение для исходной страны. Поскольку доказываемое утверждение неверно, провести рассуждение такого вида в этом случае не получится.

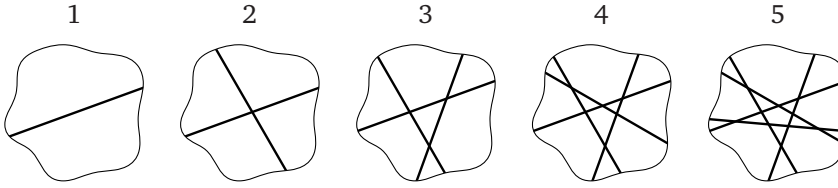
В этой задаче собраны наиболее частые ошибки, встречающиеся в неправильных рассуждениях по индукции. При этом достаточно часто исправить рассуждение просто, и поэтому отличие между правильным и неправильным рассуждением не видно. На примере этой задачи можно убедиться, что аналогичные аргументы могут привести к доказательству заведомо ложного утверждения.

Задача 8. На сколько частей делят плоскость n прямых в общем положении? (Говорят, что прямые находятся *в общем положении*, если никакие две из них не параллельны и никакие три не пересекаются в одной точке.)

Отметим, что, вообще говоря, не очевидно, что число частей, на которые делят плоскость n прямых в общем положении, не зависит от того, как проводить прямые. Найдя число частей, мы одновременно установим и этот факт.

Указание. Попробуйте нарисовать картинку для случаев $n=1, 2, 3, 4, 5$, угадать формулу, а потом доказать ее по индукции.

Решение. Попробуем угадать ответ. Для этого нарисуем картинки для $n=1, 2, 3, 4, 5$ и запишем результат в таблицу (отметим, что мы пока не утверждаем, что невозможен другой случай для, скажем, $n=4$).

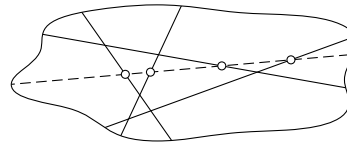


Получаются числа 2, 4, 7, 11, 16. Заметим, что эти числа удовлетворяют условию $a_n = a_{n-1} + n$. Тогда (по задаче 6а) n прямых в общем положении делят плоскость на $\frac{n(n+1)}{2}+1$ часть. Теперь докажем полученное утверждение методом математической индукции.

База индукции. Для одной прямой получаем число частей $1+1=2$. Все верно.

Шаг индукции. Предположим, что *любые* n прямых в общем положении делят плоскость на $\frac{n(n+1)}{2}+1$ часть.

Рассмотрим $n+1$ прямую в общем положении. Уберем одну из них. Оставшиеся n прямых по предположению индукции делят плоскость на $\frac{n(n+1)}{2}+1$ часть. Так как никакие две прямые не параллельны и никакие три не пересекаются в одной точке, убранная прямая делится n точками пересечения с остальными прямыми на два луча и $n-1$ отрезок.



Заметим, что каждый из этих лучей и отрезков делит некоторую часть плоскости на две. То есть при добавлении одной прямой число частей увеличивается на $n+1$. Значит, $n+1$ прямая делит плоскость на

$$\frac{n(n+1)}{2}+1+(n+1)=\frac{(n+1)(n+2)}{2}+1=\frac{(n+1)((n+1)+1)}{2}+1$$

частей.

Задача 9. Докажите, что:
а) $2^{5n+3}+5^n\cdot 3^{n+2}$ делится на 17; б) $n^{2m-1}+1$ делится на $n+1$;
в*) $2^{3^n}+1$ делится на 3^{n+1}.

Решение. а) База индукции. $2^{5\cdot 1+3}+5^1\cdot 3^{1+2}=256+135=391=$ $=23\cdot 17$.

Шаг индукции. Пусть утверждение справедливо для некоторого n, тогда докажем, что оно будет справедливо и для $n+1$:

$$2^{5(n+1)+3}+5^{n+1}\cdot 3^{(n+1)+2}=2^5\cdot 2^{5n+3}+5\cdot 5^n\cdot 3\cdot 3^{n+2}=$$
$$=32\cdot 2^{5n+3}+5\cdot 5^n\cdot 3\cdot 3^{n+2}=(15+17)\cdot 2^{5n+3}+15\cdot 5^n\cdot 3^{n+2}=$$
$$=17\cdot 2^{5n+3}+15(2^{5n+3}+5^n\cdot 3^{n+2}).$$

Первое слагаемое, очевидно, делится на 17. А второе слагаемое делится на 17 по предположению индукции.

б) В этой задаче на первый взгляд непонятно, по какой переменной мы должны вести индукцию: по n или по m? Изложим доказательство, использующее индукцию по m.

База индукции. $n^{2\cdot 1-1}+1=n+1$ делится на $n+1$.

Шаг индукции. Предположим, что формула верна для некоторого m. Докажем тогда, что она будет верна также, если мы везде вместо m подставим $m+1$:

$$n^{2(m+1)-1}+1=n^2\cdot n^{2m-1}+1=n^2\cdot((n^{2m-1}+1)-1)+1=$$
$$=n^2\cdot(n^{2m-1}+1)+1-n^2=n^2\cdot(n^{2m-1}+1)+(1-n)(1+n).$$

Полученное произведение делится на $n+1$, так как первое слагаемое делится на $n+1$ по предположению индукции.

Задача 10 (неравенство Бернулли). Докажите, что если $a > -1$, то

$$(1+a)^n \geqslant 1+na.$$

Решение. База индукции. При $n=1$ имеем: $1+a \geqslant 1+a$ — верно.

Шаг индукции. Пусть неравенство Бернулли выполнено для некоторого n. Докажем тогда, что оно выполняется и для $n+1$: $(1+a)^{n+1} = (1+a)(1+a)^n = (1+a)^n + a(1+a)^n$. По предположению индукции имеем $(1+a)^n \geqslant 1+na$. Кроме того, $a(1+a)^n \geqslant a$, так как $a > -1$ (аккуратно докажите это!). Отсюда получаем:

$$(1+a)^{n+1} \geqslant 1+na+a = 1+a(n+1).$$

Это неравенство демонстрирует, что показательная функция растет быстрее линейной. Хотя эта оценка довольно грубая, она является мощным средством доказательства неравенств.

Задача 11. Докажите, что:

а) $2^n > n$; б) $2^n > n^2$ при $n > 4$; в) $n! > 2^n$ при $n > 3$;

г*) существует такое k, что $2^n > n^{2004}$ при всех $n > k$.

Решение. База индукции проверяется прямым вычислением. Докажем шаг индукции.

а) $2^n > n$, $2^n > 1$, значит, $2^{n+1} = 2^n + 2^n > n+1$.

б) $2^n > n^2$, $2^n > 2n+1 \Rightarrow 2^n \cdot 2 > n^2 + 2n + 1 \Rightarrow 2^{n+1} > (n+1)^2$.

в) $n! > 2^n$, $n+1 > 2 \Rightarrow (n+1)! > 2^{n+1}$.

Задача 12. Вершины выпуклого многоугольника раскрашены ровно в три цвета так, что никакие две соседние вершины не окрашены в один цвет. Докажите, что многоугольник можно разбить диагоналями на треугольники так, чтобы у каждого треугольника вершины были трех разных цветов.

Решение. База — утверждение для треугольника — очевидна.

Пусть для всех многоугольников с n вершинами утверждение задачи доказано; докажем его для произвольного $(n+1)$-угольника. Докажем сначала, что в нем найдутся три подряд идущие вершины разных цветов. Действительно, в противном случае какие-то два цвета чередуются вдоль всего многоугольника, и вершины на самом деле раскрашены в два цвета, что противоречит условию задачи.

Назовем цвет, в который окрашена средняя из этих вершин, красным. Если среди остальных вершин есть хотя бы одна красная вершина, достаточно отрезать треугольник, образованный тремя найденными вершинами, и разрезать оставшийся многоугольник по предположению индукции. Иначе достаточно провести все диагонали, выходящие из единственной красной вершины.

Обобщенный принцип математической индукции. Пусть задана последовательность утверждений $A_1, A_2, \ldots, A_k, \ldots$ Известно, что:

1) (база индукции) первое утверждение истинно,

2) (шаг индукции) из истинности утверждений $A_1, A_2, \ldots, A_n$ следует истинность утверждения A_{n+1}.

Тогда все утверждения истинны.

Задача 13*. Докажите обобщенный принцип математической индукции.

Решение. Достаточно заметить, что обобщенный принцип математической индукции для последовательности утверждений A_k в точности совпадает с принципом математической индукции для последовательности утверждений B_k: «утверждения $A_1, \ldots, A_k$ верны».

Задача 14. Докажите, что если $a + \frac{1}{a}$ целое, то $a^k + \frac{1}{a^k}$ целое при любом k.

Решение. Для доказательства задачи воспользуемся обощенным принципом математической индукции.

База индукции. При $k = 1$ утверждение очевидно.

Шаг индукции. Пусть $a + \frac{1}{a}$ целое, и $a^k + \frac{1}{a^k}$ целое для всех k, не превосходящих K (в частности, для $k = K$ и для $k = K - 1$). Докажем тогда, что и $a^{K+1} + \frac{1}{a^{K+1}}$ будет целым. Рассмотрим равенство:

$$\left(a + \frac{1}{a}\right) \cdot \left(a^K + \frac{1}{a^K}\right) = \left(a^{K+1} + \frac{1}{a^{K+1}}\right) + \left(a^{K-1} + \frac{1}{a^{K-1}}\right).$$

Левая часть — целое число, так как она является произведением целых чисел (они целые по предположению). В правой части число, записанное во вторых скобках, также является целым по предположению индукции. Значит, число в первых скобках тоже целое.

Задача 15*. В классе каждый болтун дружит хотя бы с одним молчуном. При этом болтун молчит, если в кабинете находится нечетное число его друзей-молчунов. Докажите, что учитель может выгнать из класса не более половины учеников так, чтобы все болтуны молчали.

Решение. Будем называть группу школьников этого класса «молчаливой», если после удаления из класса остальных школьников все болтуны этой группы молчат. Заметим, что в задаче фактически требуется найти «молчаливую» группу школьников, содержащую не менее половины класса.

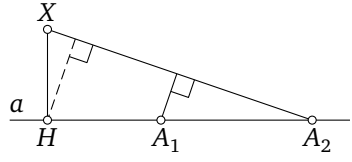
Воспользуемся обобщенным принципом математической индукции. База индукции для $n = 3$ очевидна.

Шаг индукции. Предположим, что утверждении задачи выполнено для любого класса, в котором не более N человек. Рассмотрим класс, в котором $N+1$ человек. Если в классе ровно один молчун, то класс уже молчит, и никого выгонять не надо. Пусть теперь в классе хотя бы два молчуна. Назовем одного из них Саша. Пусть с Сашей дружит k человек. По предположению индукции, среди остальных $N-k$ учеников найдется «молчаливая» группа M не менее чем из $\frac{N-k}{2}$ учеников. Если не менее $\frac{k+1}{2}$ Сашиных друзей дружат с нечетным количеством молчунов из M, то можно добавить их к M и получить «молчаливую» группу, состоящую как минимум из $\frac{N-k}{2}+\frac{k+1}{2}=\frac{N+1}{2}$ учеников. Если же менее $\frac{k+1}{2}$ Сашиных друзей дружат с нечетным количеством молчунов из M, то можно добавить к M остальных Сашиных друзей и Сашу, и получить «молчаливую» группу, состоящую как минимум из $\frac{N-k}{2}+\left[\frac{k+1}{2}\right]+1\geqslant\frac{N+1}{2}$ учеников.

Задача 16* (Задача Сильвестра). На плоскости взяты несколько точек так, что на каждой прямой, соединяющей любые две из них, лежит по крайней мере еще одна точка. Докажите, что все точки лежат на одной прямой.

У этой задачи имеется очевидно — но неверное! — решение по индукции в духе рассуждения 7 в).

Решение. Предположим обратное. Проведем прямую через каждую пару отмеченных точек. Среди всех пар (точка нашего множества, проведенная прямая) выберем пару (X, a) с наименьшим ненулевым расстоянием между ними.



Опустим из X на a перпендикуляр XH. Так как на каждой проведенной прямой лежат минимум три точки нашего множества, с какой-то стороны от H на прямой a лежат хотя бы две точки множества — A_1 и A_2 (A_1 между H и A_2). Но расстояние от A_1 до прямой XA_2 меньше отрезка XH (оно меньше даже расстояния от H до XA_2), что противоречит выбору X и a.

Задача 17*. Докажите, что $n^{n+1} > (n+1)^n$ при $n > 2$.

Решение. База легко проверяется, докажем шаг. Пусть для n неравенство верно, а для $n+1$ нет, то есть

$$n^{n+1} > (n+1)^n \quad \text{и} \quad (n+1)^{n+2} \leqslant (n+2)^{n+1}.$$

Перемножая эти неравенства, получаем

$$(n+1)^{2n+2} = ((n+1)^2)^{n+1} < ((n+2)n)^{n+1},$$

что неверно.

Комбинаторика 2. Бином Ньютона

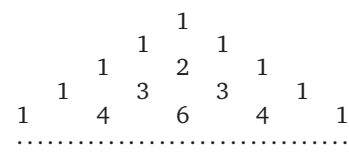
листок 5 / октябрь 2004

В этом листке изучаются биномиальные коэффициенты и соотношения между ними. Для биномиальных коэффициентов дается два определения: рекурсивное, через треугольник Паскаля, и комбинаторное, через число подмножеств (а позже в листке появляются и другие интерпретации). Из-за этого большинство задач имеет минимум два решения — формальное доказательство по индукции через рекурсивное определение и комбинаторное доказательство, объясняющее, почему левая и правая часть равенства соответствуют двум способам подсчета числа каких-то объектов. А возникающий в конце листка бином Ньютона дает третий метод доказательства, развитием которого является метод производящих функций. Все это учит, в частности, работать с объектами, имеющими несколько различных определений, используя в каждый момент наиболее удобное. (Тем не менее, полезно иногда попросить школьника, решившего задачу через одно из определений, попытаться придумать решение и через другое определение.)

Таким образом, в листке обсуждаются два метода решения комбинаторных задач из трех основных (еще один — выписывание всех вариантов и учет повторов — обсуждается в листке «Комбинаторика 1»): 1) рекурсивное вычисление с доказательством по индукции, 2) установление биекции между двумя множествами.

Вообще, установление биекций между множествами «комбинаторной природы», наравне с нахождением числа элементов, является одной из основных задач комбинаторики. Это связно, в частности, с тем, что при нахождении числа элементов множества промежуточные шаги часто можно интерпретировать как построение биекций, сводящих, в конце концов, задачу к вычислению числа элементов какого-нибудь простого множества (отличный пример такой задачи — теорема Кэли из листка «Теория графов 2»). Такой план часто оказывается проще преобразования алгебраических выражений.

Определение 1. *Треугольником Паскаля* называется треугольная таблица, составленная из чисел по следующему правилу: строка с номером n состоит из n чисел, первое и последнее числа каждой строки равны единице, а каждое из остальных чисел равно сумме двух ближайших к нему чисел предыдущей строки. Число, стоящее на $(k+1)$-м месте $(n+1)$-й строки, обозначается $\binom{n}{k}$.



Здесь полезно задать простые вопросы в стиле «Чему равно $\binom{5}{3}$, $\binom{4}{2}$?».

Задача 1. Запишите в виде $\binom{a}{b}$ числа предыдущей строки, ближайшие к числу $\binom{n}{m}$.

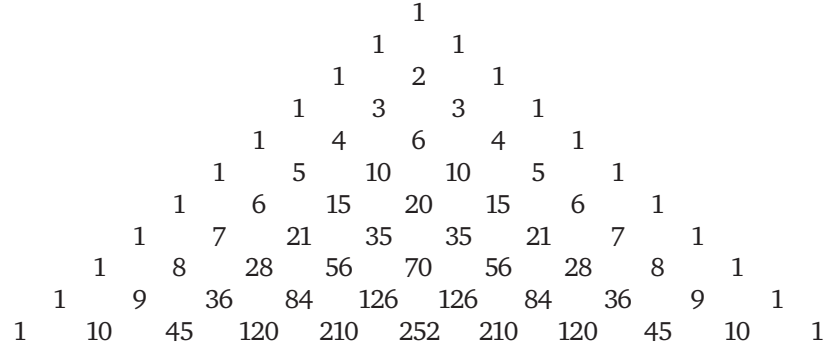
Решение. Число $\binom{n}{m}$ стоит на $(m+1)$-м месте $(n+1)$-й строки. Ближайшие к нему числа предыдущей строки стоят на m-м и $(m+1)$-м местах n-й строки, то есть имеют вид $\binom{n-1}{m}$ и $\binom{n-1}{m-1}$.

Ответ. $\binom{n-1}{m}$ и $\binom{n-1}{m-1}$.

Таким образом, имеет место соотношение $\binom{n}{m}=\binom{n-1}{m}+\binom{n-1}{m-1}$.

Задача 2. Выпишите первые 11 строк треугольника Паскаля.

Ответ.



Задача 3. Докажите, что $\binom{n}{k}=\binom{n}{n-k}$.

Решение. Заметим, что в задаче фактически требуется доказать, что треугольник Паскаля симметричен. Так как первые две строки треугольника Паскаля симметричны и правило построения следующей

строки сохраняет симметрию, все остальные строки будут симметричны.

Более формально. Докажем индукцией по n следующую последовательность утверждений A_n: «Для любого целого $0 \leqslant k \leqslant n$ выполнено равенство $\binom{n}{k} = \binom{n}{n-k}$».

База индукции. При $n = 1$ надо доказать, что $\binom{1}{0} = \binom{1}{1}$, а это верно: оба числа равны 1.

Шаг индукции. Пусть A_n верно. Докажем A_{n+1}. Для $k = 0$ и $k = n+1$ по определению треугольника Паскаля $\binom{n+1}{k} = \binom{n+1}{n+1-k} = 1$. Осталось доказать для $1 \leqslant k \leqslant n$. Для таких k

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} = \binom{n}{n-k} + \binom{n}{n-k+1} = \binom{n+1}{n-k+1}.$$

Решение 2. По задаче 4 $\binom{n}{k}$ равно числу способов пройти из левого нижнего угла прямоугольника $(n-k) \times k$ в правый верхний, идя только вверх или вправо, а $\binom{n}{n-k}$ — аналогичному числу для прямоугольника $k \times (n-k)$. Но эти числа равны из-за симметрии.

> **Задача 4.** Докажите, что число способов пройти из левого нижнего угла прямоугольника $m \times n$ в правый верхний, двигаясь только вверх или вправо по границам клеток, равно $\binom{n+m}{m}$.

Решение. Обозначим число способов пройти из левого нижнего угла прямоугольника $m \times n$ в правый верхний указанным способом через $C(m, n)$ (прямоугольником $n \times 0$ считаем отрезок длины n).

Поскольку в любой узел сетки можно попасть либо снизу, либо слева, то $C(m, n) = C(m-1, n) + C(m, n-1)$. Кроме того, заметим, что $C(n, 0) = C(0, n) = 1$. Будем писать в узлах сетки числа $C(m, n)$. Повернув получившуюся таблицу на 135° по часовой стрелке, получим новую таблицу, которая строится по тому же правилу, что и треугольник Паскаля. Следовательно, эта таблица совпадает с треугольником Паскаля.

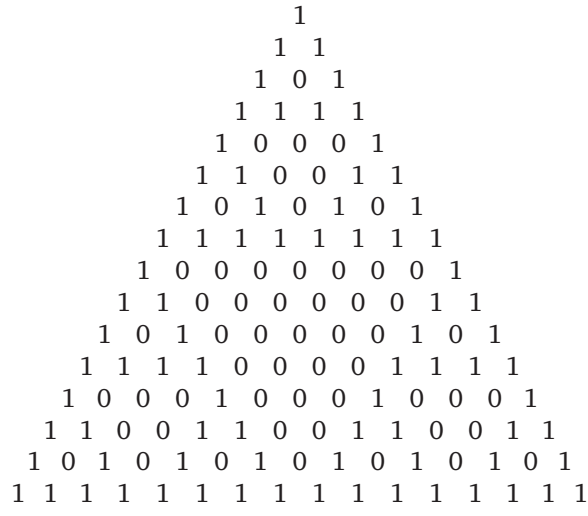
У этой задачи есть другое решение индукцией по $m+n$, на примере которого школьников можно учить аккуратно записывать рассуждения «по индукции», относящиеся к биномиальным коэффициентам.

> **Задача 5.** В каких строках треугольника Паскаля все числа нечетные?

Ответ. В строках с номерами вида 2^n.

Указание. Треугольник Паскаля «по модулю 2» получается из обычного заменой всех четных чисел на 0, а нечетных — на 1. Выпишите первые 16 строк этого треугольника. (Как по уже выписанной строке этого треугольника построить следующую?)

Решение. Рассмотрим треугольник Паскаля «по модулю 2», то есть треугольник, который получается из треугольника Паскаля заменой всех четных чисел на нули, а нечетных на единицы. Заметим, что такой треугольник может быть получен способом, аналогичным определению треугольника Паскаля, только с таблицей сложения $0+0=1+1=0$, $0+1=1+0=1$.



Рассмотрим последовательность утверждений A_n: *В 2^n-й строке треугольника Паскаля «по модулю 2» все числа — единицы, а при $2^{n-1}<k<2^n$ в k-й строке есть нуль.*

База. $n=0$. Очевидно.

Шаг индукции. Пусть утверждение A_n верно. Докажем утверждение A_{n+1}. Заметим, что в (2^n+1)-й строке первое и последнее числа — единицы, а остальные — нули. Следовательно, при $2^n<k\leqslant 2^{n+1}$ k-я строка устроена следующим образом: слева и справа $(k-2^n)$-я строка, а между ними нули (упражнение: доказать индукцией по k). При этом в 2^{n+1}-й строке будут только единицы (2^n единиц справа, 2^n слева, нулям места не хватает). Шаг индукции доказан.

Определение 2. *Числом сочетаний из n по m* называется количество m-элементных подмножеств множества из n элементов. Обозначение: C_n^m.

Другими словами, C_n^m — это число способов выбрать m предметов из n различных предметов. Существенно, что порядок выбора не имеет значения.

Задача 6. Найдите: а) C_{100}^1, б) C_4^2, в) C_5^2, г) C_6^4.

Ответ. а) $C_{100}^1 = 100$; б) $C_4^2 = 6$; в) $C_5^2 = 10$; г) $C_6^4 = 15$.

Решение. Перечислим все подмножества, число которых надо найти.

а) $\{1\}, \ldots, \{100\}$.

б) $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$.

в) Двухэлементное подмножество множества $\{1, 2, 3, 4, 5\}$ либо содержит число 5, либо не содержит. Если подмножество не содержит число 5, то оно является подмножеством множества $\{1, 2, 3, 4\}$. Двухэлементных подмножеств множества $\{1, 2, 3, 4\}$ ровно 6 (см. предыдущий пункт). Остальных подмножеств четыре: $\{1, 5\}$, $\{2, 5\}$, $\{3, 5\}$, $\{4, 5\}$.

г) Когда мы выбираем из множества $\{1, 2, 3, 4, 5, 6\}$ четыре элемента, остается два невыбранных элемента. При этом каждая пара невыбранных элементов однозначно определяет четверку выбранных (все остальные элементы), и наоборот. Следовательно, подмножеств из четырех элементов столько же, сколько и пар.

Итак, достаточно выписать все двухэлементные подмножества множества $\{1, 2, 3, 4, 5, 6\}$. Аналогично предыдущему пункту, мы получим все двухэлементные подмножества множества $\{1, 2, 3, 4, 5\}$ и еще пять: $\{1, 6\}$, $\{2, 6\}$, $\{3, 6\}$, $\{4, 6\}$, $\{5, 6\}$.

Как выписать все варианты, не забыв ни одного и не посчитав ни один вариант дважды, обсуждается в листке «Комбинаторика 1».

Задача 7. Докажите, что: а) $C_n^k = C_n^{n-k}$; б) $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$.

Пункт б) — это ключевое место при доказательстве равенства $C_n^m = \binom{n}{m}$.

Указание. а) Если взяли k элементов, сколько элементов осталось?

б) Покрасьте один элемент в красный цвет и посчитайте отдельно число подмножеств, содержащих красный элемент и не содержащих его.

Решение. а) Каждому k-элементному подмножеству соответствует $(n-k)$-элементное подмножество, состоящее из элементов, не принадлежащих данному подмножеству, и наоборот.

б) Покрасим один элемент в красный цвет, а остальные — в синий. Тогда все m-элементные подмножества разобьются на два класса: множества, содержащие красный элемент, и множества, не содержащие его. Заметим, что m-элементное подмножество, не содержащее красный элемент, — это в точности m-элементное подмножество $(n-1)$-элементного множества синих элементов. Следовательно, таких подмножеств ровно C_{n-1}^{m-1}. Аналогично, m-элементное подмножество, содержащее красный элемент, — это объединение множества, состоящего из красного элемента, и $(m-1)$-элементного подмножества множества синих элементов. Следовательно, таких подмножеств C_{n-1}^{m-1}. Итак, $C_n^m = C_{n-1}^m + C_{n-1}^{m-1}$.

Задача 8. Докажите, что $\binom{n}{k} = C_n^k$.

Решение. Докажем индукцией по n следующую последовательность утверждений A_n: «Для любого целого k, такого что $0 \leqslant k \leqslant n$, выполнено равенство $\binom{n}{k} = C_n^k$.»

База индукции очевидна.

Шаг индукции. Пусть утверждение A_n верно. Докажем утверждение A_{n+1}. Если $k \in \{0, n+1\}$, то $\binom{n+1}{k} = 1 = C_{n+1}^k$. Иначе $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} = C_n^k + C_n^{k-1} = C_{n+1}^k$. Первое равенство выполнено в силу определения треугольника Паскаля, второе — по предположению индукции, а третье — по задаче 7 б). Утверждение задачи доказано.

Задача 9. Раскройте скобки в выражении: а) $(a+b)^3$; б) $(a+b)^4$; в) $(2a+3b)^4$.

Есть разные способы раскрытия скобок. Один — последовательное раскрытие скобок. Другой: выписываем все скобки, после чего пишем сумму произведений вида «по одному сомножителю из каждой скобки».

Решение. а) $(a+b)^3 = (a+b)(a+b)(a+b) = (a^2+ab+ba+b^2)(a+b) = (a^2+2ab+b^2)(a+b) = a^3+a^2b+2a^2b+2ab^2+ab^2+b^3 = a^3+3a^2b+3ab^2+b^3$.

б) $(a+b)^4 = (a+b)^3(a+b) = (a^3+3a^2b+3ab^2+b^3)(a+b) = a^4+a^3b+3a^3b+3a^2b^2+3a^2b^2+3ab^3+ab^3+b^4 = a^4+4a^3b+6a^2b^2+4ab^3+b^4$.

в) $(2a+3b)^4 = (2a)^4 + 4(2a)^3\cdot 3b + 6(2a)^2(3b)^2 + 4\cdot 2a(3b)^3 + (3b)^4 = 16a^4 + 96a^3b + 216a^2b^2 + 216ab^3 + 81b^4$.

Решение 2. а) $(a+b)^3 = aaa + aab + aba + abb + baa + bab + bba + bbb = a^3 + 3a^2b + 3ab^2 + b^3$.

б) $(a+b)^4 = aaaa + aaab + aaba + aabb + abaa + abab + abba + abbb + baaa + baab + baba + babb + bbaa + bbab + bbba + bbbb = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4$.

Задача 10 (бином Ньютона). а) Раскройте скобки в выражениях $(a+b)$, $(a+b)^2$, $(a+b)^3$, $(a+b)^4$ и выпишите результаты друг под другом. Заметьте, что коэффициенты образуют треугольник Паскаля.

б) Докажите, что

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}b^n.$$

Указание. б) В каком количестве слагаемых при раскрытии скобок в произведении $(a+b)\ldots(a+b)$ получается член $a^{n-k}b^k$?

Решение. б) Раскроем скобки в произведении $(a+b)\ldots(a+b)$. Каждому слагаемому соответствует подмножество скобок, в которых была выбрана буква b. Следовательно, слагаемых вида $a^{n-k}b^k$ будет ровно $C_n^k = \binom{n}{k}$. Значит, после приведения подобных слагаемых мы получим в точности правую часть доказываемого равенства.

Решение 2. б) Докажем это утверждение индукцией по n.

База индукции $n=1$ очевидна.

Шаг индукции. Пусть при $n=N$ утверждение верно. Докажем его при $n=N+1$.

$$(a+b)^{N+1} = (a+b)(a+b)^N = (a+b)\left(\binom{n}{0}a^n + \ldots + \binom{n}{n}b^n\right) =$$
$$= \binom{n}{0}a^{n+1} + \left(\binom{n}{0} + \binom{n}{1}\right)a^nb + \ldots + \left(\binom{n}{n-1} + \binom{n}{n}\right)ab^n + \binom{n}{n}b^{n+1}.$$

Осталось воспользоваться тем, что $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Задача 11. Докажите, что:

а) $\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{n} = 2^n$;

б) $\binom{n}{0} - \binom{n}{1} + \ldots + (-1)^n\binom{n}{n} = 0$.

Решение. Подставив в бином Ньютона $a=1$, $b=1$, получим утверждение пункта а), а подставив $a=1$, $b=-1$, получим утверждение пункта б).

Решение 2. а) По определению треугольника Паскаля, каждое число следующей строки есть сумма двух чисел предыдущей строки. При этом каждое число предыдущей строки вносит свой «вклад» ровно в два числа следующей строки. Поэтому сумма чисел следующей строки в два раза больше суммы чисел предыдущей строки. Дальнейшее рассуждение оставляем читателю в качестве упражнения.

б) Подставим в левую часть всюду $\binom{n-1}{k}+\binom{n-1}{k-1}$ вместо $\binom{n}{k}$. Осталось заметить, что при этом каждое из чисел предыдущей строки встретится один раз со знаком «+» и один раз со знаком «−».

Решение 3. а) Найдем двумя способами количество подмножеств n-элементного множества. С одной стороны, оно равно сумме количеств k-элементных подмножеств по $0 \leqslant k \leqslant n$, то есть левой части доказываемого тождества. С другой стороны, таких подмножеств 2^n.

б) Перенесем слагаемые со знаком «−» в правую часть равенства:

$$\binom{n}{0}+\binom{n}{2}+\ldots=\binom{n}{1}+\binom{n}{3}+\ldots$$

Заметим, что в левой части равенства стоит число подмножеств n-элементного множества, состоящих из четного числа элементов, а в правой — из нечетного. Таким образом, в задаче требуется доказать, что количество подмножеств, состоящих из четного числа элементов, равно количеству подмножеств, состоящих из нечетного числа элементов. Фиксируем какой-то элемент a. Поставим в соответствие множествам, не содержащим этот элемент, их объединение с множеством $\{a\}$, а множествам, содержащим этот элемент, — их разность с $\{a\}$. Заметим, что при этом каждому подмножеству из четного числа элементов поставлено в соответствие подмножество из нечетного числа элементов, и наоборот. При этом разным подмножествам поставлены в соответствие разные. Следовательно, подмножеств из четного числа элементов столько же, сколько из нечетного.

Постройте явно это отображение для множества всех подмножеств множества из трех элементов.

Задача 12. Докажите, что $\binom{n}{k}=\frac{n!}{k!(n-k)!}$.

Указание. Найдите сначала число *упорядоченных* k-элементных подмножеств n-элементного множества.

Решение. Найдем сначала число способов выбрать *упорядоченный* k-элементный набор из n-элементного множества. Первый элемент можно выбрать n способами; для каждого из этих способов

существует $(n-1)$ способ выбора второго элемента (так как выбранный первым элемент уже выбирать нельзя); для каждого выбора первых двух элементов существует ровно $(n-2)$ способа выбрать третий и т. д. Следовательно, способов такого выбора ровно $n(n-1)\ldots(n-k+1)=\frac{n!}{(n-k)!}$. Осталось заметить, что из каждого неупорядоченного k-элементного набора можно получить ровно $k!$ упорядоченных.

Решение 2. Докажем индукцией по n следующую последовательность утверждений A_n: «Для любого целого $0\leqslant k\leqslant n$ выполнено равенство $\binom{n}{k}=\frac{n!}{k!(n-k)!}$.»

База индукции очевидна.

Шаг индукции. Пусть A_n верно. Докажем A_{n+1}. Для $k\in\{0, n+1\}$ получаем $\binom{n+1}{k}=1=\frac{(n+1)!}{0!(n+1)!}=\frac{(n+1)!}{k!(n+1-k)!}$. Пусть теперь $0<k<n+1$. Тогда

$$\binom{n+1}{k}=\binom{n}{k}+\binom{n}{k-1}=\frac{n!}{k!(n-k)!}+\frac{n!}{(k-1)!(n-k+1)!}=$$
$$=\frac{n!((n-k+1)+k)}{k!(n-k+1)!}=\frac{(n+1)!}{k!(n-k+1)!}.$$

Шаг индукции доказан. Следовательно, все утверждения A_n верны.

Задача 13. Докажите, что:

а) $\binom{n}{0}^2+\binom{n}{1}^2+\ldots+\binom{n}{n}^2=\binom{2n}{n}$;

б) $\binom{n}{0}+\binom{n+1}{1}+\ldots+\binom{n+k-1}{k-1}+\binom{n+k}{k}=\binom{n+k+1}{k}$;

в) $\binom{n}{1}+2\binom{n}{2}+\ldots+n\binom{n}{n}=n\cdot 2^{n-1}$;

г) $\binom{n}{k}\cdot\binom{n-k}{m-k}=\binom{m}{k}\cdot\binom{n}{m}$.

Указание. а) Воспользуйтесь задачей 3.

Решение. $B=\{1, 2, \ldots, 2n\}$, $A_1=\{1, 2, \ldots, n\}$ и $A_2=\{n+1, \ldots, 2n\}$. Каждому n-элементному подмножеству X множества B поставим в соответствие два подмножества: $X\cap A_1$ и $X\cap A_2$. Заметим, что мы получили биекцию между множеством всех n-элементных подмножеств множества B и множеством пар подмножеств множеств A_1 и A_2, сумма количеств элементов в которых равна n. Следовательно,

$$\binom{2n}{n}=\binom{n}{0}\binom{n}{n}+\binom{n}{1}\binom{n}{n-1}+\ldots+\binom{n}{n}\binom{n}{0}.$$

Осталось воспользоваться тем, что $\binom{n}{k}=\binom{n}{n-k}$.

а) Разобьем все k-элементные подмножества множества $\{1, 2, \ldots, n+k+1\}$ на классы подмножеств, содержащих все числа от 1 до l, но не содержащих число $l+1$. Например, подмножества, не содержащие единицу, будут отнесены при этом в класс A_0; подмножества, содержащие 1, но не содержащие 2, — в класс A_1, и т. д.

Найдем количество подмножеств, попавших в класс A_l. Все такие подмножества содержат числа $\{1, \ldots, l\}$ и еще $k-l$ чисел из множества $\{l+2, \ldots, n+k+1\}$. Следовательно, всего таких подмножеств $\binom{n+k-l}{k-l}$. Отсюда следует доказываемое равенство.

б) Найдем двумя способами количество подмножеств множества $\{1, 2, \ldots, n\}$ с одним отмеченным элементом. С одной стороны, мы можем сначала выбрать подмножество, а затем в нем выбирать отмеченный элемент. Если мы выбрали k-элементное подмножество, то отмеченный элемент в нем можно выбрать k способами. Следовательно, число способов выбрать k-элементное подмножество с одним отмеченным элементом равно $k\binom{n}{k}$. Суммируя по всем k, получаем левую часть доказываемого равенства.

С другой стороны, можно сначала выбрать отмеченный элемент, а потом выбирать содержащее его множество. Отмеченный элемент можно выбрать n способами. При любом выборе отмеченного элемента подмножеств, содержащих его, будет ровно 2^{n-1}. Следовательно, искомое число способов равно правой части доказываемого равенства.

в) Найдем двумя способами количество способов в n-элементном множестве выбрать непересекающиеся k-элементное и $(m-k)$-элементное подмножества. С одной стороны, мы можем выбрать сначала первое подмножество, а потом из оставшихся элементов выбрать второе подмножество. При этом способе получаем, что искомое число равно левой части доказываемого равенства.

С другой стороны, можно сначала выбрать объединение этих подмножеств, а потом из элементов объединения выбрать первое множество. При этом способе получаем, что искомое число равно правой части доказываемого равенства.

Решение 2. а) По задаче 4 $\binom{2n}{n}$ равно числу способов пройти из левого нижнего угла квадрата $n \times n$ в правый верхний, идя только вверх и вправо. Каждый из таких путей ровно один раз пересекает диагональ, соединяющую левый верхний угол с правым нижним. Рассмотрим множество путей, пересекающих эту диагональ в k клетках от левого верхнего угла.

По задаче 4 число способов добраться из левого нижнего угла квадрата в точку пересечения равно $\binom{n}{k}$, а число способов добраться из точки пересечения в правый верхний угол равно $\binom{n}{n-k}$, что тоже равно $\binom{n}{k}$. Следовательно, число путей, пересекающих диагональ в k клетках от левого верхнего угла, равно $\binom{n}{k}^2$. Таким образом, общее число путей равно левой части доказываемого равенства. Но оно же равно и правой части.

б) Будем доказывать утверждение задачи индукцией по k. База индукции $k=1$ следует из определения треугольника Паскаля.

Докажем шаг индукции. Пусть для $k-1$ утверждение задачи верно. Докажем его для k. По определению треугольника Паскаля $\binom{n+k+1}{k}=\binom{n+k}{k}+\binom{n+k}{k-1}$. По предположению индукции $\binom{n+k}{k-1}=$ $=\binom{n+k-1}{k-1}+\binom{n+k-2}{k-2}+\ldots+\binom{n}{0}$. Подставляя это равенство в предыдущее, получаем утверждение задачи.

> **Задача 14.** Каких подмножеств в множестве из 16 элементов больше: состоящих из более чем 8 элементов, из менее чем 8 элементов, из ровно 8 элементов?

Ответ. Подмножеств первого и второго типа поровну, и больше, чем подмножеств третьего типа.

Решение. Выпишем 17-ю строку треугольника Паскаля: 1, 16, 120, 560, 1820, 4368, 8008, 11440, 12870, 11440, 8008, 4368, 1820, 560, 120, 16, 1. Отсюда видно, что подмножеств первого и второго типа по 26333, а подмножеств третьего типа 12870.

Решение 2. Из задачи 7 следует, что подмножеств, состоящих из более чем 8 элементов, столько же, сколько и подмножеств, состоящих из менее чем 8 элементов. Обозначим это число через x. Достаточно сравнить x с $C_{16}^8=12870$. Заметим для этого, что $2x+12870$ — это число всех подмножеств в множестве из 16 элементов, то есть $2x+12870=65536$, откуда $x=26333>12870$.

> **Задача 15.** Найдите число таких последовательностей длины 16 из нулей и единиц, в которых не менее чем три единицы.

Указание. Заметьте, что это число равно разности числа всех последовательностей длины 16 из нулей и единиц и числа таких последовательностей, в которых не более двух единиц.

Решение. Учитывая указание, получаем ответ: $2^{16} - C_{16}^0 - C_{16}^1 - C_{16}^2 = 65536 - 1 - 16 - 120 = 65399$.

Задача 16. Решите указанные преподавателем задачи из листка «Комбинаторика 1» для произвольных n и k.

Задача 17*. Сколькими способами можно выбрать неотрицательные целые числа $x_1, x_2, \ldots, x_m$ такие, что $x_1 + x_2 + \ldots + x_m = n$?

Указание. Это число способов поставить в очередь $m-1$ манекен и n человек.

Решение. Заметим, что искомое число — это число способов поставить в очередь $m-1$ манекен и n человек. Действительно, каждой такой очереди можно поставить в соответствие следующий набор чисел: x_1 — количество людей, стоящих в очереди перед первым манекеном, x_2 — между первым и вторым манекеном, …, x_m — после последнего манекена. Построенное соответствие взаимно однозначно (проверьте!). Но число способов поставить в очередь $m-1$ манекен и n человек — это в точности число способов выбрать в этой очереди n мест для людей, то есть $\binom{n+m-1}{n}$.

Теория графов 1

листок 6 / ноябрь 2004

Это первый из двух листков, посвященных графам. Достоинство этой темы, во-первых, в том, что можно без долгого изучения абстрактных определений и технических лемм сразу перейти к решению содержательных задач (а при желании — даже открытых проблем). Это связано со спецификой теории графов — в ней практически нет сложных конструкций, помогающих решать много разных задач (хотя присутствуют некоторые универсальные идеи, которые, однако, тяжело сформулировать в виде формальных теорем). Во-вторых, изучаемый объект очень нагляден, и при решении задач можно использовать геометрическую интуицию.

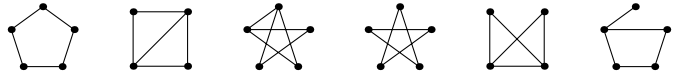
Кроме того, что графы интересны сами по себе, они довольно часто возникают при изучении взаимоотношений между объектами (именно так, как способ *записи* отношений, и возникли графы). В последнее время задачи теории графов приобретают все большее практическое значение. Причем не только при анализе тех или иных схем, но и как источник тонких конструкций в криптографии.

Определение 1. *Графом*[18] называется пара $\Gamma = (V, E)$ из конечного множества *вершин* V и множества *ребер* E, элементами которого являются (неупорядоченные) пары вершин графа Γ.

Граф можно представлять себе как множество точек, некоторые пары которых соединены линиями.

Определение 2. Графы Γ_1 и Γ_2 называются *изоморфными*, если существует такая биекция $f\colon V(\Gamma_1) \to V(\Gamma_2)$, что вершины A и B графа Γ_1 соединены ребром тогда и только тогда, когда вершины $f(A)$ и $f(B)$ соединены ребром в графе Γ_2.

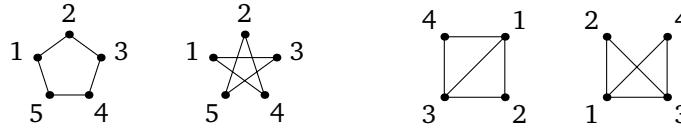
Задача 1. Какие из следующих графов изоморфны?



Решение. Заметим сначала, что в изоморфных графах поровну вершин и ребер. Следовательно, изоморфны могут быть только следующие наборы графов: первый, четвертый и шестой; второй и пятый. Второй граф действительно изоморфен пятому, а первый — четвертому. Шестой граф не изоморфен ни первому, ни четвертому, поскольку у него есть вершина, из которой выходит ровно одно ребро, а у первого и четвертого такой вершины нет. На рисунке соответственные

[18] Точнее, *неориентированным графом без петель и кратных ребер*.

вершины обозначены одинаковыми цифрами:



Вообще, задача об изоморфизме графов — очень важная и довольно сложная, а точнее, является «NP-полной задачей». И несмотря на кажущуюся простоту, проверка изоморфности двух графов является очень сложной задачей даже для мощного компьютера.

В случае положительного ответа обычно просто предъявляется биекция между множествами вершин. Для доказательства неизоморфности двух графов требуются более тонкие соображения. Например, для каждого графа можно посчитать некоторые величины, которые одинаковы для изоморфных графов (число вершин, число ребер, число вершин данной степени и т. д.). Такие величины называются *инвариантами* и часто используются, например, для доказательства неизоморфности различных математических объектов.

> **Задача 2.** Нарисуйте все неизоморфные друг другу графы с не более чем четырьмя вершинами.

Указание. Разумно перечислять эти графы, упорядочивая их по числу вершин и числу ребер.

Решение. Существует только один граф, в котором 0 вершин и только один граф, в котором одна вершина:

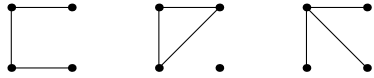
Графов с двумя вершинами существует два: тот, в котором эти вершины соединены ребром, и тот, в котором не соединены:

Существует четыре графа с тремя вершинами: без ребер, с одним, двумя и тремя ребрами:

Существует по одному графу с четырьмя вершинами и нулем, одним, пятью и шестью ребрами:

Графов с четырьмя вершинами и двумя (соответственно, четырьмя) ребрами существует по два:

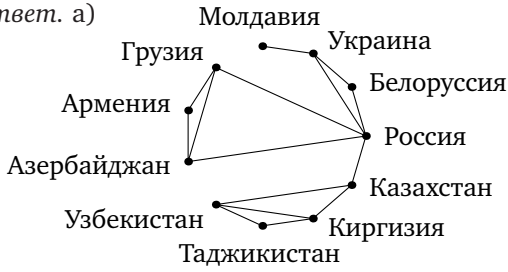
Графов с четырьмя вершинами и тремя ребрами три:



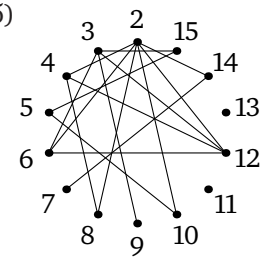
Задача 3. а) Нарисуйте граф, вершинами которого являются страны СНГ, а ребрами соединены граничащие страны.

б) Нарисуйте граф, вершинами которого являются натуральные числа от 2 до 15, а ребрами соединены различные числа, одно из которых делится на другое.

Ответ. а)



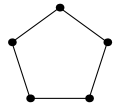
б)



Задача 4. а) Постройте граф с пятью вершинами, в котором нет ни трех попарно соединенных, ни трех попарно несоединенных вершин.

б) Докажите, что в каждой компании из шести человек найдутся либо три попарно знакомых, либо три попарно незнакомых человека.

Решение. а) Например, подходит пятиугольник.



б) Допустим, нашлась компания, в которой нет ни трех попарно знакомых человек, ни трех попарно незнакомых. Пусть один их них Саша. Так как кроме него в компании еще 5 человек, он либо знаком хотя бы с тремя людьми этой компании, либо незнаком хотя бы с тремя. Без ограничения общности можно считать, что Саша знаком хотя бы с тремя людьми из этой компании. Если какие-то двое из Сашиных знакомых знакомы между собой, они вместе с Сашей образуют тройку

попарно знакомых людей. Если же все Сашины знакомые незнакомы друг с другом, то они образуют тройку попарно незнакомых людей этой компании.

Эта задача — важный частный случай теоремы Рамсея, первый пример содержательного рассуждения на графах. Важно научиться логически стройно проводить доказательства на графах.

> **Задача 5.** Пусть в некоторой компании среди любых трех человек найдутся два друга. Обязательно ли эту компанию можно разбить на две группы, так что всякие два человека из одной группы — друзья?

Ответ. Нет, не обязательно.

Решение. Например, для компании из пяти человек, знакомых «по кругу» (А с Б, Б с В, В с Г, Г с Д, Д с А), условие задачи выполнено, а разбить ее указанным способом на две группы невозможно.

> **Задача 6.** Найти наибольшее возможное количество ребер в графе с n вершинами, если известно, что среди произвольных трех его вершин есть две, не соединенные ребром.

Решение. Немного поэкспериментировав, можно обнаружить, что n нарисованных на бумаге точек удается соединить наибольшим количеством отрезков, как просят в задаче (то есть так, чтобы среди произвольных трех всегда были бы две, не соединенные ребром), следующим образом: надо поделить множество точек на две «примерно равные» группы и затем соединить каждую точку из первой группы со всеми точками второй группы. Поясним, что мы имеем ввиду, когда говорим «примерно равные»: если точек было $2k$, то мы разбиваем на две группы по k точек в каждой; если же у нас была нарисована $2k+1$ точка, то в одной группе должно быть k точек, а в другой $k+1$.

Введем обозначение: наибольшее возможное количество ребер в графе с n вершинами и свойством, что среди произвольных трех его вершин есть две, не соединенные ребром, будем называть M_n.

Нетрудно посчитать, что если соединять точки так, как описано выше, то $M_n = k \cdot k = k^2$, если $n = 2k$, и $M_n = k(k+1)$, если $n = 2k+1$. Оказывается, что описанным выше способом мы действительно получаем наибольшее возможное количество ребер. Поэтому докажем по индукции следующее утверждение: «Если $n = 2k$, то $M_n = k^2$. Если же $n = 2k+1$, то $M_n = k(k+1)$».

База индукции. При $n = 2$ и $n = 3$ утверждение очевидно.

Шаг индукции. *Первый случай.* Пусть для $n = 2k-1$ утверждение верно. Докажем тогда, что $M_{2k} = k^2$. Предположим, что это не так.

То есть $M_{2k} > k^2$ ($M_{2k} < k^2$ быть не может, так как описанным выше способом мы умеем рисовать по крайней мере k^2 ребер).

Лемма (вспомогательное утверждение). Рассмотрим граф Г с $2k$ вершинами, реализующий случай с M_{2k} ($> k^2$) ребрами. Докажем, что вершина минимальной степени (обозначим ее буквой a) в нем соединена не более, чем с k другими вершинами.

Действительно, предположим, что она соединена более чем с k вершинами: $a_1, a_2, \ldots, a_k, \ldots$ Возьмем одну из них. Например, a_1. Ее степень не меньше, чем степень вершины a. А значит, она тоже соединена не менее чем с k вершинами: $b_1, b_2, \ldots, b_k, \ldots$ При этом (так как у нас «запрещены треугольники») ни одна из вершин a_i не совпадает ни с какой вершиной b_j. А значит, в нашем графе имеется по крайней мере $2k+1$ различная вершина, что противоречит нашему предположению о количестве вершин графа Г.

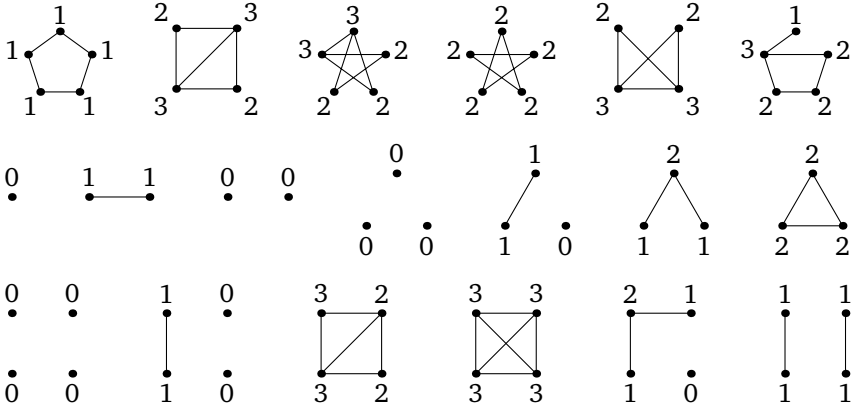
Из утверждения леммы следует, что в рассматриваемом графе существует вершина, соединенная не более, чем с k другими вершинами. Если мы выкинем из графа эту вершину вместе со всеми ребрами, выходящими из нее, то получим граф с $2k-1$ вершиной и не менее, чем $M_{2k} - k > k^2 - k = k(k-1)$ ребрами. А это противоречит предположению индукции.

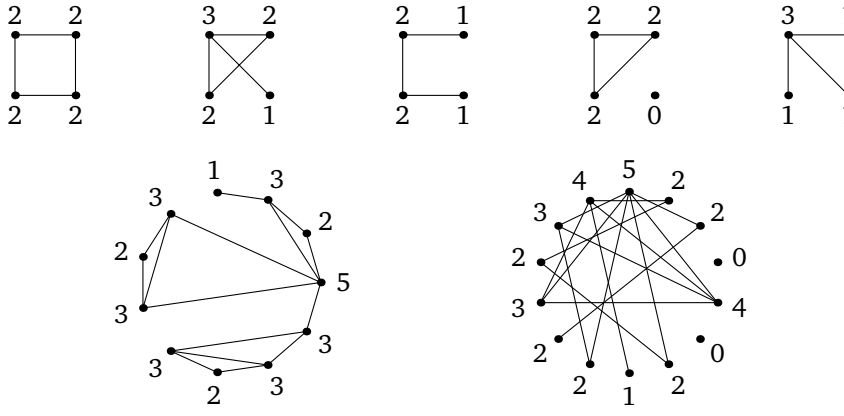
Второй случай аналогичен первому и остается читателю в качестве упражнения.

Определение 3. *Степенью* (или *валентностью*) *вершины A* называется число выходящих из нее ребер. Обозначение: $\deg A$.

Задача 7. Укажите степени всех вершин графов из задач 1, 2 и 3.

Ответ. На рисунке около каждой вершины написана ее степень:





Задача 8. Докажите, что в графе с более чем одной вершиной есть две вершины одинаковой степени.

Решение. Допустим, существует граф с $n > 1$ вершинами, в котором степени всех вершин различны. Степень каждой из этих вершин — целое число от 0 до $n-1$, всего n вариантов. Поскольку степени всех вершин различны, в графе есть одна вершина степени 0, одна степени 1, …, одна степени $n-1$. Рассмотрим вершины степени 0 и $n-1$. Так как $n > 1$, это разные вершины. Но вершина степени 0 не соединена ни с одной вершиной, а вершина степени $n-1$ соединена со всеми вершинами. Поэтому эти две вершины одновременно соединены и не соединены между собой. Полученное противоречие доказывает утверждение задачи.

Задача 9. Докажите, что сумма степеней вершин произвольного графа равна удвоенному количеству его ребер.

Решение. Посчитаем двумя способами число пар вида (вершина графа, ребро, выходящее из этой вершины). С одной стороны, число таких пар, содержащих данную вершину, равно ее степени, поэтому общее число таких пар равно сумме степеней вершин графа. С другой стороны, каждое ребро входит ровно в две такие пары, поэтому число пар равно удвоенному числу ребер, откуда следует утверждение задачи.

Определение 4. *Путем* в графе называется конечная последовательность вершин и соединяющих их ребер, то есть последовательность вида $v_0e_1v_1e_2v_2\ldots e_nv_n$, где v_i — вершины графа, а ребро e_i соединяет вершины v_{i-1} и v_i. Число n называется *длиной пути*. *Циклом* называется путь, в котором первая и последняя вершины совпадают.

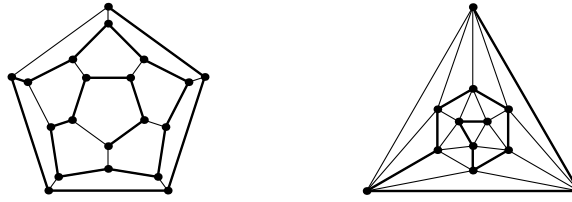
В графе без кратных ребер (а в этом листке изучаются только такие графы) путь однозначно восстанавливается по последовательности своих вершин, поэтому обычно выписывают именно эту последовательность. Однако технически удобнее включать ребра в определение.

Понятие пути является математическим аналогом инструкции по проезду из одного пункта в другой по сети дорог: такая инструкция должна говорить, через какие промежуточные пункты и по каким дорогам следует ехать.

Определение 5. Граф Г называется *гамильтоновым*, если в нем существует путь, содержащий каждую вершину ровно один раз.

Задача 10. Докажите, что графы додекаэдра и икосаэдра гамильтоновы.

Ответ. На рисунке изображены графы додекаэдра и икосаэдра.



Додекаэдр (двенадцатигранник) и икосаэдр (двадцатигранник) являются двумя из пяти возможных правильных многогранников (то есть многогранников у которых все грани равны). Удивительно, но факт: можно доказать, что в пространстве существует всего пять типов правильных многогранников, в то время как на плоскости существует бесконечно много правильных многоугольников. Доказывать это утверждение мы сейчас не будем, а ограничимся лишь тем, что перечислим все правильные многогранники: тетраэдр (или треугольная пирамида, или правильный четырехгранник), гексаэдр (или куб, или правильный шестигранник), октаэдр (или правильный восьмигранник), додекаэдр (или правильный двенадцатигранник), икосаэдр (или правильный двадцатигранник).

Сделаем еще одно интересное наблюдение: если соединить середины соседних граней тетраэдра, то снова получим тетраэдр. Про такие многогранники говорят, что они являются самодвойственными.

Если соединить середины соседних граней куба, то получим октаэдр. И наоборот: если соединить середины соседних граней октаэдра, то получим куб. Про такие многогранники говорят, что они являются

двойственными друг другу. Оказывается, что додекаэдр и икосаэдр также являются двойственными друг другу.

Полезно также обсудить граф футбольного мяча. В частности, выяснить, является ли футбольный мяч правильным многогранником, понять, какие у него грани и т. д.

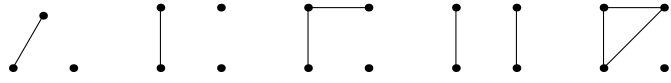
Определение 6. Граф называется *связным*, если для любых двух различных его вершин существует путь, начинающийся в первой из них и заканчивающийся во второй.

Менее формально, связный граф — это граф, в котором из любой вершины можно добраться до любой другой по ребрам. В случае сети дорог это означает, что можно проехать из любого населенного пункта в любой другой.

Если граф не является связным, то его можно разбить на так называемые *компоненты связности*, то есть на связные подграфы, между которыми нет ребер. Для этого можно взять вершину графа и посмотреть, до каких вершин можно из нее добраться по ребрам — это и будет компонента связности этой вершины. Формализовать эту конструкцию можно с помощью понятия отношения эквивалентности.

Задача 11. Какие из графов задач 1, 2 и 3 связны?

Ответ. Связными являются все графы, встречающиеся в первой задаче. Во второй задаче связными являются все графы, кроме графов без ребер и следующих:



Задача 12. Докажите, что если граф, число вершин которого больше 1, связен, то степень любой его вершины положительна. Верно ли обратное?

Решение. Допустим, что в связном графе, число вершин которого больше 1, нашлась вершина степени 0. Это означает, что из этой вершины не выходит ни одного ребра, а значит, ее нельзя соединить путем ни с одной другой вершиной графа.

Обратное утверждение неверно, например, для следующего графа:

Определение 7. Связный граф называется *деревом*, если в нем не существует цикла (т. е. пути, конец которого совпадает с началом), все ребра которого различны.

Задача 13. Докажите, что в любом дереве есть: а) хотя бы одна; б) хотя бы две вершины степени 1.

Решение. а) Рассмотрим произвольное дерево. Выйдем из одной из вершин этого дерева и будем идти по его ребрам, никогда не возвращаясь по ребру, по которому мы только что пришли в вершину. Поскольку в дереве нет циклов, мы никогда не вернемся в вершину, в которой уже были, а значит, не более чем через n ходов (n — число вершин дерева) попадем в вершину, из которой не сможем выйти. Ясно, что степень этой вершины должна быть равна 1.

б) Достаточно повторить рассуждения предыдущего пункта, выходя из вершины степени 1.

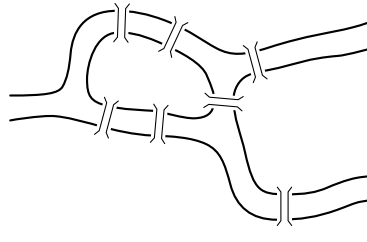
Задача 14. Докажите, что в дереве число вершин на 1 больше числа ребер.

Решение. Докажем утверждение задачи индукцией по числу n вершин дерева.

База индукции очевидна.

Шаг индукции. Пусть утверждение задачи верно для деревьев с n вершинами. Докажем его для деревьев с $n+1$ вершиной. Рассмотрим произвольное дерево с $n+1$ вершиной. Найдем в нем вершину степени 1 и выбросим вместе с выходящим из нее ребром. Очевидно, что получилось дерево с n вершинами. По предположению индукции в этом дереве $n-1$ ребро. Следовательно, в исходном дереве было $n-1+1=n$ ребер.

Задача 15. На рисунке изображена схема расположения мостов в городе Кёнигсберге XVIII века. Можно ли совершить прогулку так, чтобы пройти по каждому мосту ровно один раз?



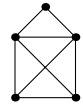
Ответ. Нет, нельзя.

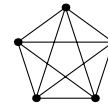
Решение. Пусть наша прогулка не начиналась и не закончилась на острове X. Заметим, что впервые пройдя через него, мы воспользовались двумя выходящими из X мостами (по одному пришли, по другому ушли). Но это значит, что воспользоваться оставшимся выходящим из X мостом мы уже не могли, иначе на X прогулка бы закончилась.

Определение 8. Граф называется *эйлеровым*, если в нем существует цикл, проходящий по каждому ребру ровно один раз.

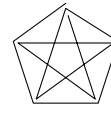
Менее формально, граф называется эйлеровым, если его можно нарисовать, не отрывая карандаша от бумаги и не проводя одну линию дважды так, что карандаш остановится там же, где начнет движение.

Задача 16. Какие из следующих графов эйлеровы?





Решение. Первый граф не является эйлеровым по соображениям, аналогичным задаче 15. Один из возможных обходов второго графа изображен на рисунке:

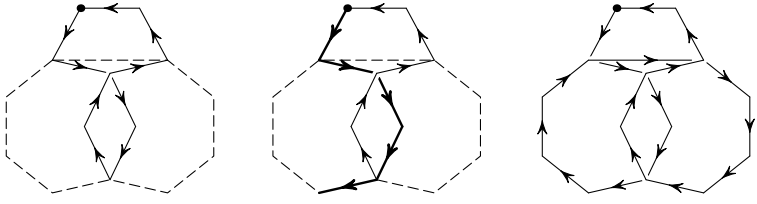


Задача 17. Докажите, что граф эйлеров тогда и только тогда, когда он связен и степень каждой его вершины четна.

Решение. Докажем сначала, что в эйлеровом графе степень каждой вершины четна. Для этого рассмотрим произвольную вершину нашего графа. Аналогично задаче 15, посмотрим на то, сколько раз эйлеров цикл входит в эту вершину и сколько раз из нее выходит. Заметим, что эти числа равны: каждый раз, входя в вершину по какому-то ребру, мы из нее выходим по какому-то другому. При этом, если цикл начинается в рассматриваемой вершине, то первому «выходу» из вершины надо поставить в соответствие последнее «возвращение». Следовательно, степень вершины четна. В силу произвольности выбора вершины, степени всех вершин четны.

Докажем теперь, что связный граф, степени всех вершин которого четны, эйлеров. Для этого сначала выйдем из какой-нибудь вершины, и будем ходить по ребрам графа произвольным способом, не проходя

ни по какому ребру дважды, пока это возможно. Аналогично предыдущему пункту, можно доказать, что остановимся мы в той же вершине, из которой выходили, и из каждой вершины графа выходит четное число еще неиспользованных ребер. Если полученный цикл проходит не по всем ребрам графа, выйдем из какой-нибудь его вершины A, из которой выходит неучтенное ребро, и построим цикл, проходящий только по неучтенным ребрам. Теперь можно построить новый цикл, который доходит до вершины A вдоль старого цикла, потом полностью проходит только что построенный цикл и завершает маршрут по старому циклу. Ясно, что новый цикл не будет проходить ни по какому ребру дважды и будет содержать больше ребер, чем старый. Продолжая этот процесс далее, мы за несколько шагов получим цикл, проходящий по всем ребрам графа.



Задача 18*. В турнире без ничьих участвовало n команд. Каждая команда сыграла с каждой ровно по одному разу. Докажите, что можно так занумеровать команды числами $1, \ldots, n$, что $(i+1)$-я команда выиграла у i-й (для произвольного $i = 1, \ldots, n-1$).

Решение. Докажем утверждение задачи индукцией по n. База индукции $n = 1$ очевидна. Докажем шаг индукции. Пусть для n команд утверждение задачи выполнено. Рассмотрим произвольный турнир без ничьих между $n+1$ командой. Заметим, что между первыми n командами произошел турнир без ничьих. Следовательно, их можно так занумеровать, что $(i+1)$-я команда выиграла у i-й для каждого $i = 1, \ldots, n-1$. Если $(n+1)$-я команда выиграла у всех остальных, ей можно присвоить номер $n+1$. Иначе, $(n+1)$-ю команду можно вставить в список сразу перед командой с наименьшим номером среди тех, кому она проиграла.

Задача 19* (теорема Рамсея). а) Докажите, что для произвольных натуральных m, n существует натуральное k такое, что в произвольном графе с k вершинами найдется либо m попарно соединенных ребрами вершин, либо n попарно несоединенных. Наименьшее такое k обозначается $R(m, n)$.

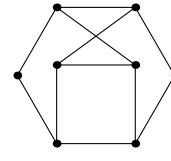
б) Найдите $R(3, 4)$.

Решение. а) Докажем индукцией по $m+n$, что если $R(m-1,n)$ и $R(m,n-1)$ существуют, то в любом графе с числом вершин, не меньшим чем $R(m-1,n)+R(m,n-1)$, найдется либо m попарно соединенных ребрами вершин, либо n попарно несоединенных. Из этого будет следовать, что $R(m,n)$ существует для всех m,n и $R(m,n)\leqslant \leqslant R(m-1,n)+R(m,n-1)$.

Рассмотрим какую-нибудь вершину v в произвольном графе с не менее чем $R(m-1,n)+R(m,n-1)$ вершинами. Эта вершина либо соединена ребром хотя бы с $R(m-1,n)$ вершинами, либо не соединена ребром хотя бы с $R(m,n-1)$ вершинами. В первом случае среди вершин, соединенных с v, найдется либо $m-1$ попарно соединенных (тогда они вместе с v образуют m попарно соединенных вершин), либо n попарно не соединенных. Во втором случае среди вершин, не соединенных с v, найдется либо m попарно соединенных, либо $n-1$ попарно не соединенная (которые вместе с v образуют n попарно соединенных). Итак, в любом случае найдется либо m попарно соединенных вершин, либо n попарно не соединенных.

б) В силу предыдущего пункта $R(3,4)\leqslant R(2,4)+R(3,3)$. Заметим, что $R(2,n)=n$ для любого n. Кроме того, по задаче 4 $R(3,3)=6$. Следовательно, $R(3,4)\leqslant 4+6=10$. Допустим, существует граф из 9 вершин, не содержащий ни трех попарно соединенных, ни четырех попарно несоединенных вершин. В предыдущем пункте было доказано, что степень каждой вершины меньше $R(2,4)=4$, и вершина не может быть не соединена с какими-то $R(3,3)=6$ другими. Следовательно, степень каждой вершины меньше 4 и больше $8-6=2$, а значит, равна 3. Следовательно, сумма степеней всех вершин равна $3\cdot 9=27$, то есть нечетна, что невозможно. Следовательно, $R(3,4)\leqslant 9$.

Приведем теперь пример графа с 8 вершинами, в котором нет ни трех попарно соединенных, ни четырех попарно несоединенных вершин:



Итак, $R(3,4)=9$.

Определение 9. Назовем *расстоянием* между вершинами связного графа наименьшую длину пути, соединяющего эти вершины (длина каждого ребра считается равной 1). *Диаметром графа* называется наибольшее расстояние между его вершинами.

Определение 10. Граф называется *регулярным* графом *валентности* k, если степень каждой его вершины равна k.

Определение 11. *Графом Мура* называется регулярный граф валентности k, диаметр которого не превосходит двух, а число вершин равно k^2+1.

Задача 20*. а) Докажите, что в регулярном графе валентности k и диаметра 2 не может быть больше k^2+1 вершины.

б) Приведите примеры графов Мура при $k=1, 2, 3$.

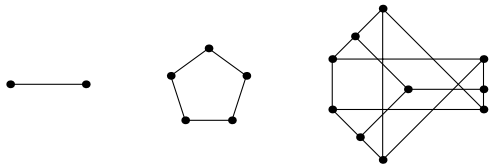
в) Существует ли граф Мура при $k=7$?

г**) Существует ли граф Мура при $k=57$?

д) Докажите, что ни при каких других значениях k не существует графов Мура.

Решение. а) Рассмотрим какую-нибудь вершину регулярного графа валентности k и диаметра 2. Она соединена с k вершинами, каждая из которых соединена еще с $k-1$ вершиной. Если предположить, что все вышеупомянутые вершины различны, то мы получим, что их было $k+k\cdot(k-1)+1=k^2+1$. Так как мы рассматриваем граф диаметра 2, то никаких других вершин в нашем графе быть не может.

б) $k=1$ $k=2$ $k=3$



в) Пока это открытая проблема.

г) Элементарное решение этой задачи авторам неизвестно. Набросок решения есть в материалах курса С. В. Дужина «Комбинаторные структуры в топологии» (НМУ, осенний семестр 1998 г.; см. `http://ium.mccme.ru/f98/combtop.html`).

Задача 21*. Дан правильный 50-угольник. В одной из его вершин стоит доктор Фауст. У него есть три возможности: 1) бесплатно перейти в диаметрально противоположную точку; 2) заплатив Мефистофелю 1 рубль 05 копеек, перейти на соседнюю вершину против часовой стрелки; 3) получив от Мефистофеля 1 рубль 05 копеек перейти на соседнюю вершину по часовой стрелке. Известно, что доктор Фауст везде побывал (хотя бы один раз). Докажите, что на каком-то отрезке пути кто-то кому-то заплатил не меньше 25 рублей.

Указание. «Склейте» пары противоположных вершин.

Набросок решения. Склеим пары противоположных вершин (то есть рассмотрим 25-угольник, вершины которого соответствуют парам противоположных вершин исходного 50-угольника). Заметим, что при этом понятия «по часовой» и «против часовой» стрелки сохраняют смысл. Учитывая, что $1{,}05 \cdot 24 = 25{,}20$, задача сводится к следующей:

> Гуляя по сторонам правильного 25-угольника, доктор Фауст побывал во всех вершинах. Докажите, что на каком-то участке времени модуль разности числа ходов доктора по и против часовой стрелки не меньше 24.

Занумеруем вершины 25-угольника числами от 0 до 24 по часовой стрелке и рассмотрим отображение из множества целых чисел в 25-угольник, сопоставляющее числу a вершину с номером «остаток от деления a на 25». Сопоставим пути доктора Фауста на 25-угольнике путь на целочисленной прямой, начинающийся в точке 0, в котором движению против часовой стрелки по 25-угольнику соответствует движению влево на прямой, а движение по часовой стрелке соответствует движению вправо.

Все прообразы точки с номером k, лежащей на 25-угольнике, имеют вид $k + 25n$, $n \in \mathbb{Z}$. Рассмотрим самую левую и самую правую точки на прямой, в которых побывал доктор Фауст. Тогда расстояние между ними не меньше 24, так как доктор Фауст побывал во всех точках 25-угольника, а следовательно, во время прогулки по прямой встретил все остатки от деления на 25. Это завершает решение задачи.

Подстановки 2

листок 2д / декабрь 2004

Листок состоит из двух частей. Первая часть посвящена понятию четности подстановки. С его помощью удается, в частности, решить классическую задачу об игре в пятнашки. Во второй части в основном обсуждается возведение подстановок в степень и порядок перестановки. В дополнительных задачах листка появляется понятие сопряженных подстановок.

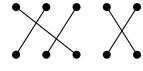
Одной из целей изучения подстановок является подготовка к абстрактной теории групп: с одной стороны, подстановки дают важный (но доступный) пример группы, с другой — часть рассуждений из этого листка без существенных изменений переносится на случай произвольной группы. Поработав с конкретной, достаточно содержательной группой, можно почувствовать дух теории групп. После этого абстрактное определение группы будет более понятным и естественным. Да и вообще, по теореме Кэли любая конечная группа есть подгруппа группы подстановок, так что даже формально все богатство теории конечных групп можно увидеть на группах подстановок.

Определение 1. Пусть дана подстановка $\begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$. *Беспорядком* называется пара (k, l), $1 \leqslant k < l \leqslant n$, такая что $j_k > j_l$. Подстановка называется *четной*, если число беспорядков в ней четно, и *нечетной* в противном случае.

В частности, тождественная подстановка четна, поскольку не имеет беспорядков в канонической записи. Таким образом, чтобы найти по этому определению четность подстановки, нужно сначала привести ее к канонической форме.

Задача 0. Определим четность подстановки, записанной в произвольной форме, как четность суммы беспорядков в верхней и нижней строках. Докажите, что тем самым получится эквивалентное определение (т. е. все подстановки, являющиеся четными (нечетными) по определению 1, будут также являться четными (нечетными) по новому определению и наоборот).

Указание. Эквивалентное определение: подстановка $\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$ называется четной, если число пар (k, l), таких что $i_k > i_l$, но $j_k < j_l$, четно. Другими словами, четность перестановки σ есть четность числа пересечений совокупности отрезков, соединяющих i с $\sigma(i)$.



Решение. Заметим, что определение из указания эквивалентно определению 1 для подстановки, записанной в канонической форме. Кроме того, ясно, что это определение не зависит от формы записи подстановки.

Осталось показать, что это определение эквивалентно определению из задачи. То есть нужно проверить, что общее число беспорядков в обеих строках записи подстановки имеет ту же четность, что и число пар (k, l), таких что $i_k > i_l$, но $j_k < j_l$.

Это достаточно проверить для каждой *неупорядоченной* пары $\{k, l\}$ (будем для определенности считать, что $k < l$): если $i_k > i_l$, $j_k < j_l$ или $i_k < i_l$, $j_k > j_l$, в обе суммы эта пара дает вклад, равный 1 (отметим, что в одном случае вклад во вторую сумму дает пара (k, l), а в другом — (l, k)); если же $i_k > i_l$, $j_k > j_l$ или $i_l < i_l$, $j_k < j_l$, то вклад в одну сумму равен 0, а в другую — 2.

Задача 1. Найдите четности подстановок из задач 1, 2 предыдущего листка.

Решение. $\binom{1}{1}$ — тождественная, а потому четная. $\binom{123}{123}$ — также тождественная. $\binom{514632}{164253} = \binom{123456}{635412}$. Беспорядков 12: (3, 6), (4, 6), (1, 6), (2, 6), (1, 3), (2, 3), (4, 5), (1, 5), (2, 5), (3, 5), (1, 4), (3, 4). Значит, подстановка четная. $\binom{4321}{1234} = \binom{1234}{4321}$. Беспорядков 6: (4, 3), (4, 2), (4, 1), (3, 2), (3, 1), (2, 1). Подстановка также является четной. $\binom{1}{1}$ — четная. $\binom{12}{12}$ — четная, $\binom{12}{21}$ — нечетная. $\binom{123}{132}$ — нечетная, $\binom{123}{213}$ — нечетная, $\binom{123}{231}$ — четная, $\binom{123}{321}$ — нечетная, $\binom{123}{312}$ — четная.

Задача 2. Пусть a и b — подстановки на множестве из четырех элементов, $a = (1, 2, 3, 4)$, $b = (1, 4, 3)$. Какие из следующих подстановок четны, а какие нечетны:

а) e; б) a; в) b; г) $b^2 = b \cdot b$; д) $b^3 = b \cdot b \cdot b$; е) ab; ж) ba?

Ответ. а) Четная; б) $a = \binom{1234}{2341}$ — нечетная; в) $b = \binom{1234}{4213}$ — четная; г) $b^2 = \binom{1234}{3241}$ — четная; д) $b^3 = \binom{1234}{1234}$ — четная; е) $ab = \binom{1234}{1324}$ — нечетная; ж) $ba = \binom{1234}{2134}$ — нечетная.

Задача 3. Докажите, что а) при умножении на транспозицию (справа или слева) четность меняется; б) четность произведения k транспозиций равна четности числа k.

Полезно, перед тем, как переходить к доказательству, разобрать несколько примеров.

Решение. а) Рассмотрим произвольную подстановку, записанную канонически: $\begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_i & \dots & \sigma_j & \dots & \sigma_n \end{pmatrix}$. При умножении ее на транспозицию $(i\,j)$ *справа* получается подстановка $\begin{pmatrix} 1 & 2 & \dots & j & \dots & i & \dots & n \\ \sigma_1 & \sigma_2 & \dots & \sigma_i & \dots & \sigma_j & \dots & \sigma_n \end{pmatrix}$. Видно, что число беспорядков в нижней строке не изменилось, а в верхней появилось $2(j-i)-1$ беспорядков. Следовательно (в силу задачи 0), четность подстановки изменилась.

Полезное упражнение на понимание этого рассуждения — это явно повторить его для умножения слева.

б) Решение следует из предыдущей задачи.

Задача 4. а) Как выражается четность ab через четность a и четность b?

б) Как выражается четность a^n через четность a?

Решение. а) Из задачи 9 листка «Подстановки 1» мы знаем, что любую подстановку можно представить в виде произведения транспозиций. Кроме того, из предыдущей задачи мы знаем, что четность числа этих транспозиций будет равна четности подстановки. Поэтому, если a представима в виде произведения k транспозиций, а b представима в виде произведения l транспозиций, то ab будет представима в виде произведения $k+l$ транспозиций. Отсюда получаем правило: четности подстановок при умножении складываются.

б) Как следует из предыдущего пункта, четность подстановки a^n равна произведению четности n на четность a.

Решение 2. Запишем подстановку a канонически, а b — так, чтобы числа в нижней строке стояли по порядку: $a = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$, $b = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ 1 & 2 & \dots & n \end{pmatrix}$. Тогда $ab = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$. В силу задачи 0 четность подстановки a равна четности числа беспорядков в строке $a_1, \dots, a_n$, подстановки b — в строке $b_1, \dots, b_n$, а подстановки ab — четности суммы этих чисел.

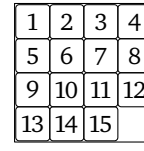
Задача 5. Каких подстановок в S_n больше: четных или нечетных?

Ответ. Число четных подстановок равно числу нечетных.

Решение. Построим биекцию между множествами четных и нечетных подстановок: зафиксируем некоторую транспозицию t и каждой четной подстановке σ поставим в соответствие (нечетную, как мы уже доказали) подстановку σt. Осталось убедится в том, что это

биекция. Для этого достаточно заметить, что у него есть обратное — то же самое отображение (на нечетных подстановках).

Задача 6*. Докажите, что если в игре «пятнашки» поменять местами фишки с номерами «14» и «15», то, играя в эту игру, невозможно получить первоначальное расположение фишек.



Набросок решения. Допустим, из начального расположения фишек можно поменять фишки «14» и «15» местами, вернув остальные на свои места. Положим на место пустой клетки фишку с надписью «16». Тогда каждому расположению фишек соответствует некоторая подстановка $a \in S_{16}$. Ход заключается в том, что мы меняем некоторую фишку с фишкой «16», то есть умножаем имеющуюся у нас подстановку на некоторую транспозицию. Следовательно, при каждом ходе четность подстановки меняется, а значит, всего было сделано нечетное число ходов.

С другой стороны, пустая клетка вернулась на свое место, значит, число ходов вправо равно числу ходов влево, а число ходов вверх равно числу ходов вниз, то есть общее число ходов четно. Полученное противоречие завершает доказательство.

Задача 7*. Докажите, что из любого расположения фишек можно, соблюдая правила игры, получить либо начальное расположение, либо расположение, описанное в предыдущей задаче.

Указание. Сначала поставьте на свои места фишки от 1 до 12. Фишку 13 можно поставить на свое место, сдвинув правильно поставленные фишки от 9 до 12 «змейкой» в правый нижний угол.

Определение 2. Подстановкой, *обратной* к подстановке $a \in S_n$, называется такая подстановка $b \in S_n$, что $ab = ba = e$. Обозначение: a^{-1}.

Задача 8. Докажите, что для любых двух подстановок a и b имеет место равенство $(ab)^{-1} = b^{-1}a^{-1}$.

Решение. Чтобы доказать, что подстановка $b^{-1}a^{-1}$ является обратной к подстановке ab нужно проверить, что $abb^{-1}a^{-1} = e = b^{-1}a^{-1}ab$, что очевидно.

Задача 9. Найдите все $a \in S_n$, такие что для любой подстановки $b \in S_n$ выполняются равенства: а) $ba = b$; б) $ba = ab$; в*) $ba = ab^{-1}$.

Решение. а) Домножим обе части равенства $ba = b$ на b^{-1} слева. Получим, что $b^{-1}ba = b^{-1}b$, то есть $a = e$.

б) Пусть найдена искомая подстановка $a = \begin{pmatrix} 1\,2\ldots n \\ i_1 i_2 \ldots i_n \end{pmatrix}$. Тогда $\begin{pmatrix} 1\,2\ldots n \\ i_1 i_2 \ldots i_n \end{pmatrix}(k\,m) = (k\,m)\begin{pmatrix} 1\,2\ldots n \\ i_1 i_2 \ldots i_n \end{pmatrix}$ для любых k и m.

Заметим, что если подстановка a записана канонически, то подстановка $a(k\,m)$ получается из a, если просто поменять местами в нижней строке элементы i_k и i_m (докажите!); а подстановка $(k\,m)a$ получается из a, если поменять местами в нижней строке элементы k и m (это тоже следует доказать!).

Таким образом, если $a(k\,m) = (k\,m)a$, то либо $k = i_k$ и $m = i_m$, либо $k = i_m$ и $m = i_k$. А так как k и m мы можем выбрать произвольными, при $n > 2$ подстановка a может быть только тождественной. При $n = 2$ подходят обе подстановки.

в) Заметим, что ответ и решение в этой задаче целиком совпадают с ответом и решением предыдущего пункта, так как для любой транспозиции b верно $b = b^{-1}$.

> **Задача 10* (замена переменных).** Пусть даны подстановки $a, c \in S_n$, и пусть $b = c^{-1}ac$.
>
> а) Докажите, что если подстановка a задана таблицей $a = \begin{pmatrix} i_1 \ldots i_n \\ j_1 \ldots j_n \end{pmatrix}$, то $b = \begin{pmatrix} c(i_1)\ldots c(i_n) \\ c(j_1)\ldots c(j_n) \end{pmatrix}$.
>
> б) Докажите, что если подстановка a задана в виде произведения независимых циклов $a = (i_1 \ldots i_k)\cdot(j_1 \ldots j_l)\cdot\ldots$, то $b = (c(i_1) \ldots c(i_k))\cdot (c(j_1) \ldots c(j_l))\cdot\ldots$

См. комментарий к задаче 8 листка «Отношения эквивалентности».

Решение. См. задачу 8 листка «Отношения эквивалентности».

> **Задача 11.** Дайте определение *степени подстановки* a^k для любого целого k.

Решение. Естественно, в этой задаче требуется дать не произвольное определение, а соответствующее нашим интуитивным представлениям об определяемом объекте. Например, желательно, чтобы выполнялись равенства из следующей задачи, аналогичные свойствам степеней чисел.

Приведем такое определение:

1) $a^k := \underbrace{a\cdot a\cdot\ldots\cdot a}_{k}$, где k — натуральное число, большее единицы;

2) $a^1 := a$;

3) $a^0 := e$;
4) a^{-1} — подстановка, обратная к a;
5) $a^{-k} := (a^k)^{-1}$, k — натуральное, $k > 2$.

Более формально это определение можно давать по индукции: $a^0 := e$, $a^{k+1} := a^k a$ при $k \geqslant 0$, a^{-k} — подстановка, обратная к a^k, при $k > 0$.

a^{-k} в последнем пункте можно было бы определить и так: $a^{-k} := (a^{-1})^k$. При этом получается (проверьте) эквивалентное определение.

Задача 12. Докажите, что для любых $a, b \in S_n$ и любых целых k и l выполняется следующее: а) $a^0 = e$; $a^1 = a$; $a^{k+l} = a^k a^l$; $a^{kl} = (a^k)^l$; б) если $ab = ba$, то $(ab)^k = a^k b^k$.

Решение. а) Доказательство во всех случаях несложно следует из определения. Докажем последнее утверждение:

$$(a^k)^l = \underbrace{a^k \cdot \ldots \cdot a^k}_{l} = \underbrace{a \cdot \ldots \cdot a}_{kl} = a^{kl}, \text{ если } k \text{ и } l \text{ натуральные.}$$

Если одно из чисел k или l отрицательно, то нужно в соответствующем месте вместо произведения вида $a \cdot \ldots \cdot a$ рассматривать произведение вида $a^{-1} \cdot \ldots \cdot a^{-1}$.

б) В этом пункте тоже нужно не забыть, что проверить тождество мы должны для всех целых k, а не только для натуральных. Если $k > 0$, то

$$(ab)^k = \underbrace{ab \cdot \ldots \cdot ab}_{k} = \underbrace{a \cdot \ldots \cdot a}_{k} \cdot \underbrace{b \cdot \ldots \cdot b}_{k} = a^k b^k,$$

так как $ab = ba$. Если же $k < 0$, то

$$(ab)^k = \underbrace{b^{-1}a^{-1} \cdot \ldots \cdot b^{-1}a^{-1}}_{-k} = \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{-k} \underbrace{b^{-1} \cdot \ldots \cdot b^{-1}}_{-k} =$$
$$= (a^{-1})^{-k}(b^{-1})^{-k} = a^k b^k.$$

Задача 13. а) Докажите, что для любых $a, b \in S_n$ существуют и при том единственные $x, y \in S_n$, такие что $ax = b$, $ya = b$. Обязательно ли $x = y$?

б) Докажите, что для любых $a, b, c \in S_n$

$$(a = b) \iff (ac = bc) \iff (ca = cb).$$

Решение. а) Если взять $x = a^{-1}b$ и $y = ba^{-1}$, то они, очевидно, будут удовлетворять условию задачи. Подстановка x при этом совершенно

не обязательно должна быть равна подстановке y. Например, если взять $a = \binom{123}{321}$, $b = \binom{123}{132}$, то они получатся разными.

б) Достаточно заметить, что при умножении обеих частей равенства на одну и ту же подстановку (слева или справа) равенство сохраняется.

Задача 14. Докажите, что для любой подстановки $a \in S_n$ существует натуральное k, такое что $a^k = e$.

Решение. Так как подстановок длины n конечное число, среди степеней подстановки a найдутся две совпадающие: $a^n = a^m$. Тогда в качестве k можно взять $n - m$.

Определение 3. Наименьшее натуральное k, такое что для подстановки $a \in S_n$ выполняется равенство $a^k = e$, называется *порядком подстановки* a.

Задача 15. Пусть подстановка σ представлена в виде произведения независимых циклов $c_1, \ldots, c_n$. Докажите, что порядок подстановки σ равен НОК($|c_1|, \ldots, |c_n|$) (где $|c_i|$ есть длина цикла c_i).

Решение. Пусть $k = \text{НОК}(|c_1|, \ldots, |c_n|)$. Так как k делит $|c_i|$, $c_i^k = e$. Кроме того, независимые циклы коммутируют, поэтому $\sigma^k = c_1^k \cdot \ldots \cdot c_n^k = e$.

Осталось доказать, что $\sigma^l \neq e$ для $0 < l < k$. Действительно, для некоторого i число l не делит $|c_i|$, а значит $c_i^l \neq e$. Поэтому σ^l имеет нетривиальную циклическую структуру. В частности, она не равна тождественной перестановке.

Задача 16. Если k — порядок подстановки a, то $a^n = e$ тогда и только тогда, когда n делится на k.

Указание. Следует разделить n на k с остатком и доказать, что остаток не может быть отличным от нуля.

Задача 17. Вычислите: а) $\binom{123}{321}^{100}$; б) $\binom{1234}{2341}^{1000}$; в) $\binom{12345}{35214}^{-2007}$; г) $\binom{12345}{45213}^{500}$; д) $\binom{123456}{452631}^{-127}$; е) $\binom{1234567}{7651234}^{1001}$.

Указание. Для нахождения степеней подстановки удобно найти ее порядок (для чего, в свою очередь, часто бывает удобно разложить подстановку в произведение независимых циклов).

Ответ. а) $\binom{123}{123}$; б) $\binom{1234}{1234}$; в) $\binom{12345}{51423}$; г) $\binom{12345}{13542}$; д) $\binom{123456}{635124}$; е) $\binom{1234567}{4657231}$.

Целые числа 1. Делимость целых чисел

листок 7 / декабрь 2004

Это первый из серии листков про целые числа. Развитая в этих листках техника используется и для работы с многочленами (а также для работы над более общими кольцами и модулями над кольцами).

Отметим, что обсуждение целых чисел сразу начинается с делимости, а никакого определения целых чисел мы не даем. Формальное определение целых чисел можно дать, но это только запутывает суть дела.

В первой части листка обсуждаются простейшие свойства делимости. Для их доказательства достаточно аккуратно расписать определение: число a делится на число b, если и только если существует такое целое число k, что $a = k \cdot b$. Этот несложный прием может помочь и при решении более сложных задач, так как дает возможность использовать весь арсенал средств работы с равенствами — можно прибавлять к обеим частям одно и то же число, умножать левую и правую часть на одно и то же число, и т. д. Отметим еще, что если $a \vdots b$, то обязательно $b \neq 0$, поэтому равенства можно сокращать на b всюду, где это необходимо.

Важно понимать, что в листке определяется *отношение* делимости, но не *операция* деления: мы можем сказать, что некоторые числа *делятся* на другие, но нигде пока не было определено, что означает *разделить* одно число на другое (это будет сделано позже, в листках «Поля» и «Рациональные числа»). Поэтому рассуждения в стиле «разделим 5 на 7 — получим число $5/7$, которое не является целым; значит, 5 на 7 не делится» пока (до определения рациональных чисел) формально лишны смысла.

Во второй части листка впервые возникают простые числа и обсуждается разложение на простые множители (но доказательство единственности разложения отложено до следующего листка).

До последнего времени теория простых чисел являлась, в основном, предметом глубоких исследований наиболее абстрактных областей математики. Однако в последние десятилетия ряд значительных открытий в криптографии привел к тому, что такие задачи, как разложение числа на простые множители, проверка простоты числа, построение больших простых чисел, играют важнейшую роль в обмене конфиденциальной информацией. Так, в 2004 году был создан достаточно быстрый («полиномиальный») алгоритм проверки простоты числа. Но при этом задача о *разложении* числа на простые множители на сегодняшний день еще далека от эффективного решения. Одна из

наиболее популярных криптографических систем RSA основана как раз на том, что даже зная, что (достаточно большое) число m имеет ровно два простых множителя, найти их — очень сложная задача.

Соглашение. Все числа в этом листке предполагаются целыми.

Определение 1. Целое число a *делится* на ненулевое целое число b, если существует такое целое число k, что $a = kb$. В этом случае b называется *делителем* a. Говорят также, что b *делит* a.

Обозначения: $a \vdots b$ или $b \mid a$.

Задача 1. Докажите, что для любого a:

а) если $a \neq 0$, то $a \vdots a$; б) $a \vdots 1$; в) если $a \neq 0$, то $0 \vdots a$.

Решение. а) $a = 1 \cdot a$; б) $a = a \cdot 1$; в) $0 = a \cdot 0$.

Задача 2. Докажите, что для любых a, b, c, x, y:

а) если $a \vdots b$ и $b \vdots c$, то $a \vdots c$;

б) если $a \vdots b$ и $a \neq 0$, то $|a| \geqslant |b|$;

в) если $c \neq 0$, то $a \vdots b \iff ac \vdots bc$;

г) если $a \vdots b$ и $c \vdots b$, то $(a \pm c) \vdots b$;

д) если $a \vdots b$ и $c \vdots b$, то $ax + cy \vdots b$;

е) если $a \vdots b$ и $b \vdots a$, то $a = b$ или $a = -b$;

ж) если $a \vdots b$, то $ac \vdots b$;

з) если $a \vdots b$ и $c \not\vdots b$, то $(a + c) \not\vdots b$;

и) если $ab = cd$ и $a \vdots c$, то $d \vdots b$.

Решение. а) Запишем делимость в виде равенств: $a \vdots b \Rightarrow \exists k \in \mathbb{Z}\colon a = kb$, аналогично $b \vdots c \Rightarrow \exists l \in \mathbb{Z}\colon b = lc$. Получаем $a = klc \Rightarrow a \vdots c$;

б) $a \vdots b$ и $a \neq 0 \Rightarrow \exists k \in \mathbb{Z}\colon a = bk \Rightarrow |a| = |bk| = |b| \cdot |k| \Rightarrow |a| \geqslant |b|$, так как $|k| \geqslant 1$;

в) $a \vdots b \Rightarrow \exists k \in \mathbb{Z}\colon a = bk$. Обе части равенства можно домножить на ненулевое число c. Получаем $ac = bck$. Что и требовалось доказать. Обратное утверждение докажите самостоятельно.

г) $a \vdots b$ и $c \vdots b \Rightarrow \exists k, l \in \mathbb{Z}\colon (a = bk,\ c = bl) \Rightarrow a \pm c = bk \pm bl = b(k \pm l) \vdots b$.

д) $a \vdots b$ и $c \vdots b \Rightarrow \exists k, l \in \mathbb{Z}\colon (a = bk,\ c = bl) \Rightarrow ax + cy = bkx + bly = b(kx + ly) \vdots b$;

е) $a \vdots b$ и $b \vdots a \Rightarrow \exists k, l \in \mathbb{Z}\colon (a = bk, b = al) \Rightarrow a = bk = alk \Rightarrow lk = 1 \Rightarrow (l = 1, k = 1)$ или $(l = -1, k = -1)$;

ж) $a \vdots b \Rightarrow \exists k \in \mathbb{Z}\colon a = bk \Rightarrow ac = bkc \Rightarrow ac \vdots b$;

з) Докажем от противного[19]. Пусть $a + c \vdots b$, $a \vdots b$, $c \not\vdots b$, тогда $\exists k, l \in \mathbb{Z}\colon (a + c = bk, a = bl) \Rightarrow (a + c) - a = c = bk - bl = b(k - l) \Rightarrow c \vdots b$. Противоречие.

[19] В дальнейшем мы также сможем доказывать подобные утверждения, используя метод деления с остатком.

и) $ab = cd$ и $a \vdots c \Rightarrow \exists k \in \mathbb{Z}: a = ck \Rightarrow ckb = cd$. Так как $c \neq 0$, на c можно разделить обе части. Получим $kb = d$, что и требовалось доказать.

Задача 3. Верно ли, что для любых a, b, c, d:
а) если $b \mid a$ и $c \not\mid b$, то $c \mid a$;
б) если $b \mid a$ и $c \mid a$, то $bc \mid a$;
в) если $c \mid ab$, то $c \mid a$ или $c \mid b$?

Ответ. а) Нет. Например, если $a = 6$, $b = 2$, $c = 5$.

б) Нет. Например, если $a = 30$, $b = 10$, $c = 15$. Суть заключается в том, что в произведении bc простых сомножителей (с учетом повторений) больше, чем в числе a. Это достигается за счет того, что b и c содержат «повторяющийся» сомножитель 5. Заметим, что если бы b и c были бы взаимно простыми, то утверждение было бы верным. Об этом речь пойдет дальше.

в) Нет. Например, если $a = 10$, $b = 15$, $c = 6$. Здесь мы играем на том, что число c получается перемножением всех простых делителей числа ab, которые делят либо только a либо только b. Как мы увидим позднее (см. задачу 15 из листка «Целые числа 2»), для простых c это утверждение верно.

Задача 4. Сформулируйте признаки делимости (натурального числа): а) на 2; б) на 3; в) на 4; г) на 5; д) на 9; е) на 11.

Ответ. а) Число делится на 2, если его последняя цифра делится на 2 (то есть четная).

б) Число делится на 3, если сумма его цифр делится на 3.

в) Число делится на 4, если число, составленное из двух последних его цифр, делится на 4.

г) Число делится на 5, если его последняя цифра — 5 или 0.

д) Число делится на 9, если сумма его цифр делится на 9.

е) Число делится на 11, если сумма цифр, стоящих на четных местах, равна сумме цифр, стоящих на нечетных местах, по модулю 11.

Решение. Докажем сначала признаки делимости на 2 и на 5. Любое число может быть записано в виде $10k + l$, где k — какое-то целое число, а l удовлетворяет условиям $0 \leqslant l < 10$. Если у нас имеется десятичная запись числа, то его последняя цифра и есть то самое l (например, $2547 = 254 \cdot 10 + 7$). Теперь видно, что утверждения признаков делимости на 2 и на 5 элементарно следуют из задачи 2. Аналогично доказывается и признак делимости на 4. Надо лишь «отбрасывать» не один, а два последних знака.

Теперь докажем признаки делимости на 3 и на 9. Для определенности будем рассматривать десятичное число, содержащее 5 знаков — $\overline{abcde}$ (например 54728). Его можно представить в виде:

$$\begin{aligned}\overline{abcde} &= e+10d+100c+1000b+10000a = \\ &= e+d+9d+c+99c+b+999b+a+9999a = \\ &= (a+b+c+d)+9(d+11c+111b+1111a).\end{aligned}$$

Отсюда опять-таки по задаче 2з следует утверждение этого пункта.

Признак делимости на 11 доказывается при помощи очень похожего трюка:

$$\begin{aligned}\overline{abcde} &= e+10d+100c+1000b+10000a = \\ &= e+11d-d+99c+c+1001b-b+9999a+a = \\ &= 11(d+9c+91b+909a)+(a-b+c-d+e).\end{aligned}$$

Многие школьники помнят неверную формулировку признака делимости на 11, а именно: «Число делится на 11, если сумма цифр, стоящих на четных местах равна сумме цифр, стоящих на нечетных местах». Бывают числа, которые не удовлетворяют этому «признаку», однако делятся на 11. Например, число $11\cdot 5658 = 62238$.

Задача 5. Может ли число, сумма цифр которого равна 2004, быть полным квадратом?

Решение. Нет, не может. Так как сумма цифр этого числа делится на 3 и не делится на 9, само число делится на 3, но не делится на 9.

Надо сказать, что при решении задач на делимость очень часто оказывается полезным рассмотреть, какие остатки дают разные числа в задаче при делении на одно и то же число (например, на 3 и на 9, как в этой задаче).

Задача 6*. Число a в три раза больше суммы своих цифр. Докажите, что число a делится на 27.

Решение. Пусть сумма цифр числа a равна b. По условию $a = 3b$. Значит a делится на 3, тогда, по признаку делимости на 3, $b = 3c$, то есть $a = 9c$. Значит a делится на 9, и, по признаку делимости на 9, $b = 9d$, то есть $a = 27d$, что и требовалось доказать.

Задача 7. Докажите, что а) если $a^2 \vdots (a+b)$, то $b^2 \vdots (a+b)$; б*) если $x+y+z \neq 0$, то $(x^3+y^3+z^3-3xyz) \vdots (x+y+z)$.

Решение. а) Так как по условию $a^2 \vdots (a+b)$ и $a^2 - b^2 = (a-b)(a+b) \vdots (a+b)$, то, значит, и разность $a^2 - (a^2 - b^2) = b^2$ делится на $a+b$.

б) Делимость будет доказана, если мы сможем найти такой многочлен $P(x, y, z)$ с целыми коэффициентами, что $P(x, y, z)(x+y+z) = x^3 + y^3 + z^3 - 3xyz$. Ясно, что это должен быть симметричный (относительно перестановки x, y и z) однородный многочлен степени 2, поэтому его можно искать в виде $P(x, y, z) = a(x^2+y^2+z^2) + b(xy+yz+zx)$. Из определения P находим, что $a=1$, $b=-1$.

Задача 8. У каких натуральных чисел количество положительных делителей нечетно?

Ответ. У полных квадратов.

Указание. У всех остальных чисел делители разбиваются на пары (надо лишь понять — по какому принципу). Например, для числа 30 пары будут такие: (1, 30), (2, 15), (3, 10), (5, 6).

Решение. Разобъем все делители числа N на пары вида $\{k, N/k\}$. Если N не является полным квадратом, то все пары состоят из различных делителей числа N, поэтому их количество четно. Если же N — полный квадрат, то будет ровно одна пара из совпадающих делителей, поэтому их количество будет нечетно.

Определение 2. Число $p > 1$ называется *простым*, когда оно делится лишь на 1, -1, p и $-p$. Остальные натуральные числа, кроме единицы, называются *составными*.

Задача 9. Докажите, что простых чисел бесконечно много.

Указание. Следует воспользоваться следующим фактом: число $a \cdot b \cdot c + 1$ не делится ни на a, ни на b, ни на c, если каждое из них больше единицы.

Решение. Докажем методом от противного. Предположим, что простых чисел конечное число. Пронумеруем их. Пусть a_1 — первое простое число, a_2 — второе, и так далее до a_n — последнего простого числа. Тогда рассмотрим число $x = a_1 \cdot a_2 \cdot \ldots \cdot a_n + 1$. Оно не является простым. Но, с другой стороны, оно не может делиться ни на одно число, кроме x, $-x$, 1 и -1, а значит, является простым. Получили противоречие.

Пользуясь идеей этого рассуждения можно предложить следующий «алгоритм» построения простых чисел: «пусть мы знаем все простые числа до p_n включительно; тогда число $p_1 \cdot \ldots \cdot p_n + 1$ — простое». Стоит разобраться, почему это рассуждение неверно.

(Первый контрпример — $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.)

Задача 10. Докажите, что для любого n найдутся n подряд идущих составных чисел.

Решение. Вот пример n подряд идущих составных чисел: $(n+1)!+2$, $(n+1)!+3$, …, $(n+1)!+(n+1)$. Каждое из них не является простым. Действительно, первое делится на 2, второе — на 3, третье — на 4, и так далее. Напомним, что $n!$ — это обозначение для произведения $1\cdot 2\cdot \ldots \cdot (n-1)\cdot n$.

Задача 11*. Обозначим через $n?$ произведение всех простых чисел, меньших n. Докажите, что при $n>3$ выполняется неравенство $n?>n$.

Решение. Пусть $p_1, \ldots, p_k$ — все простые числа, меньшие n. Рассмотрим $N = n? - 1 = p_1 p_2 \ldots p_k - 1$; пусть m — какой-либо его простой делитель. Число N не делится ни на одно из чисел p_i, поэтому $m \geqslant n$. С другой стороны, $N+1>m$. Значит, $n?>n$.

Задача 12. а) Найдите все простые p такие, что $p+2$ и $p+4$ также простые.

б**) Докажите, что существует бесконечно много таких простых чисел p, что число $p+2$ также простое.

Ответ. а) 3.

Решение. а) Пусть p имеет вид $3k$ для некоторого целого k. Тогда оно может быть равно лишь трем. Если же p имеет вид $3k+1$ для некоторого целого k, то тогда $p+2=3k+3$ — составное, следовательно p не может иметь такой вид. Остается последняя возможность: $p=3k+2$ для некоторого целого k, но тогда $p+4=3k+6$ делится на 3, следовательно такого тоже быть не может.

б) Эта несложная на вид задача представляет собой нерешенную проблему.

Задача 13 (решето Эратосфена). На доске написаны все числа от 2 до 1000. Эратосфен обводит число 2 в кружочек и стирает все числа, отличные от 2, которые делятся на 2. Затем он повторяет этот процесс, а именно обводит в кружочек наименьшее необведенное число и стирает все остальные числа, которые делятся на это число. Процесс заканчивается, когда на доске остаются только обведенные числа. Какие числа останутся на доске? (Их не нужно выписывать.)

Ответ. На доске останутся только простые числа.

Решето Эратосфена — древний способ выписывания подряд простых чисел. Задача построения простых чисел, с одной стороны, интересовала людей еще с древности как теоретическая задача, а с другой стороны, в последнее время в связи с задачами криптографии

она приобрела и практическую ценность. Но существенно лучших алгоритмов перечисления простых чисел до сих пор не придумано.

Задача 14. Выпишите все простые числа, меньшие 100.

Решение.

91	92	93	94	95	96	97	98	99	100
81	82	83	84	85	86	87	88	89	90
71	72	73	74	75	76	77	78	79	80
61	62	63	64	65	66	67	68	69	70
51	52	53	54	55	56	57	58	59	60
41	42	43	44	45	46	47	48	49	50
31	32	33	34	35	36	37	38	39	40
21	22	23	24	25	26	27	28	29	30
11	12	13	14	15	16	17	18	19	20
	2	3	4	5	6	7	8	9	10

91				95		97			
		83		85				89	
71		73				77		79	
61				65		67			
		53		55				59	
41		43				47		49	
31				35		37			
		23		25				29	
11		13				17		19	
	②	③		5		7			

91		93		95		97		99	
81		83		85		87		89	
71		73		75		77		79	
61		63		65		67		69	
51		53		55		57		59	
41		43		45		47		49	
31		33		35		37		39	
21		23		25		27		29	
11		13		15		17		19	
	②	3		5		7		9	

91						97			
		83						89	
71		73				77		79	
61						67			
		53						59	
41		43				47		49	
31						37			
		23						29	
11		13				17		19	
	②	③		⑤		7			

						97			
				83				89	
			71		73			79	
			61				67		
					53			59	
			41		43		47		
			31				37		
					23			29	
			11		13		17	19	
				②	③	⑤	⑦		

Задача 15. Докажите, что число a — составное, если и только если a делится на какое-нибудь простое число, не превосходящее $\sqrt{a}$.

Решение. В одну сторону утверждение очевидно (a — составное, если a делится на какое-нибудь простое число, не превосходящее $\sqrt{a}$).

Докажем другую часть утверждения. Пусть a составное. Это значит, что найдутся два целых числа m и n таких, что $a = mn$, $m > 1$, $n > 1$. Если предположить, что $m > \sqrt{a}$, $n > \sqrt{a}$, то перемножая эти неравенства, получим, что $mn > a$. Противоречие.

Утверждение этой задачи существенно облегчает проверку простоты числа. Действительно, для того чтобы число было простым необходимо и достаточно, чтобы оно не делилось ни на одно простое, не превосходящее корень из данного числа, а таких простых сравнительно немного.

Задача 16. Докажите, что:

а) любое целое число, большее 1, можно представить в виде произведения простых чисел;

б) каждое целое число x, большее 1, можно представить в виде

$$x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n},$$

где $p_1 < p_2 < \dots < p_n$ — простые числа, $a_1, a_2, \dots, a_n$ — положительные целые числа;

в*) (*Основная теорема арифметики*) если число x представлено двумя способами в таком виде, а точнее

$$x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} = q_1^{b_1} q_2^{b_2} \dots q_m^{b_m},$$

то эти разложения совпадают, то есть $m = n$ и при любом $1 \leqslant i \leqslant n$ $p_i = q_i$, $a_i = b_i$;

г) если в этом разложении все a_i четны, то x есть точный квадрат, то есть найдется такое целое y, что $x = y^2$.

Решение. а) Любое целое число, большее 1, если оно не является простым, раскладывается (возможно, не единственным способом) в произведение двух чисел, больших единицы. Каждое из них либо является простым, либо также в свою очередь раскладывается в произведение. Так как на каждом шаге у нас числа уменьшаются, то ясно, что процесс разложения рано или поздно закончится и мы получим разложение на простые.

б) Очевидно следует из предыдущего пункта: надо просто сгруппировать одинаковые сомножители.

в) Основная трудность этой задачи состоит в доказательстве следующей леммы: если $ab \vdots c$, где c — простое, то либо $a \vdots c$, либо $b \vdots c$.

Эту лемму мы докажем в следующем листочке (см. задачи 16 и 17 следующего листка). А пока будем считать, что мы ее доказали.

Предположим, что у нас есть два разных разложения на простые: $x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ и $x = q_1^{b_1} q_2^{b_2} \dots q_m^{b_m}$. Запишем тождество $x = x$ в следующем виде: $(p_1 \cdot \dots \cdot p_1) \dots (p_n \cdot \dots \cdot p_n) = (q_1 \cdot \dots \cdot q_1) \dots (q_n \cdot \dots \cdot q_n)$. Поделим обе части выражения на p_1. Так как левая часть равенства делится на p_1, то делится и правая часть. Отсюда, воспользовавшись леммой (как именно?), мы получаем, что одно из чисел q делится на p_1. А так как все q простые, то отсюда следует, что $q_i = p_1$ для некоторого i. Поделим тогда обе части равенства на p_1. Получим равенство, в котором в левой и правой частях будет на один сомножитель меньше. Если предположить, что разложения у нас были разные, то, продолжая этот процесс, получим в итоге 1 с одной стороны и произведение каких-то чисел, больших единицы, с другой. Противоречие.

г) Если все a_i четны, то $x = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} = \left(p_1^{a_1/2} p_2^{a_2/2} \dots p_n^{a_n/2}\right)^2$.

Задача 17. Разложите на простые множители числа 1024, 57, 84, 91, 391, 101, 1000, 1001, 1543.

Ответ. $1024 = 2^{10}$, $57 = 3 \cdot 19$, $84 = 3 \cdot 2^2 \cdot 7$, $91 = 7 \cdot 13$, $391 = 17 \cdot 23$, 101 — простое, $1000 = 2^3 \cdot 5^3$, $1001 = 11 \cdot 13 \cdot 7$, 1543 — простое.

Целые числа 2. Алгоритм Евклида

листок 8 / декабрь 2004

В этом листке обсуждаются деление целых чисел с остатком и алгоритм Евклида нахождения наибольшего общего делителя двух целых чисел. С помощью этого доказывается ключевая лемма: если произведение делится на простое число, то на него делится один из сомножителей. Эта лемма позволяет завершить доказательство основной теоремы арифметики.

При этом, как всегда в наших листочках, утверждения сложных задач следуют из утверждений более легких, предшествующих задач. Именно поэтому, решив первые 15 задач листочка (относительно несложных), школьник без особых проблем сможет решить шестнадцатую.

Важно отметить, что техника, развиваемая в листке, позволит нам впоследствии работать с кольцом многочленов (а также с другими евклидовыми кольцами).

Соглашение. Все числа в этом листке предполагаются целыми.

Задача 1. Докажите, что для любых a и $b \neq 0$ существуют и единственны q и r такие, что: 1) $a = qb + r$; 2) $0 \leqslant r < |b|$.

Определение 1. Такие q и r называются, соответственно, *частным* и *остатком* при делении a на b.

Зададимся вопросом: какую свободу имеет математик, когда он дает определение какому-либо новому объекту. Оказывается, что не такую уж и большую. Конечно, каждый волен придумать любое определение любого объекта. Например, «ляпки — это такие тяпки, которые окапывают грядки». Но нас ведь интересуют только содержательные определения. Иными словами, когда мы определяем некоторый объект, мы обычно уже представляем его. А потому хотим, чтобы выполнялись какие-то свойства. В связи с чем довольно часто очень полезными для понимания определяемого объекта являются вопросы: «А почему нам дали именно такое определение? Нельзя ли что-нибудь заменить или выкинуть из него так, чтобы оно все еще соответствовало нашим представлениям об объекте? Существует ли то, что мы определили?» И тому подобные вопросы.

Вышеописанной «игрой» с определением мы сейчас и займемся на примере. Заметим еще раз, что основной целью является лучшее понимание и усвоение материала школьниками.

Итак, вопрос: что будет с определением 1, если условие 2 заменить на одно из следующих условий?

а) $0 < r < |b|$

(Ответ: такое определение нам не подходит, потому что по нему не для любых двух чисел a и $b \neq 0$ найдутся частное и остаток. А именно: не найдутся они для чисел, одно из которых делится на другое.)

б) $0 < r \leqslant |b|$

(Ответ: а вот такое определение вполне можно было бы принять. Оно отличается от нашего только тем, что остаток от деления одного числа на другое в случае, когда первое делится нацело на второе, равен второму числу, а не нулю.)

в) $0 \leqslant r < 2|b|$

(Ответ: если бы было такое определение, то частное и остаток были бы определены неоднозначно. Например, $7 = 2 \cdot 3 + 1 = 1 \cdot 3 + 4$. В этом случае при делении 7 на 3 мы получаем частное 2 и остаток 1 или частное 1 и остаток 4.)

г) $0 \leqslant r < b$

(Ответ: при таком определении остатка не существует для отрицательных b.)

д) $-|b| \leqslant r < |b|$

(Ответ: в этом случае у нас опять-таки частное и остаток определены неоднозначно.)

Решение. Случаи $b < 0$ и $b > 0$ разбираются аналогично, поэтому мы приведем решение только для случая $b < 0$. Поскольку $b(|a| + 1) < a < b(-|a| - 1)$, множество целых чисел q, для которых $bq \leqslant a$, непусто и ограничено снизу. Рассмотрим наименьший элемент q_0 этого множества. Тогда $bq_0 \leqslant a$, $b(q_0 - 1) > a$, то есть $0 \leqslant a - q_0 b < -b = |b|$. Таким образом, можно взять q_0 в качестве неполного частного, а $r_0 = a - q_0 b$ в качестве остатка.

Докажем теперь единственность частного и остатка. Пусть существует две пары (q_1, r_1) и (q_2, r_2): $a = bq_1 + r_1$, $a = bq_2 + r_2$. Вычитая эти равенства, получаем $b(q_1 - q_2) = r_2 - r_1$, то есть число $r_2 - r_1$ делится на число b. Но при $0 \leqslant r_1 < |b|$, $0 \leqslant r_2 < |b|$ модуль разности $r_2 - r_1$ не превосходит $|b| - 1$, а значит, $r_1 = r_2$, откуда $q_1 = \frac{a - r_1}{b} = \frac{a - r_2}{b} = q_2$, и пары (q_1, r_1) и (q_2, r_2) на самом деле совпадают.

> **Задача 2.** Найдите частное и остаток при делении: а) -17 на 4; б) 23 на -7; в) -1 на -5.

Ответ. а) $q = -5$, $r = 3$, так как $-17 = 4 \cdot (-5) + 3$.

б) $q = -3$, $r = 2$.

в) $q = 1$, $r = 4$.

Задача 3. Какие частные могут получиться при делении числа 59?

Ответ. 59, −59, 29, −29, 19, −19, 14, −14, 11, −11, 9, −9, 8, −8, 7, −7, 6, −6, 5, −5, 4, −4, 3, −3, 2, −2, 1, −1, 0.

Ответ получен путем перебора делителей от 1 до 60 с разными знаками. Очевидно, что если брать делители по модулю большие 60, то частное будет нулем.

Задача 4. Найдите частное и остаток при делении: а) n^2 на $n+1$; б) n^2+n+2 на $n-1$; в) $2^{100}-1$ на 2^7-1; г*) 2^m-1 на 2^n-1.

Решение. а) $n^2=(n-1)(n+1)+1$. Частное — $(n-1)$, остаток — 1.

б) В этой задаче речь идет о делении чисел, но решается она при помощи метода деления многочленов «столбиком»:

$$\begin{array}{r|l} n^2+n+2 & n-1 \\ \underline{n^2-n} & \underline{} \\ 2n+2 & n+2 \\ \underline{2n-2} & \\ 4 & \end{array}$$

благодаря которому находим следующее соотношение: $n^2+n+2=$ $=(n-1)(n+2)+4$. Поэтому при $n>5$ и $n<-4$ остаток будет равен 4, а частное — $(n+2)$. Случаи, когда $n-1$ равно ±4, ±3, ±2, ±1 следует рассмотреть отдельно (сделайте это самостоятельно в качестве упражнения).

в) В этом пункте также следует применить деление «столбиком».

$$\begin{array}{r|l} 2^{100}-1 & 2^7-1 \\ \underline{2^{100}-2^{93}} & \underline{\phantom{2^{93}+2^{86}+2^{79}+2^{72}+\ldots+2^2}} \\ 2^{93}-1 & 2^{93}+2^{86}+2^{79}+2^{72}+\ldots+2^2 \\ \underline{2^{93}-2^{86}} & \\ 2^{86}-1 & \\ \underline{2^{86}-2^{79}} & \\ 2^{79}-1 & \\ \underline{2^{79}-2^{72}} & \\ \ddots & \\ \underline{} & \\ 2^9-1 & \\ \underline{2^9-2^2} & \\ 2^2-1 & \end{array}$$

г) Начнем делить 2^m-1 на 2^n-1 в столбик: $2^m-1-2^{m-n}(2^n-1)=$ $=2^{m-n}-1$. Заметим, что мы свели задачу к аналогичной для чисел $m-n$ и n. Продолжая деление дальше, получим формулу

$$2^m-1=(2^{m-n}+2^{m-2n}+\ldots+2^{m-qn})(2^n-1)+2^r-1,$$

где q и r — частное и остаток от деления m на n. Итак, получили частное $2^{m-n}+\ldots+2^{m-qn}$ и остаток 2^r-1.

Задача 5*. а) Покажите, что $a^{2k+1}+1$ всегда делится на $a+1$ без остатка.

б) Найдите остаток от деления $a^{2k}+1$ на $a+1$.

Вообще, можно показать, что остаток от деления многочлена $P(x)$ на многочлен $x-x_0$ есть число $P(x_0)$.

Решение. а) $a^{2k+1}+1=(a+1)(a^{2k}-a^{2k-1}+\ldots+1)$.

б) Докажем, что остаток равен 2, то есть $a^{2k}-1$ делится на $a+1$. Действительно, $a^{2k}-1=a(a^{2k-1}+1)-(a+1)$. Вычитаемое делится на $a+1$ в силу предыдущего пункта, следовательно, и разность делится на $a+1$.

Определение 2. *Наибольшим общим делителем* чисел a и b называется наибольшее из таких чисел d, что $a\vdots d$, $b\vdots d$.

Обозначение: НОД(a,b).

Задача 6. Докажите, что для любых a и b ($a\neq 0$ или $b\neq 0$) НОД(a,b) существует и единственен.

Решение. Множество чисел, которые делят сразу и a, и b, непусто, так как по крайней мере оно содержит единицу. Кроме того, среди всех таких чисел существует наибольшее, так как каждое из них не превосходит $|b|$ (почему?), следовательно, их существует лишь конечное количество для каждой пары a и b. Значит, перебрав их все, мы можем найти наибольшее (оно точно будет положительным).

Задача 7. Докажите, что для любых a, b и c ($a\neq 0$ или $b\neq 0$):

а) НОД$(a,b)\geqslant 1$; б) НОД$(a,b)=|a|\Leftrightarrow b\vdots a$;

в) НОД$(a,ca+b)=$НОД(a,b).

Решение. а) См. решение предыдущей задачи.

б) Заметим, что НОД$(a,b)=|a|\Rightarrow b\vdots a$. Теперь докажем, что $b\vdots a\Rightarrow$ $\Rightarrow$ НОД$(a,b)=|a|$. Так как $b\vdots a$, то $|a|$ — общий делитель чисел a и b. Но ясно также, что большего делителя обоих чисел быть не может, так как a не может делиться на число, большее по модулю, чем $|a|$.

в) Эта на первый взгляд несложная и ничем вроде не примечательная задача очень важна для доказательства того, что при помощи алгоритма Евклида действительно получается НОД двух чисел.

Итак, начнем доказательство. Введем обозначения: пусть $d = \text{НОД}(a, b)$, $D = \text{НОД}(a, ca + b)$, $a = dx$, $b = dy$. Заметим, что и $a = dx$, и $ca + b = d(cx + y)$ делятся на d. Значит, d — общий делитель чисел a и $ca + b$. Следовательно, $D \geqslant d$ (потому что D — *наибольший* общий делитель чисел a и $ca + b$).

Теперь докажем неравенство в другую сторону. Так как a делится на D, то и ca делится на D. А из того, что ca и $ca + b$ делятся на D, следует, что и их разность b делится на D. Значит, D — общий делитель чисел a и b. Следовательно, $d \geqslant D$.

Из всего вышесказанного следует, что $D = d$.

Задача 8 (алгоритм Евклида). Рассмотрим следующий процесс. Пусть (a, b) — пара положительных чисел такая, что $a \geqslant b$. Она заменяется на пару (b, r), где r — остаток от деления a на b. Пара (b, r) заменяется по тому же правилу и так далее. Процесс завершается, когда получается пара вида $(d, 0)$. Покажите, что:

а) процесс всегда завершается;

б) $d = \text{НОД}(a, b)$.

Решение. а) Процесс всегда завершается, так как для каждой следующей пары второе число будет по модулю строго меньше (условие 2 в определении 1) второго числа предыдущей пары. Поэтому ясно, что рано или поздно мы получим пару, в которой второе число будет равно нулю, и процесс завершится.

б) Из пункта в) предыдущей задачи следует, что при каждой замене у пар (a, b) и (b, r) будет одинаковый НОД. Значит, у первой пары и у последней — одинаковые НОД. А это и означает, что $d = \text{НОД}(a, b)$.

Задача 9. Вычислите при помощи алгоритма Евклида

а) НОД(91, 147); б) НОД(−144, −233).

Решение. а) $\text{НОД}(91, 147) = \text{НОД}(147, 91)$. Распишем для последней пары алгоритм Евклида: $(147, 91) \to (91, 56) \to (56, 35) \to (35, 21) \to$ $\to (21, 14) \to (14, 7) \to (7, 0)$. Значит, $\text{НОД}(91, 147) = 7$.

б) $\text{НОД}(-144, -233) = \text{НОД}(233, 144)$. Распишем для последней пары алгоритм Евклида: $(233, 144) \to (144, 89) \to (89, 55) \to$ $\to (55, 34) \to (34, 21) \to (21, 13) \to (13, 8) \to (8, 5) \to (5, 3) \to (3, 2) \to$ $\to (2, 1) \to (1, 0)$. Значит, $\text{НОД}(-144, -233) = 1$.

Задача 10. Пусть $0 < a < 1000$, $0 < b < 1000$. Верно ли, что алгоритм Евклида закончится после не более, чем а) 14; б) 13 шагов?

Решение. Рассмотрим следующую последовательность пар алгоритма Евклида, записанную в обратном порядке: $(1, 0) \leftarrow (2, 1) \leftarrow (3, 2) \leftarrow$ $\leftarrow (5, 3) \leftarrow (8, 5) \leftarrow (13, 8) \leftarrow (21, 13) \leftarrow (34, 21) \leftarrow (55, 34) \leftarrow (89, 55) \leftarrow$ $\leftarrow (144, 89) \leftarrow (233, 144) \leftarrow (377, 233) \leftarrow (610, 377) \leftarrow (987, 610)$. $(*)$

Если обратить эту последовательность, то мы получим алгоритм Евклида, который заканчивается после 14 шагов (таким образом, ответ на второй вопрос задачи отрицательный).

Будем говорить что пара (a, b) «не меньше» пары (c, d), если $a \geqslant c$ и $b \geqslant d$. Теперь предположим, что нам удалось найти такие a и b, по модулю меньшие тысячи, что алгоритм Евклида для них заканчивается более чем через 14 шагов. Запишем его «задом наперед» и обозначим $(**)$. Докажем, что для каждого номера i будет выполняться следующее: i-я скобка $(**)$ «не меньше» i-й скобки $(*)$. Доказательство проведем по индукции.

База индукции: первая пара $(**)$ имеет вид $(d, 0)$, а значит, она не меньше пары $(1, 0)$.

Шаг индукции: Пусть некоторая i-я пара (m, n) последовательности $(**)$ не меньше пары (k, l) последовательности $(*)$. Тогда пара $(m+n, m)$, которая следует после пары (m, n) в $(**)$, не меньше пары $(k+l, k)$, которая следует после пары (k, l) в $(*)$.

Тогда получается, что пара, полученная после 15 шагов алгоритма $(**)$, будет не меньше пары $(1597, 987)$, но это противоречит тому, что и a и b меньше 1000.

Задача 11. Покажите, как при помощи алгоритма Евклида можно по произвольным a и b найти такие k и l, что $ak + bl = \text{НОД}(a, b)$.

Набросок решения. Выполняя алгоритм Евклида, будем представлять каждое возникающее при этом число в виде $ak + bl$. Тогда на предпоследнем шаге $\text{НОД}(a, b)$ окажется представленным в этом виде. Продемострируем это на примере $a = 147$, $b = 91$:

$$
\begin{array}{rrr}
(147, 91) & 147 = & 147 \cdot 1 + 91 \cdot 0 \\
 & 91 = & 147 \cdot 0 + 91 \cdot 1 \\
(91, 56) & 56 = 147 - 91 = & 147 \cdot 1 - 91 \cdot 1 \\
(56, 35) & 35 = 91 - 56 = & -147 \cdot 1 + 91 \cdot 2 \\
(35, 21) & 21 = 56 - 35 = & 147 \cdot 2 - 91 \cdot 3 \\
(21, 14) & 14 = 35 - 21 = & -147 \cdot 3 + 91 \cdot 5 \\
(14, 7) & 7 = 21 - 14 = & 147 \cdot 5 - 91 \cdot 8 \\
(7, 0) & 0 = 14 - 2 \cdot 7 = & -147 \cdot 13 + 91 \cdot 21
\end{array}
$$

Задача 12. Докажите, что уравнение $ax + by = d$ имеет решение в целых числах тогда и только тогда, когда $d \vdots \text{НОД}(a, b)$. В частности, $\text{НОД}(a, b)$ — это наименьшее натуральное число, представимое в виде $ax + by$.

Решение. ($\Rightarrow$) Пусть уравнение $ax + by = d$ имеет решение в целых числах. Но тогда правая часть делится на $\text{НОД}(a, b)$, а значит, должна делиться и левая. То есть $d \vdots \text{НОД}(a, b)$.

($\Leftarrow$) Пусть $d \vdots \text{НОД}(a, b)$, т. е. $m\,\text{НОД}(a, b) = d$. В силу предыдущей задачи существуют такие целые числа k_0 и l_0, что $ak_0 + bl_0 = \text{НОД}(a, b)$. Тогда $x = k_0 m$, $y = l_0 m$ — решение уравнения $ax + by = d$.

Задача 13. Даны углы в 32° и 25°. Постройте угол в 1°.

Решение. Воспользовавшись задачей 11, найдем целые числа k и l, для которых $32k + 25l = 1$: $7 = 32 - 25$, $4 = 25 - 3 \cdot 7 = 4 \cdot 25 - 3 \cdot 32$, $3 = 7 - 4 = 4 \cdot 32 - 5 \cdot 25$, $1 = 4 - 3 = 9 \cdot 25 - 7 \cdot 32$. Таким образом, достаточно отложить от некоторого луча девять раз угол в 25° против часовой стрелки, а от получившегося луча отложить семь раз угол в 32° по часовой стрелке.

Задача 14. Докажите, что если p — простое, то либо a делится на p, либо найдутся такие x и y, что $ax + py = 1$.

Решение. Если p — простое и a не делится на p, то это означает, что a и p взаимно просты (т. е. их НОД равен единице), а отсюда и из задачи 11 следует, что найдутся такие x и y, что $ax + py = 1$.

Задача 15. Пусть p — простое число. Докажите, что если $ab \vdots p$, то $a \vdots p$ или $b \vdots p$.

Решение. Предположим противное. То есть пусть $ab \vdots p$, но $a \not\vdots p$ и $b \not\vdots p$. Тогда по предыдущей задаче найдутся такие x_1, x_2, y_1 и y_2, что будет выполнено следующее: $ax_1 + py_1 = 1$, $bx_2 + py_2 = 1$. Теперь перемножим левые и правые части этих равенств и получим: $abx_1x_2 + py_1bx_2 + py_2ax_1 + p^2y_1y_2 = 1$; так как $ab \vdots p$, то левая часть делится на p, а правая — не делится. Получили противоречие.

Задача 16. Докажите основную теорему арифметики (задача 16в листка «Целые числа 1»).

Решение. Напомним, что в предыдущем листочке мы свели доказательство основной теоремы арифметики к следующему факту. Пусть у нас есть два разложения числа на простые множители:

$$x = p_1 \cdot p_2 \cdot \ldots \cdot p_n = q_1 \cdot q_2 \cdot \ldots \cdot q_m$$

(где $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_n$ — необязательно различные простые множители), тогда каждый простой множитель из левой части обязательно присутствует в правой и наоборот.

Докажем, например, что p_1 присутствует в правой части. Так как $q_1 \cdot q_2 \cdot \ldots \cdot q_n = q_1 \cdot (q_2 \cdot \ldots \cdot q_n) \vdots p_1$, то по задаче 15 либо $q_1 \vdots p_1$ (и тогда $q_1 = p_1$, так как оба числа простые), либо $q_2 \cdot \ldots \cdot q_n = q_2 \cdot (q_3 \cdot \ldots \cdot q_n) \vdots \vdots p_1$. Опять, воспользовавшись задачей 15, получаем, что либо $q_2 \vdots p_1$ (и тогда $q_2 = p_1$, так как оба числа простые), либо $q_3 \cdot \ldots \cdot q_n = = q_3 \cdot (q_4 \cdot \ldots \cdot q_n) \vdots p_1$. Применяя вышеописанную процедуру, мы рано или поздно получаем, что p_1 совпадет с одним из множителей q_i.

Определение 3. *Наименьшим общим кратным* чисел a и b называется наименьшее из таких положительных чисел d, что $d \vdots a$, $d \vdots b$.

Обозначение: НОК(a, b).

Задача 17. Докажите, что для любых a и b $(ab \neq 0)$:

а) НОК(a, b) существует и единственен;

б) НОК$(a, b) \cdot$ НОД$(a, b) = ab$.

Решение. а) Множество положительных чисел, которые делятся на a и на b, непусто, так как по крайней мере число $|ab|$ там содержится. Кроме того, оно ограничено снизу, так как наименьшее общее кратное не может быть меньше модулей каждого из чисел a и b. Значит, в этом множестве найдется наименьший элемент.

б) Обозначим НОД(a, b) через d. Пусть a_1 и b_1 — такие числа, что $a = d \cdot a_1$, $b = d \cdot b_1$. Обозначим НОК$(a, b)/d$ через D. Тогда D делится и на a_1, и на b_1. Поскольку a_1 и b_1 взаимно просты, D делится на их произведение $a_1 b_1$, а значит, НОК(a, b) делится на $a_1 b_1 d$, откуда НОК$(a, b) \geqslant a_1 b_1 d$. Но число $a_1 b_1 d$ делится на a и b. Следовательно, НОК$(a, b) = a_1 b_1 d$ и НОД$(a, b) \cdot$ НОК$(a, b) = d \cdot a_1 b_1 d = ab$.

Задача 18. Найдите НОК$(12, 15)$, НОК$(120, 45)$.

Ответ. НОК$(12, 15) = 3 \cdot 4 \cdot 5 = 60$, НОК$(120, 45) = 3 \cdot 5 \cdot 2^3 \cdot 3 = 360$.

Задача 19. Пусть (x_0, y_0) — решение уравнения

$$ax + by = d.$$

Пусть a_0 и b_0 — такие числа, что НОД$(a, b)a_0 = a$, НОД$(a, b)b_0 = b$. Покажите, что каждое решение уравнения $ax + by = d$ имеет вид

$$x = x_0 + b_0 t, \quad y = y_0 - a_0 t,$$

где $t \in \mathbb{Z}$.

Решение. Очевидно, что x и y такого вида являются решением. Докажем, что все решения имеют такой вид. Пусть (x, y) — какое-либо

решение уравнения. Тогда, вычитая равенство $ax_0 + by_0 = d$ из равенства $ax + by = d$, получаем $a(x - x_0) + b(y - y_0) = 0$. Сокращая на НОД$(a, b)$, приходим к $a_0(x - x_0) + b_0(y - y_0) = 0$.

Выберем теперь k и l так, что $a_0k + b_0l = 1$. Тогда $a_0(x - x_0) + b_0(y - y_0) = 0$ влечет

$$0 = a_0k(x - x_0) + b_0k(y - y_0) = (x - x_0) + b_0(k(y - y_0) - l(x - x_0)).$$

Значит, $x - x_0$ делится на b_0, и можно записать $x - x_0 = b_0t$. Отсюда получаем, что $a_0b_0t + b_0(y - y_0) = 0$, откуда $y - y_0 = -a_0t$.

Задача 20. Решите уравнения:
а) $121x + 91y = 1$; б) $-343x + 119y = 42$; в) $111x - 740y = 11$.

Решение. а) Найдем частное решение при помощи алгоритма Евклида (см. задачу 11): $30 = 121 - 91$, $1 = 91 - 3 \cdot 30 = 4 \cdot 91 - 3 \cdot 121$, то есть $(-3, 4)$ — частное решение. Отсюда и из предыдущей задачи получаем, что общее решение исходного уравнения будет иметь вид

$$x = -3 + 91t, \quad y = 4 - 121t,$$

б) Аналогично предыдущему пункту воспользуемся алгоритмом Евклида: $105 = 343 - 2 \cdot 119$, $14 = 119 - 105 = 3 \cdot 119 - 343$, $7 = 105 - 7 \cdot 14 = 8 \cdot 343 - 23 \cdot 119$. Получили, что НОД$(343, 119) = 7 = 8 \cdot 343 - 23 \cdot 119$. При этом в качестве частного решения можно взять $x = -8 \cdot 6 = -48$, $y = -23 \cdot 6 = -138$ и $343 = 49 \cdot 7$, $119 = 17 \cdot 7$. Следовательно, в силу задачи 19 общий вид решения этого уравнения имеет вид

$$x = -48 + 17t, \quad y = -138 + 49t.$$

в) Поскольку левая часть уравнения делится на 37, а правая не делится, уравнение не имеет решения.

Задача 21*. Есть шоколадка в форме равностороннего треугольника со стороной n, разделенная бороздками на равносторонние треугольники со стороной 1. Играют двое. За ход можно отломить от шоколадки треугольный кусок вдоль бороздки, съесть его, а остаток передать противнику. Тот, кто получит последний кусок — треугольник со стороной 1, — победитель. Тот, кто не может сделать ход, досрочно проигрывает. Кто выигрывает при правильной игре?

Решение (дается по книге: Р. М. Федоров и др., Московские математические олимпиады 1993–1995 г., МЦНМО, 2006). После первого хода всегда образуется равнобедренная трапеция. Посмотрим, какие фигуры могут образоваться на последующих ходах при правильной игре.

Пусть на каком-то ходу один из игроков (назовем его А) получил шоколадку в форме равнобедренной трапеции с меньшим основанием a и большим основанием b (длина боковой стороны такой трапеции равна $b-a$). Если А отломит треугольник, сторона которого меньше, чем $b-a$, то другой игрок (назовем его Б) отломит треугольник со стороной 1, и у игрока А не будет возможности сделать ход и он проиграет. Следовательно, в этой ситуации он должен отломать треугольник со стороной $b-a$. После этого хода остается параллелограмм, длины сторон которого равны a и $b-a$.

Пусть игрок получил шоколадку в форме параллелограмма со сторонами a и b, причем $a<b$. Тогда по аналогичным соображениям он должен отломать треугольник со стороной a. После этого хода остается равнобедренная трапеция с основаниями $b-a$ и b.

Таким образом, если в некоторый момент один из игроков получил шоколадку в форме параллелограмма со сторонами a и b $(a<b)$, то через два хода он получит шоколадку в форме параллелограмма со сторонами a и $b-a$. Если же один из игроков получил параллелограмм с равными сторонами (т. е. ромб), то после его хода образуется треугольник.

Теперь приведем выигрышную стратегию для второго игрока при простом n: ему достаточно каждый раз отламывать кусок наибольшего размера. Покажем, что эта стратегия приводит к выигрышу. Пусть первый игрок отломал треугольник со стороной k. После хода второго игрока образовался параллелограмм со сторонами k и $n-k$. Эти числа взаимно просты, так как n — простое число. Далее, после каждого хода второго игрока будет получаться параллелограмм (пока в конце концов не получится ромб). Длины сторон этого параллелограмма взаимно просты. Значит, длины сторон ромба тоже взаимно просты. Но это означает, что получится ромб со стороной 1! Первый будет вынужден отломать от него треугольник со стороной 1, после чего второй выигрывает.

Если $n=1$, то первый уже выиграл.

Пусть теперь число n составное. Обозначим через p любой простой делитель числа n. Пусть первый сначала отломает треугольник со стороной p, а потом каждый раз отламывает самый большой кусок (за исключением случая, когда он получает пятиугольник — тогда он отламывает треугольник со стороной 1 и игра заканчивается). Через некоторое время второй игрок получит треугольник со стороной p и, как было разобрано выше, через несколько ходов проиграет.

Описанный процесс есть не что иное, как алгоритм Евклида.

Отношения эквивалентности

листок 9 / январь 2005

Чтобы решить задачу, часто полезно выделить то существенное, что нужно для ее решения. Для это можно некоторые объекты объявить «равными». Например, в геометрии обычно считают равными фигуры, которые можно «совместить наложением», так как они (хотя и отличаются как множества точек) имеют одинаковые свойства; проявлением этой идеи в наших листках является переход от чисел к остаткам (например, при решении целочисленных уравнений). В ботанике растения делят на классы, семейства или виды в зависимости от конкретных задач исследования.

Математической формализацией этой идеи являются отношения эквивалентности.

Определение 1. Пусть M — множество. Произвольное множество $R \subset \{(a, b) \mid a, b \in M\}$ упорядоченных пар элементов M называется (*бинарным*) *отношением* на M. Если $(a, b) \in R$, то пишут $a \sim_R b$, или просто $a \sim b$.

Бинарные отношения на конечном множестве можно задавать в виде таблицы. А именно, по отношению R построим таблицу $n \times n$, где над строками и перед столбцами написаны наши элементы в одной и той же последовательности. А в клетке с координатами (a, b) стоит 1 тогда и только тогда, когда пара (a, b) принадлежит R.

Можно также задавать отношение с помощью ориентированного графа с петлями — точек и стрелок, таких что из одной точки в другую ведет не более одной стрелки: из a в b ведет стрелка, если и только если $a \sim_R b$; при этом, если $a \sim_R a$, то это условие обозначается «петлей» — стрелкой, ведущей из вершины в себя.

Задача 0. Изобразите в виде таблицы и в виде графа отношения:

а) $a \sim_R b$, если $a \equiv b \pmod 2$ на $X = \{0, \ldots, 9\}$.

б) $a \sim_R b$, если $b \mid a$ на $X = \{2, \ldots, 15\}$ (в этом пункте таблицу рисовать не надо).

в) $A \sim_R B$, если $A \subset B$ на множестве всех подмножеств множества $\{0, 1, 2\}$.

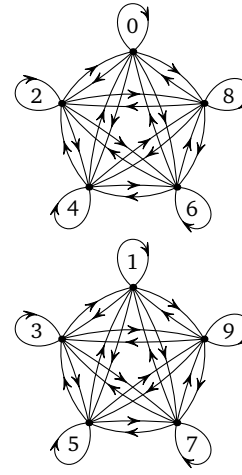
г) $a \sim_R b$, если $a = b$ на $X = \{0, \ldots, 5\}$.

д) $a \sim_R b$, если $a \geqslant b$ на $X = \{0, \ldots, 5\}$.

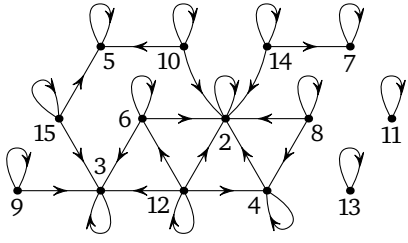
Ответ. См. страницы 172–173.

а)

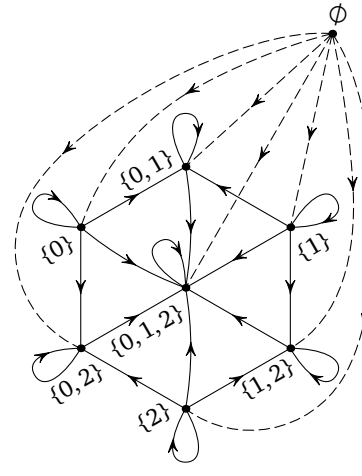
	0	1	2	3	4	5	6	7	8	9
0	1		1		1		1		1	
1		1		1		1		1		1
2	1		1		1		1		1	
3		1		1		1		1		1
4	1		1		1		1		1	
5		1		1		1		1		1
6	1		1		1		1		1	
7		1		1		1		1		1
8	1		1		1		1		1	
9		1		1		1		1		1



б)



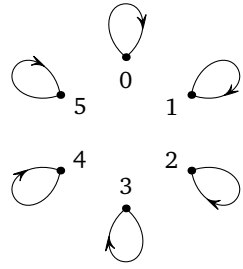
в)



	∅	{0}	{1}	{2}	{0, 1}	{1, 2}	{0, 2}	{0, 1, 2}
∅	1	1	1	1	1	1	1	1
{0}		1			1		1	1
{1}			1		1	1		1
{2}				1		1	1	1
{0, 1}					1			1
{1, 2}						1		1
{0, 2}							1	1
{0, 1, 2}								1

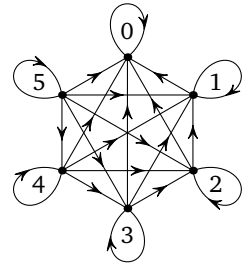
г)

	0	1	2	3	4	5
0	1					
1		1				
2			1			
3				1		
4					1	
5						1



д)

	0	1	2	3	4	5
0	1					
1	1	1				
2	1	1	1			
3	1	1	1	1		
4	1	1	1	1	1	
5	1	1	1	1	1	1



Определение 2. Отношение $\sim$ на M называется:

1) рефлексивным, если из $a \in M$ следует $a \sim a$;

2) симметричным, если для любых $a, b \in M$ из $a \sim b$ следует $b \sim a$;

3) транзитивным, если для любых $a, b, c \in M$ из $a \sim b$ и $b \sim c$ следует $a \sim c$.

Решать задачи 1–4 надо «одновременно», разбирая конкретные примеры из задач 3 и 4, возвращаясь к утверждениям задач 1 и 2.

Задача 1. Сколько существует отношений на множестве из n элементов? Сколько существует симметричных отношений на множестве из n элементов?

Решение. Отметим, что отношение — это множество упорядоченных пар элементов, а симметричное отношение — это множество неупорядоченных пар. Число отношений на множестве из n элементов — это число подмножеств в множестве упорядоченных пар, т. е. в множестве из n^2 элементов. Как мы уже знаем, число таких подмножеств равно 2^{n^2}.

Если задавать отношение в виде таблицы, то симметричным отношениям отвечают симметричные относительно диагонали таблицы, поэтому если заполнена диагональ и верхний треугольник, то тогда нижний треугольник заполняется из соображений симметрии. При этом диагональ и верхний треугольник можно заполнять произволь-

но, а это $\frac{n(n+1)}{2}$ клеток. Поэтому симметричных отношений будет $2^{n(n+1)/2}$.

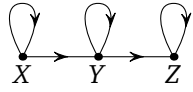
Задача 2. Приведите примеры отношений, которые удовлетворяют ровно одному, ровно двум свойствам из определения 2.

Как мы уже заметили, симметричным отношениям отвечают симметричные относительно диагонали таблицы. У рефлексивных отношений в таблице на главной диагонали стоят единицы. Транзитивность легко увидеть из таблицы нельзя.

Если задавать отношение в виде графа, то симметричным отношениям отвечают графы, в которых, если есть стрелка из a в b, то есть и обратная стрелка из b в a. Для графа рефлексивного отношения у всех вершин должны быть петли. Если отношение транзитивно, то «для любого длинного пути есть прямой путь», а именно, если есть ориентированный путь из a в b, то из a в b ведет стрелка.

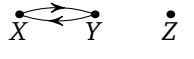
Решение. В этой задаче мы приведем примеры в виде таблицы и в виде графа.

1) Рефлексивное, но не симметричное и не транзитивное отношение.



	X	Y	Z
X	1		
Y	1	1	
Z		1	1

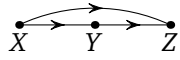
2) Симметричное, но не рефлексивное и не транзитивное отношение.



	X	Y	Z
X		1	
Y	1		
Z			

Другой пример — отношение «$a \neq b$».

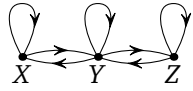
3) Транзитивное, но не симметричное и не рефлексивное отношение.



	X	Y	Z
X			
Y	1		
Z	1	1	

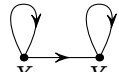
Другой пример — отношение «$a > b$» (например, на множестве целых чисел).

4) Рефлексивное и симметричное, но не транзитивное отношение. Отношение «a и b учились в одной школе». Это отношение не транзитивно, поскольку человек b моге учиться в двух школах (в одной школе вместе с a, а в другой — вместе с c).



	X	Y	Z
X	1	1	
Y	1	1	1
Z		1	1

5) Рефлексивное и транзитивное, но не симметричное отношение.



	X	Y
X	1	
Y	1	1

Другим примером является отношение «$a \leqslant b$».

6) Симметричное и транзитивное, но не рефлексивное отношение. Самый простой пример — это пустое отношение на множестве из одного элемента.

На самом деле из симметричности и транзитивности отношения R «почти следует» рефлексивность. Действительно, если $a \sim_R b$, то по симметричности $b \sim_R a$ и по транзитивности $a \sim_R a$. Значит, если элемент a находится в отношении R с каким-то элементом b, то для a «выполняется рефлексивность». Поэтому если на X задано симметричное и рефлексивное отношение R, то множество X делится на две непересекающиеся части: $X = X_1 \sqcup X_2$, при этом на X_1 отношение R будет отношением эквивалентности, а на X_2 отношение R будет пустым отношением, т. е. никакой элемент из X_2 не находится в отношении ни с каким элементом X.

Задача 2 показывает, что ни из каких двух свойств отношений не следует третье.

Определение 3. Отношение $\sim$ на M называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Задача 3. Укажите, какие из следующих отношений являются рефлексивными, симметричными, транзитивными, отношениями эквивалентности (в кавычках указано условие, при котором $a \sim b$)

а) $a \sim b$ для всех $a, b \in M$, на множестве M;
б) $\varnothing$ на множестве M;
в) «$a \mid b$» на множестве натуральных чисел;
г) «a и b можно соединить путём» на множестве вершин графа;
д) «$A \subset B$» на множестве всех подмножеств данного множества;

е) «a и b имеют один и тот же остаток при делении на 2» на множестве натуральных чисел;

ж) «a и b имеют одну и ту же последнюю цифру» на множестве натуральных чисел;

з) «a и b учатся в одном классе» на множестве учеников 57 школы;

и) «a и b родились в одном месяце» на множестве учеников 8 «в» класса 57 школы;

к) «между a и b существует биекция» на множестве всех подмножеств множества натуральных чисел;

л) «$a > b$» на множестве натуральных чисел;

м) фиксируем $X \subset M$. Отношение на множестве M зададим правилом «$a \sim a$ и, если $a \neq b$, то $a \sim b$, если и только если $a, b \in X$»;

н) фиксируем $f\colon X \to Y$. Отношение на множестве X зададим правилом «$a \sim b$ если и только если $f(a) = f(b)$;

о) «a и b являются гражданами одного государства» на множестве людей на Земле;

п) «три стороны одного треугольника равны трём сторонам второго треугольника» на множестве всех треугольников на плоскости;

р) выбранное вами отношение на множестве натуральных чисел;

с) выбранное вами отношение на множестве учеников 57 школы.

Решение. а) Это отношение является отношением эквивалентности (так как все возможные пары в него входят).

б) Если M — непустое множество, то это отношение не будет рефлексивным, но будет симметричным и транзитивным.

Этот пункт обычно трудно дается школьникам. В этом месте стоит напомнить, что «все летающие крокодилы являются учениками этого класса.» И точно так же для любых $a, b \in M$, таких что $a \sim b$, выполнено $b \sim a$ (потому что таких a и b не найдется!).

в) Отношение рефлексивно, так как всегда $a \mid a$, транзитивно (если $a \mid b$ и $b \mid c$, то $a \mid c$), но не симметрично ($2 \mid 4$, но $4 \nmid 2$).

г) Это отношение эквивалентности.

д) Ясно, что это отношение рефлексивно и не симметрично. Отношение транзитивно, так как если $A \subset B$ и $B \subset C$, то тогда $A \subset C$.

е) Это отношение эквивалентности (при этом можно рассматривать остатки при делении на любое число).

Заметим, что можно это переформулировать следующим способом: «$a \sim b$ тогда и только тогда, когда a и b оба четны или оба нечетны.»

Это отношение эквивалентности в будущем понадобится при рассмотрении остатков по модулю какого-либо числа.

ж) Это отношение эквивалентности (просто остатки при делении на 10).

з) Отношение эквивалентности.

и) Отношение эквивалентности.

к) Это отношение эквивалентности (для доказательства симметричности надо воспользоваться тем, что отображение, обратное биекции, тоже биекция; для транзитивности — тем, что композиция биекций — биекция).

л) Отношение, очевидно, не рефлексивно и не симметрично, но транзитивно.

м) Это отношение по определению рефлексивно, симметрично и транзитивно (если a и b принадлежат X и b и c принадлежат X, то и a и c принадлежат X).

Это очень важное отношение эквивалентности: отождествление всех элементов множества X. Важные примеры приведены в комментарии к задаче 6.

н) Отношение эквивалентности.

о) Рефлексивность и симметричность очевидны. С транзитивностью возникают проблемы, если разрешено двойное гражданство. Например, если Вася является гражданином страны А и страны Б, а Петя — гражданин только страны А, а Коля — гражданин только страны Б, то Петя $\sim$ Вася и Вася $\sim$ Коля, но неверно, что Петя $\sim$ Коля. Если запретить двойное гражданство, то это отношение будет отношением эквивалентности.

п) Это условие просто означает равенство треугольников. Отношение рефлексивно, поскольку треугольник равен самому себе. Симметричность тоже очевидна. Заметим, что если треугольник T_1 равен треугольнику T_2 и треугольник T_2 равен треугольнику T_3, то треугольник T_1 равен треугольнику T_3, поэтому отношение транзитивно.

Эта задача поможет школьнику видеть отношение эквивалентности в разных задачах и осознанно пользоваться его свойствами.

> **Задача 4.** Докажите, что отношение эквивалентности на множестве задаёт отношение эквивалентности на каждом его подмножестве.

Если задавать отношение в виде графа, то утверждение задачи очевидно.

Решение. Пусть $A \subset B$. Пусть на B задано отношение R. Как же определить соответствующее ему отношение R_A на A? Будем говорить, что $a_1 \sim_{R_A} a_2$, где $a_1, a_2 \in A$, если пара $(a_1, a_2) \in R$. Теперь легко заметить, что если R было отношением эквивалентности, то и отношение на A будет отношением эквивалентности (попросите школьников строго выписать все свойства!).

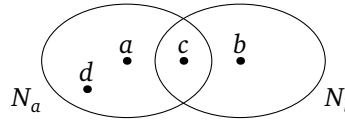
> **Определение 4.** Пусть $\sim$ — отношение эквивалентности на M, $a \in M$. Множество $N_a = \{x \in M \mid a \sim x\}$ называется *классом эквивалентности* элемента a.

Обязательно разберите определение на простом примере. Например, пусть множество M — это множество учеников школы, а $a \sim b$, если ученики a и b учатся в одном классе. Тогда N_a — это все одноклассники a (включая самого a).

> **Задача 5.** Докажите, что для любого отношения эквивалентности классы эквивалентности либо не пересекаются, либо совпадают.
>
> Докажите, что каждое отношение эквивалентности на M задаёт разбиение множества M на непересекающиеся классы эквивалентности.

Это одна из самых важных задач в листочке.

Решение. Предположим, что два класса эквивалентности N_a и N_b пересекаются, то есть существует c, принадлежащее обоим классам (см. рисунок). Докажем, что эти классы эквивалентности совпадают. Для



этого достаточно доказать, что $N_a \subset N_b$ и $N_b \subset N_a$. Докажем первое включение. Для любого элемента $d \in N_a$ верно, что $d \sim a$ (на самом деле $a \sim d$, но отношение эквивалентности симметрично!) и $a \sim c$, а значит, по транзитивности $d \sim c$, но мы знаем, что $c \sim b$, а значит, опять применяя транзитивность, получаем, что $d \sim b$, то есть $d \in N_b$.

Можно также воспользоваться такой леммой: если $a \in N_b$, то $N_a \subset N_b$.

> **Определение 5.** Пусть $\sim$ — отношение эквивалентности на M. Множество классов эквивалентности называется *фактормножеством* и обозначается $M/\sim$.

Это определение еще труднее понимается школьниками. Вернемся к примеру, который мы разбирали в комментарии к определению 4. Каждый класс эквивалентности — это ученики из одного класса, значит, фактормножество — это множество классов в этой школе.

> **Задача 6.** Опишите классы эквивалентности и фактормножества для отношений эквивалентности задачи 3.

Решение. а) Здесь один класс эквивалентности, состоящий из всех элементов множества. Фактормножество — множество из одного элемента.

г) Класс эквивалентности — это связная компонента графа, а фактормножество — множество связных компонент.

е) У нас есть два класса эквивалентности: четные числа и нечетные числа. Фактормножество — это множество из двух элементов 0 и 1.

Если рассматривать остатки при делении на любое число, то фактормножество — это множество остатков от деления на это число.

ж) Класс эквивалентности — все числа, оканчивающиеся на одну цифру, т. е. числа, дающие один и тот же остаток при делении на 10. Фактормножество — это множество возможных остатков при делении на 10, т. е. множество чисел $\{0, 1, \ldots, 9\}$.

з) Класс эквивалентности — это множество учеников в одном классе, а фактормножество — множество классов в этой школе.

и) Класс эквивалентности — это множество учеников, родившихся в одном месяце, а фактормножество — множество месяцев, в которых родился хотя бы один ученик из класса.

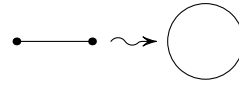
к) Классы эквивалентности будут следующие: пустое множество, множества из n элементов (для каждого n — свой класс) и бесконечные подмножества. Фактормножеством будет $\{0\} \cup \mathbb{N} \cup \{\infty\}$. Строго доказать, что не бывает биекции между двумя конечными множествами с разным числом элементов, можно по индукции. Утверждение о том, что все бесконечные подмножества натуральных чисел равномощны, т. е. между ними существует биекция, здесь принимается без доказательства, а строго будет доказано в листочке «Мощность множеств» 9 класса.

м) Классами эквивалентности будут все одноэлементные подмножества M для элементов, не лежащих в X, и само множество X.

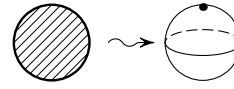
н) Классами эквивалентности будут полные прообразы элементов Y. Фактормножество естественно изоморфно образу отображения.

В этой задаче рекомендуется задавать дополнительные вопросы про то, каким получится фактормножество для конкретных множеств M и X. А именно, что получится, если:

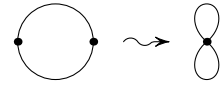
1) $M = [0, 1]$, а $X = \{0, 1\}$? В этом случае получится окружность.



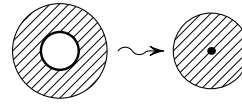
2) M — круг, а X — граничная окружность? Получается сфера.



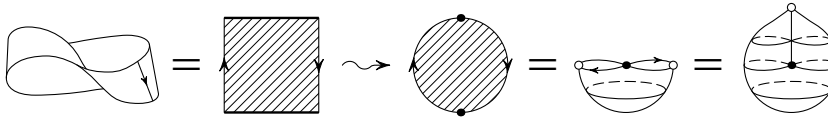
3) M — окружность $x^2 + y^2 = 1$, а X — две диаметрально противоположные точки? Получается «восьмерка».



4) M — кольцо $1 \leqslant x^2 + y^2 \leqslant 2$, а X — одна из границ, например, $x^2 + y^2 = 1$? Получается круг. Такой переход к фактормножеству позволяет «заклеивать дырку».



5*) M — лист Мёбиуса, а X — его граничная окружность? Получается проективная плоскость.



о) Если нет двойного гражданства, то класс эквивалентвности — это граждане одной страны, а фактормножество — это множество стран (так как каждый класс эквивалентности задается страной).

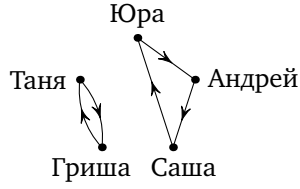
п) Класс эквивалентности — это множество треугольников, равных данному, а фактормножество — это множество различных треугольников.

Задача 7. Рассмотрим следующее отношение на множестве S_n: $a \sim b$, если существует такая подстановка c, что $c^{-1}ac = b$.

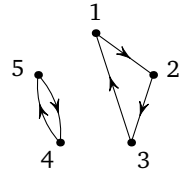
а) Докажите, что это отношение является отношением эквивалентности (такие подстановки называются *сопряженными*, а отношение — и иногда операция — называется *сопряжением*).

б*) Придумайте простой способ проверки, эквивалентны ли подстановки a и b, и выясните, какие из указанных преподавателем подстановок эквивалентны.

Прежде чем решать данную задачу, полезно рассмотреть следующий пример. Пусть имеется пять школьников, которые сидели за партами, по одному за каждой: Юра, Андрей, Саша, Гриша и Таня. Они пересели так: Юра сел на место Андрея, Андрей — на место Саши, Саша — на место Юры, а Гриша и Таня поменялись местами. Схематично это можно изобразить так:

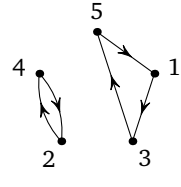


Ваня решил записать, как ребята пересели, занумеровав их следующим образом: 1 — Юра, 2 — Андрей, 3 — Саша, 4 — Гриша, 5 — Таня. У Вани получилась подстановка a: $\begin{pmatrix}12345\\23154\end{pmatrix}$. Нарисуем ее граф:



Получился тот же граф, что и раньше, только вместо имен стоят номера ребят.

Аккуратный Боря тоже решил записать, как ребята пересели, но он занумеровал ребят по алфавиту 1 — Андрей, 2 — Гриша, 3 — Саша, 4 — Таня, 5 — Юра. У него получилась подстановка b: $\begin{pmatrix}12345\\34521\end{pmatrix}$. Нарисуем ее граф:



Итак, Ваня и Боря получали две подстановки, которые показывают, как пересели школьники, соответствующие разным способам нумерации ребят.

Давайте посмотрим, как связаны подстановки a и b. Из рисунка видно, что их графы изоморфны. В частности, они имеют одну и ту же циклическую структуру (набор циклов в разложении в произведение независимых циклов). Однако формально они различны.

Попробуем из одной подстановки получить другую. Заметим, что получить нумерацию Вани из нумерации Бори можно при помощи подстановки c, которая ставит в соответствие Бориному номеру школьника его Ванин номер: $c = \binom{12345}{24351}$. Теперь, чтобы узнать, куда пересел школьник с Бориным номером n, можно сначала применить подстановку c, чтобы узнать его Ванин номер, затем применить подстановку a, чтобы узнать, куда пересел школьник (также в нумерации Вани), затем применить подстановку c^{-1}, чтобы узнать, какой номер у этого места в нумерации Бори. Получаем: $b = c^{-1} \cdot a \cdot c$.

Итак, содержательный смысл сопряжения состоит в замене способа нумерации. Иногда говорят, что подстановка просто переставляет объекты, в то время как после нумерации возникает ее запись, зависящая от способа нумерации. Если один способ нумерации из другого получается с помощью подстановки c («замены координат»), то записи подстановки при разных способах нумерации получаются друг из друга с помощью сопряжения подстановкой c.

Решение. а) На самом деле, утверждение очевидно, ведь сопряженные подстановки — это одна и та же подстановка, только по-разному записанная (т. е. при разных способах нумерации). Тем не менее, очень полезно провести формальное алгебраическое доказательство.

Рефлексивность: a сопряжено с a с помощью тождественной подстановки.

Симметричность: Если a сопряжено с b с помощью c, то b сопряжено с a с помощью c^{-1}. Это ясно из геометрических соображений, но все же проверим формально. Действительно, если $b = c^{-1} \cdot a \cdot c$, то, домножив справа на c^{-1} и слева на c, получаем: $a = c \cdot b \cdot c^{-1}$.

Транзитивность: Если a сопряжено с b с помощью c_1, а b сопряжено с d с помощью c_2, то a сопряжено с d с помощью $c_1 \cdot c_2$. Проведем доказательство формально: $b = c_1^{-1} \cdot a \cdot c_1$, $d = c_2^{-1} \cdot b \cdot c_2$; теперь, подставив первое равенство во второе, имеем

$$d = c_2^{-1} \cdot (c_1^{-1} \cdot a \cdot c_1) \cdot c_2 = (c_1 \cdot c_2)^{-1} \cdot a \cdot (c_1 \cdot c_2).$$

То есть d и a сопряжены с помощью подстановки $c_3 = c_1 \cdot c_2$.

Попробуем объяснить смысл этой формулы на примере. Пусть у нас есть три нумерации школьников: Ванина, Борина и Сережина, и пусть Ванина нумерация из Бориной получается с помощью c_1, а Борина из Сережиной — с помощью c_2. Тогда, чтобы узнать Сережину подстановку d, зная Ванину a, надо сначала получить Борины номера из Сережиных с помощью c_2, потом Ванины из Бориных с помощью c_1, потом применить Ванину подстановку, потом обратно получить Борины номера с помощью c_1^{-1}, затем получить Сережины номера с помощью c_2^{-1}.

б) *Указание.* Из геометрических соображений видно, что следующие три утверждения эквивалентны:

1) подстановки a и b сопряжены;

2) графы подстановок a и b изоморфны;

3) подстановки a и b имеют одинаковую циклическую структуру (то есть один и тот же набор длин циклов в разложении в произведение независимых циклов.)

Целые числа 3. Сравнения

листок 10 / февраль 2005

Этот листок посвящен более подробному изучению остатков от деления целых чисел на целые. На этом примере происходит фактически знакомство с понятиями группы, кольца и поля.

При решении многих задач важно уметь правильно выделять существенные свойства рассматриваемых объектов. Так, в ряде задач теории чисел, переходя к остаткам от деления, мы сохраняем те свойства числа, которые нам понадобятся, отбрасывая ненужные, и решение задачи упрощается, а иногда становится очевидным. При переходе к остаткам отношению равенства чисел соответствует равенство их остатков от деления на некоторое число m. Это отношение и называется сравнимостью по модулю m. Технике работы со сравнениями и остатками и посвящен данный листок.

Некоторые из задач листка возникают, как мы увидим позднее, в теории конечных абелевых групп и конечных полей; они играют важную роль и в практических приложениях математики (например, в криптографии — при проверке простоты чисел) — отметим, прежде всего, китайскую теорему об остатках и малую теорему Ферма.

Определение 1. Числа a и b *сравнимы* по модулю $m \neq 0$, если $a - b \vdots m$. Обозначение: $a \equiv b \pmod{m}$.

Задача 1. Докажите, что a сравнимо с b по модулю m тогда и только тогда, когда остаток от деления a на m равен остатку от деления b на m.

Решение. Действительно, $a \equiv b \pmod{m}$ означает по определению, что $a - b \vdots m$, то есть $a - b = km$. Разделим b на m с остатком: $b = lm + r$. Мы показали, что $a \equiv b \pmod{m}$ равносильно $a - (lm + r) = km$, $b = lm + r$, или (что то же самое) $a = (l + k)m + r$, $b = lm + r$. Но последнее условие и означает совпадение остатков a и b при делении на m.

Задача 2. Докажите, что сравнимость по модулю m является отношением эквивалентности.

Указание. Воспользуйтесь предыдущей задачей.

Задача 3. Докажите, что для любых a_1, a_2, b_1, b_2, c, m

а) $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$;

б) $a_1 \equiv b_1 \pmod{m} \Rightarrow ca_1 \equiv cb_1 \pmod{m}$;

в) $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

Решение. а), б) Это непосредственно следует из уже известных свойств делимости:

$$a_1 \equiv b_1 \pmod m,\ a_2 \equiv b_2 \pmod m \iff a_1 - b_1 \vdots m,\ a_2 - b_2 \vdots m \Rightarrow$$
$$\Rightarrow a_1 - b_1 + a_2 - b_2 \vdots m \iff a_1 + a_2 \equiv b_1 + b_2 \pmod m;$$

$$a_1 \equiv b_1 \pmod m \iff a_1 - b_1 \vdots m \Rightarrow c(a_1 - b_1) \vdots m \iff$$
$$\iff ca_1 - cb_1 \vdots m \iff ca_1 \equiv cb_1 \pmod m;$$

в) $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m \iff a_1 = b_1 + k_1 m$, $a_2 = b_2 + k_2 m$. Но тогда $a_1 a_2 = b_1 b_2 + m(k_1 b_2 + k_2 b_1) + m^2 k_1 k_2 \equiv b_1 b_2 \pmod m$.

Задача 4. Докажите, что если $a \equiv b \pmod m$, то
а) $a^n \equiv b^n \pmod m$ для любого неотрицательного n;
б*) для любого многочлена $f(x)$ с целыми коэффициентами $f(a) \equiv f(b) \pmod m$.

Решение. а) Получается из 3 в) индукцией по n.
б) Получается из предыдущего пункта и 3 а) индукцией по степени многочлена.

Задача 5. Верно ли, что если $a \equiv b \pmod m$ и $a, b \geqslant 0$, то $2^a \equiv 2^b \pmod m$?

Решение. Нет. В этом можно убедиться, подставив $m = 2$, $a = 0$, $b = 2$.

Задача 6. Пусть $\overline{a_n a_{n-1} \ldots a_1 a_0}$ — десятичная запись числа x. Докажите, что
а) $x \equiv a_0 + \ldots + a_n \pmod 3$, $x \equiv a_0 + \ldots + a_n \pmod 9$;
б) $x \equiv a_0 \pmod 2$, $x \equiv a_0 \pmod 5$;
в) $x \equiv a_0 - a_1 + \ldots + (-1)^n a_n \pmod{11}$.

Решение. См. листок «Целые числа 1», задачу 4.

Задача 7. Докажите, что если x нечетно, то $x^2 \equiv 1 \pmod 8$.

Указание. Рассмотрите случаи разных остатков x по модулю 8.

Решение. Можно перебрать все возможные остатки от деления x на 8, а можно решить задачу следующим образом. Пусть $x = 2n + 1$, тогда $x^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1$. Осталось заметить, что одно из чисел n, $n+1$ обязательно четно, а значит, произведение $n(n+1)$ четно, и $x^2 - 1$ делится на 8.

Задача 8*. Докажите, что следующие уравнения не имеют ненулевых решений в целых числах: а) $x^2 + y^2 = 3z^2$; б) $x^2 + y^2 + z^2 = 4t^2$.

Решение. а) Допустим, это уравнение имеет ненулевое целочисленное решение. Разделив x, y и z на их НОД, получим решение, для которого НОД$(x, y, z) = 1$. В силу предыдущей задачи, квадрат нечетного числа дает остаток 1 при делении на 4. С другой стороны, квадрат четного числа имеет вид $(2n)^2 = 4n^2$, а значит, делится на 4. Итак, числа x^2, y^2 и z^2 равны 0 или 1 по модулю 4. Следовательно, левая часть равна 0, 1 или 2 по модулю 4, а правая — 0 или 3, откуда обе части делятся на 4. Но левая часть может делиться на 4 только при четных x и y. Таким образом, числа x, y и z четны, что противоречит условию НОД$(x, y, z) = 1$. Полученное противоречие доказывает отсутствие ненулевых целочисленных решений данного уравнения.

б) Доказательство аналогично.

Задача 9*. Докажите, что существует бесконечно много натуральных чисел, не представимых в виде суммы трех а) квадратов; б) кубов натуральных чисел.

Решение. а) Это непосредственно следует из предыдущей задачи.

б) Пусть $K(N)$ — количество чисел от 1 до N^3, представимых в виде суммы трех кубов натуральных чисел. Оценим общее число представлений чисел от 1 до N^3 в виде суммы трех кубов натуральных чисел (представления, отличающиеся порядком слагаемых, считаем разными).

Заметим, что для каждого представления, в котором не все слагаемые равны между собой, найдется другое представление того же числа (например, отличающееся только порядком слагаемых). Следовательно, каждому из как минимум $K(N) - N$ чисел соответствует как минимум по два представления. Значит, общее число таких представлений не меньше $2(K(N) - N)$.

Но каждое слагаемое в таком представлении — это куб числа от 1 до N, а значит, общее число таких представлений не превосходит N^3. Таким образом, $2(K(N) - N) \leqslant N^3$, откуда $K(N) \leqslant 0{,}5N^3 + N$, то есть не менее $0{,}5N^3 - N$ чисел от 1 до N^3 не представимы в виде суммы трех кубов натуральных чисел. Осталось заметить, что при достаточно больших значениях числа N выражение $0{,}5N^3 - N$ становится больше любого фиксированного натурального числа.

Задача 10. Решите сравнения
а) $3x \equiv 1 \pmod 7$; б) $6x \equiv 5 \pmod 9$; в) $4x \equiv 2 \pmod{10}$.

Решение. Заметим, что остаток левой части каждого из сравнений (по соответствующему модулю) зависит только от остатка x. В частности, множество решений периодично (и модуль сравнения является пери-

одом). Поэтому достаточно проверить, какие остатки удовлетворяют сравнению.

а) $x = 5 + 7k$;

б) решения отсутствуют: действительно, $6x$ делится на 3, а потому не может иметь вид $5 + 9k = 2 + 3(1 + 3k)$;

в) $x = 3 + 10k$, $x = 8 + 10k$, другими словами, $x = 3 + 5k$.

> **Задача 11.** Сравнение $ax \equiv b \pmod m$ имеет решение тогда и только тогда, когда $b \vdots \text{НОД}(a, m)$.

Решение. Наличие решения у сравнения $ax \equiv b \pmod m$ равносильно наличию решения уравнения $ax - b = ym$ (относительно (x, y)). Остается применить задачу 11 из листка «Целые числа 2».

> **Задача 12.** Пусть p — простое число, $a \not\equiv 0 \pmod p$, тогда сравнение $ax \equiv b \pmod p$ имеет решение, причем любые два решения этого сравнения сравнимы по модулю p.

Решение. Существование решения мгновенно следует из предыдущей задачи; проверим, что любые два решения совпадают по модулю p. Действительно, если x, y — два решения, то $ax \equiv ay \pmod p$, то есть $a(x - y) \vdots p$. Значит (так как p простое), либо a, либо $x - y$ делится на p; но по условию a на p не делится, значит, $x \equiv y \pmod p$.

Последняя задача показывает, что на остатках по простому модулю имеется однозначное деление. Таким образом, они образуют не только кольцо, но даже *поле*.

> **Задача 13* (китайская теорема об остатках).** Пусть числа $a_1, a_2, \ldots, a_n$ попарно взаимно просты. Тогда для любых $b_1, b_2, \ldots, b_n$ найдется x такое, что
>
> $$x \equiv b_i \pmod{a_i}, \quad i = 1, \ldots, n,$$
>
> причем любые два числа, удовлетворяющие этому условию, сравнимы по модулю $a_1 \ldots a_n$.

Указание. Начните с $n = 2$.

Набросок решения. Начнем со случая $n = 2$. Как мы уже знаем, все решения первого сравнения имеют вид $x = x_1 + ya_1$, где $x_1 = b_1$. Нам нужно найти среди них решения второго сравнения. Запишем, что это значит: $b_1 + ya_1 \equiv b_2 \pmod{a_2}$, то есть $a_1 y \equiv (b_2 - b_1) \pmod{a_2}$. Так как a_1 и a_2 взаимно просты, у этого сравнения имеются решения, причем все они имеют вид $y = c + ka_2$. Подставляя в выражение для x получаем, что (все) решения исходной системы имеют вид

$x = x_2 + la_1a_2$, где l — произвольное число, а x_2 — некоторое фиксированное решение (в наших обозначениях $x_2 = x_1 + a_1c$).

Если теперь посмотреть, что же произошло, станет видно, что мы доказали эквивалентность системы из *двух* сравнений

$$x \equiv b_i \pmod{a_i}, \quad i = 1, 2,$$

системе из *одного* сравнения

$$x \equiv x_2 \pmod{a_1a_2}.$$

Теперь нетрудно изучить и системы из любого числа сравнений: можно просто последовательно уменьшать их количество, и в конце концов свести к одному сравнению по модулю $a_1 \ldots a_n$ (что, собственно, и требовалось доказать).

Достоинство этого решения заключается в том, что оно объясняет, *как именно* искать решения такой системы (см. следующую задачу).

Задачу можно переформулировать следующим образом. Первая часть утверждает, что естественное отображение $\nu\colon \mathbb{Z} \to \bigoplus_i \mathbb{Z}/a_i\mathbb{Z}$ (приведение по модулям $a_1, \ldots, a_n$) является сюръективным. Далее, так как прибавление числа, кратного a_i, не меняет остаток по модулю a_i, значение ν зависит только от остатка по модулю $a_1 \ldots a_n$; то есть имеется отображение $\tilde{\nu}$ из $\mathbb{Z}/(\prod_i a_i)\mathbb{Z}$ в $\bigoplus_i \mathbb{Z}/a_i\mathbb{Z}$. Вторая часть утверждает, что $\tilde{\nu}$ инъективно.

В такой формулировке решать задачу естественно следующим образом.

Набросок решения. Заметим, что вторая часть нам по сути уже известна. Действительно, если у какого-то остатка имеется два прообраза относительно ν, то их разность делится на каждое из a_i, то есть (так как a_i взаимно просты) эти числа сравнимы по модулю $\prod a_i$; что и означает инъективность $\tilde{\nu}$.

Таким образом $\tilde{\nu}$ — инъективное отображение конечных множеств с одинаковым количеством элементов, а значит, $\tilde{\nu}$ — биекция, что и требовалось доказать.

Отметим еще, что $\tilde{\nu}$ является *гомоморфизмом* (переводит сумму в сумму, а произведение в произведение), поэтому $\tilde{\nu}$ является не просто биекцией множества, а изоморфизмом колец $\mathbb{Z}/(\prod_i a_i)\mathbb{Z}$ и $\bigoplus_i \mathbb{Z}/a_i\mathbb{Z}$.

Такой изоморфизм позволяет сводить разные вопросы об остатках по произвольному модулю к вопросам об остатках по модулям вида p^k. Это соображение можно применить, например, к решению уравнения $x^2 = 1 \pmod{n}$ (да и любого другого).

Задача 14*. Найдите все решения системы сравнений

$$\begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 7 \\ x \equiv 4 \pmod 9. \end{cases}$$

Ответ. $x = 148 + 315k$.

Решение. Предыдущая задача гарантирует, что множество решений имеет вид $x_0 + 5 \cdot 7 \cdot 9k = x_0 + 315k$, где x_0 — какое-то решение.

Будем решать задачу, последовательно добавляя уравнения (см. также решение предыдущей задачи). Множество решений первого уравнения имеет вид $3 + 5k$; найдем *среди них* какое-нибудь решение второго уравнения. Перебирая последовательно k, видим, что подходит уже $3 + 5 = 8 = 1 + 7$. Таким образом, у нас имеется полное решение системы первых двух уравнений: $8 + 5 \cdot 7k = 8 + 35k$, и в этой последовательности надо найти какое-нибудь решение последнего сравнения. Несложный перебор показывает, что подходит $k = 4$, то есть $x_0 = 148$ является (частным) решением системы.

Задача 15. Пусть p — простое число. Докажите, что:
а) $C_p^k \vdots p$ при $0 < k < p$;
б) $(a+b)^p \equiv a^p + b^p \pmod p$;
в) (*малая теорема Ферма*) $a^p - a \vdots p$.

Решение. а) Вспомним, что $C_p^k = \dfrac{p!}{(p-k)!\,k!}$. Но при $0 < k < p$ число p делит числитель, но не знаменатель (так как при $n < p$ число $n!$ есть произведение чисел меньших p, а значит, на p не делящихся).

б) По биному Ньютона $(a+b)^p = \sum_k C_p^k a^k b^{p-k}$. Остается только заметить, что (по предыдущему пункту) все слагаемые, кроме первого и последнего, в этой сумме сравнимы с 0 по модулю p.

в) Из предыдущего пункта видно, что по модулю p возведение в степень аддитивно (то есть переводит сумму в сумму). В частности, $a^p = (1 + \ldots + 1)^p \equiv 1^p + \ldots + 1^p = a \pmod p$, что и требовалось доказать.

Решение 2. Пусть мы хотим покрасить колесо обозрения, состоящее из p одинаковых кабинок, в не более чем a различных цветов. Подсчитаем, сколькими различными способами это можно сделать.

Сначала разберемся, какие способы являются различными. Так как колесо обозрения крутится, то способы, получающиеся друг из друга поворотом, естественно считать одинаковыми. Будем также

считать, что с разных сторон колесо обозрение разное, то есть способы, получающиеся друг из друга симметрией относительно вертикальной плоскости, считаются разными.

Каждую из p кабинок можно покрасить в a цветов, так что, на первый взгляд, число способов равно a^p. Но некоторые способы мы считали несколько раз. Хочется сказать, что каждый способ мы подсчитали p раз (число различных положений колеса обозрения при поворотах), то есть число a^p надо разделить на p. Но это неправильно: например, если мы покрасим все кабинки в один цвет, то при поворотах эта раскраска переходит в себя (кроме того, a^p далеко не всегда делится на p). Есть ли еще способы, которые при некотором повороте переходят в себя? Так как p — простое число[20], в себя при некотором повороте переходят только «одноцветные» раскраски (докажите!).

Итак, все способы, кроме одноцветных, подсчитаны p раз, а все одноцветные способы подсчитаны один раз. Значит, общее число способов раскрасить колесо обозрения, состоящее из p одинаковых кабинок, в не более чем a различных цветов равно числу неодноцветных раскрасок, деленному на p, плюс число одноцветных раскрасок, то есть $\frac{a^p-a}{p}+a$. В частности, a^p-a делится на p.

Решение 3. Еще одно решение. Случай $a\equiv 0 \pmod p$ очевиден, поэтому будем решать для ненулевых остатков a. Рассмотрим ориентированный граф, вершины которого соответствуют ненулевым остаткам по модулю p, и из вершины x выходит ребро в вершину ax. Поскольку умножение обратимо, в каждую вершину входит ровно одно ребро. Таким образом, все остатки разбиваются на циклы. Заметим, что длины всех циклов равны, и равны наименьшему натуральному k, для которого $a^k\equiv 1 \pmod p$. Следовательно, общее число ненулевых остатков (а именно, $p-1$) делится на это число k, откуда $a^{p-1}\equiv (a^k)^{\frac{p-1}{k}}\equiv 1 \pmod p$ и $a^p-a\equiv a(a^{p-1}-1)\equiv 0 \pmod p$.

> **Задача 16* (теорема Вильсона).** Пусть p — простое число, тогда $(p-1)!\equiv -1 \pmod p$.

Указание. Докажите, что по модулю p все остатки, кроме ± 1, разбиваются на пары с произведением 1.

Решение. По задаче 12 для любого ненулевого остатка a по модулю p можно найти «обратный» остаток a^{-1}, такой что $aa^{-1}\equiv 1 \pmod p$,

[20] Если p не является простым, то это неверно. Например, если p — четное, то раскраска «белый, черный, белый, черный, ...» переходит в себя при повороте «на две кабинки».

причем $(a^{-1})^{-1} = a$. Таким образом, все остатки, для которых $a^{-1} \neq a$, разбиваются на пары остатков, дающих в произведении единицу, и не влияют на значение $(p-1)! \bmod p$. Найдем теперь все остатки, для которых $a^{-1} = a$, то есть $a^2 \equiv 1 \pmod{p}$, что равносильно $(a-1)(a+1) \equiv 0 \pmod{p}$, откуда $a \in \{-1, 1\}$.

Итак, произведение всех остатков, кроме 1 и -1, равно 1, а $1 \cdot (-1) = -1$, откуда $(p-1)! \equiv -1 \pmod{p}$.

Задача 17. Какими правильными многоугольниками можно замостить плоскость?

Решение. Угол α_n при вершине правильного n-угольника равен $\pi - 2\pi/n$. Если n-угольниками можно замостить плоскость, то $2\pi/k = \alpha_n$ (где k — число многоугольников, сходящихся в одной вершине), то есть $2n = k(n-2)$, причем $n > 2$, $k > 2$. Заметим, что $k(n-2) > 2n$ при $n > 6$ (так как $k > 2$). Осталось заметить, что $n = 5$ не является решением, а правильными 3-, 4- и 6-угольниками действительно можно замостить плоскость.

Задача 18. Докажите, что имеется бесконечное количество простых чисел вида

а) $4n+3$; б*) $4n+1$; в**) $an+b$, где НОД$(a, b) = 1$.

Указание. Вспомните, как доказывалась бесконечность множества всех простых чисел.

Решение. а) Предположим, что это не так. Тогда обозначим за N произведение всех простых чисел вида $4n+3$. Рассмотрим число $M = 4N - 1$. Оно нечетно и не делится ни на одно из простых чисел вида $4n+3$, а значит, представляется в виде произведения простых чисел вида $4n+1$. Но тогда оно сравнимо с единицей по модулю 4, что неверно.

б) Предположим, что это не так. Тогда обозначим за N произведение всех простых чисел вида $4n+1$ и рассмотрим число $M = (2N)^2 + 1$. Это число не может делиться на простое число p вида $4n+3$. Действительно, если $p \mid (2N)^2 + 1$, то $(2N)^2 \equiv -1 \pmod{p}$, а значит, $(2N)^{2(\frac{p-1}{2})} \equiv (-1)^{\frac{p-1}{2}} = (-1)^{2n+1} \equiv -1 \pmod{p}$. Но по малой теореме Ферма $(2N)^{2(\frac{p-1}{2})} = (2N)^{p-1} \equiv 1 \pmod{p}$. Получили противоречие. Осталось заметить, что на простые числа вида $4n+1$ оно не делится по построению. Противоречие.

Пункт в) представляет собой один очень изящный и сложный результат теории чисел — в любой арифметической прогрессии со взаимнопростыми основанием и разностью бесконечно много простых чисел.

Для конкретных прогрессий (см. пункт а) иногда удается найти «школьные» доказательства, но доказательство общей теоремы использует аппарат математического анализа.

Задача 19*. Найдите количество решений сравнения $x^2 \equiv 1 \pmod{n}$: а) при простом n; б) при произвольном n.

Так как множество решений n-периодично, если есть одно решение, то есть и бесконечно много решений. Поэтому естественно искать количество решений по модулю n.

Ответ. а) 2, если $n > 2$; 1, если $n = 2$;

б) если n раскладывается на простые множители как $2^{n_0} p_1^{n_1} \dots p_k^{n_k}$, то число решений есть

$$\begin{cases} 2^k, & n_0 = 0, 1; \\ 2^{k+1}, & n_0 = 2; \\ 2^{k+2}, & n_0 > 2. \end{cases}$$

Решение. а) Заметим, что сравнение $x^2 \equiv 1 \pmod{n}$ равносильно сравнению $(x-1)(x+1) \equiv 0 \pmod{n}$. Так как произведение делится на *простое* число только тогда, когда на него делится хотя бы один из сомножителей, последнее сравнение дает $x \equiv \pm 1 \pmod{n}$. Осталось только не забыть, что по модулю 2 эти случаи совпадают: $1 \equiv -1$.

б) (*Набросок*.) Согласно китайской теореме об остатках, если $n = 2^{n_0} \prod p_i^{n_i}$, то исходное уравнение равносильно системе

$$\begin{cases} x_0^2 \equiv 1 \pmod{2^{n_0}}; \\ x_1^2 \equiv 1 \pmod{p_1^{n_1}}; \\ \dots\dots\dots\dots\dots \\ x_k^2 \equiv 1 \pmod{p_k^{n_k}}. \end{cases}$$

Поэтому достаточно научиться решать задачу для $n = p^k$ (где p — простое).

Нас интересуют решения уравнения $x^2 \equiv 1 \pmod{p^k}$. Разложим его на множители: $(x-1)(x+1) \vdots p^k$. Выражения в скобках отличаются на 2, поэтому при $p > 2$ даже на p может делиться только одна из них, то есть $x = \pm 1 \pmod{p^k}$. Таким образом, при $p > 2$ имеется два различных решения.

При $p = 2$ все сложнее, но не намного: хотя на 2 могут делиться выражения в обеих скобках, на 4 уже может делиться только одна из

них; таким образом, либо $x \equiv \pm 1 \pmod{2^k}$ (причем оба эти остатка совпадают при $k = 1$), либо $x \equiv 2^{k-1} \pm 1 \pmod{2^k}$ (последний случай возможен для $k > 1$, но отличается от первого только при $k > 2$). Таким образом, при $p = 2$ имеется одно решение при $k = 1$, два решения при $k = 2$ и четыре решения при $k > 2$.

Суть происходящего заключается в следующем. Для любого кольца R можно рассмотреть группу обратимых элементов (по умножению) $R^\times$; это некоторая коммутативная группа. В аддитивной записи наше уравнение принимает вид $2x = 0$, $x \in (\mathbb{Z}/n\mathbb{Z})^\times$. Найти число решений такого уравнения в любом кольце вида $\bigoplus_i (\mathbb{Z}/a_i\mathbb{Z})$ несложно (обозначим его за $N_{a_1,\ldots,a_n}$; тогда $N_{a_1,\ldots,a_n} = \prod N_{a_i}$, а N_n есть 1 для n нечетного и 2 для четного — проверьте!), вопрос в том, как представить $(\mathbb{Z}/n\mathbb{Z})^\times$ в таком виде.

Согласно китайской теореме об остатках $(\mathbb{Z}/nm\mathbb{Z})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \oplus (\mathbb{Z}/m\mathbb{Z})^\times$, поэтому достаточно изучить $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Ответ в этом случае такой:

$$(\mathbb{Z}/p^n)^* = \begin{cases} Z/(p-1)p^n, & p > 2; \\ \mathbb{Z}/2 \oplus \mathbb{Z}/2^{n-2}, & p = 2,\ n > 1; \\ 0, & p = 2,\ n = 1. \end{cases}$$

Доказывать его можно индукцией по n.

Целые числа 4. Практические задачи

листок 11 / март 2005

Листок состоит из несложных упражнений на целые числа.

Все числа в этом листке предполагаются целыми.

Задача 1. Верно ли, что для любого $n>1$ выполняется:
а) $n^3+5n \vdots 6$; б) $2n^3+3n^2+7n \vdots 6$; в) $n^5-n \vdots 30$; г) $2^{2n}-1 \vdots 6$;
д) $11^{6n+3}+1 \vdots 148$?

Решение. а) Верно. $n^3+5n \vdots 6$, так как

$$n^3+5n = n^3-n+6n = n\cdot(n-1)\cdot(n+1)+6n.$$

А среди трех последовательных натуральных чисел $(n-1,\ n,\ n+1)$ обязательно есть хотя бы одно четное и ровно одно, делящееся на три (докажите это в качестве простого, но полезного упражнения). Значит, по основной теореме арифметики все произведение $n\cdot(n-1)\cdot(n+1)$ делится на $2\cdot 3=6$.

б) Верно.

$$2n^3+3n^2+7n = n\cdot(2n^2+3n+1)+6n = n\cdot(n+1)\cdot(2n+1)+6n.$$

Либо n, либо $n+1$ делится на 2. Кроме того, или $n \vdots 3$, или $n+1 \vdots 3$, или n имеет вид $n=3k+1$, где k — целое число. Но в последнем случае $2n+1=6k+3 \vdots 3$. Значит, и все выражение делится на 3. Опять применяем основную теорему арифметики и получаем, что исходное выражение должно делиться нацело на 6.

в) Верно.

$$n^5-n = n(n^4-1) = n(n^2-1)(n^2+1) = (n-1)n(n+1)(n^2+1).$$

Так как n, $n-1$ и $n+1$ — три последовательных натуральных числа, среди них обязательно есть хотя бы одно четное и ровно одно, делящееся на три. Значит, все произведение делится на 6. Осталось доказать, что n^5-n делится на 5. Но это следует из малой теоремы Ферма.

г) Неверно. Например, при $n=2$: $2^{2n}-1=2^4-1=15 \not\vdots 6$.

д) Докажем утверждение по индукции.

База индукции. При $n=0$ имеем $11^3+1=1332=148\cdot 9$.

Шаг индукции. Пусть для некоторого n выполнено: $11^{6n+3}+1 \vdots 148$. Тогда

$$11^{6n+9}+1 = 11^6\cdot(11^{6n+3}+1-1)+1 = 11^6\cdot(11^{6n+3}+1)-11^6+1 =$$
$$= 11^6\cdot(11^{6n+3}+1)+(1-11^3)(1+11^3) \vdots 148.$$

Задача 2. Дайте определение: а) НОД; б) НОК чисел $a_1, a_2, \ldots, a_n$ $(n > 2)$.

Определение 1. *Наибольшим общим делителем* чисел $a_1, a_2 \ldots, a_n$ называется наибольшее из таких чисел d, что $a_1 \vdots d$, $a_2 \vdots d$, $\ldots$, $a_n \vdots d$.

Определение 2. *Наименьшим общим кратным* чисел $a_1, a_2, \ldots, a_n$ называется наименьшее из таких положительных чисел d, что $d \vdots a_1$, $d \vdots a_2$, $\ldots$, $d \vdots a_n$.

Задача 3. Докажите, что для любых a, b и c, таких что $a \cdot b \cdot c \neq 0$:

а) $\text{НОД}(a, b, c) = \text{НОД}(a, \text{НОД}(b, c)) = \text{НОД}(\text{НОД}(a, b), c)$;

б) $\text{НОК}(a, b, c) = \dfrac{|abc| \cdot \text{НОД}(a, b, c)}{\text{НОД}(a, b) \cdot \text{НОД}(b, c) \cdot \text{НОД}(a, c)}$.

Решение. Докажем, например, что $\text{НОД}(a, b, c) = \text{НОД}(a, \text{НОД}(b, c))$. Остальное доказывается аналогично.

1) Пусть $\text{НОД}(a, b, c) \vdots p$, где p — какое-то целое число. Это означает, что $a \vdots p$, $b \vdots p$ и $c \vdots p$. А значит, $\text{НОД}(b, c) \vdots p$. Отсюда следует, что $\text{НОД}(a, b, c) \vdots p$. Значит, $\text{НОД}(a, \text{НОД}(b, c)) \vdots \text{НОД}(a, b, c)$.

2) Пусть $\text{НОД}(a, \text{НОД}(b, c)) \vdots p$, где p — какое-то целое число. Отсюда $a \vdots p$, $\text{НОД}(b, c) \vdots p$. А значит, $a \vdots p$, $b \vdots p$ и $c \vdots p$. Отсюда следует, что $\text{НОД}(a, \text{НОД}(b, c)) \vdots p$. Значит, $\text{НОД}(a, b, c) \vdots \text{НОД}(a, \text{НОД}(b, c))$.

Задача 4. Существует ли число, которое при делении на числа 2, 3, 4, 5 и 6 дает в остатке соответственно:

а) 1, 2, 3, 4, 5; б) 0, 1, 2, 3, 4; в) 0, 1, 2, 3, 2?

Решение. а) Существует: например, 59. Здесь удобно воспользоваться китайской теоремой об остатках (см. листок «Целые числа 3», задача 12).

б) Существует: например, 58.

в) Не существует. Так как число, которое при делении на 6 дает в остатке 2, имеет вид $6k + 2$ для некоторого целого k. Но отсюда видно, что это число при делении на три должно давать остатке 2, а не 1.

Задача 5. Вычислите НОД чисел:

а) 923 и 1207; б) 279 и -589; в) -693 и 2475;

г) -697 и -1377; д) 1517 и 1591; е) 1134, 2268 и 1575.

Ответ. а) 71; б) 31; в) 99; г) 17; д) 37; е) 63.

Задача 6. Вычислите НОК чисел:

а) 16 и 84; б) 819 и 504; в) 30, 56 и 72;

г) 340, 990 и 46; д) 41, 85 и 36; е) 2, 5, 7, 9 и 11.

Ответ. а) 336; б) 6552; в) 2520; г) 774189; д) 125460; е) 6930.

Задача 7. Для $n>0$ найдите значения следующих выражений:

а) $1\cdot 2+2\cdot 3+\ldots+(n-1)\cdot n$;

б) $\frac{1}{4\cdot 5}+\frac{1}{5\cdot 6}+\ldots+\frac{1}{(n+3)(n+4)}$;

в*) $1\cdot 2\cdot 3+2\cdot 3\cdot 4+\ldots+n\cdot(n+1)\cdot(n+2)$.

Указание. а) Представим выражение в следующем виде:

$$1\cdot 2+2\cdot 3+\ldots+(n-1)\cdot n=(2-1)\cdot 2+(3-1)\cdot 3+\ldots+(n-1)\cdot n=$$
$$=(2^2+3^2+\ldots+n^2)-(2+\ldots+n).$$

Теперь можно воспользоваться выражением для суммы подряд идущих натуральных чисел и суммы квадратов подряд идущих натуральных чисел (см. листок «Метод математической индукции»).

б) Следует представить выражение в таком виде:

$$\frac{1}{4\cdot 5}+\frac{1}{5\cdot 6}+\ldots+\frac{1}{(n+3)(n+4)}=\frac{1}{4}-\frac{1}{5}+\frac{1}{5}-\frac{1}{6}+\ldots+\frac{1}{n+3}-\frac{1}{n+4}.$$

Задача 8. Докажите тождества:

а) $(n+1)\cdot(n+2)\cdot\ldots\cdot(n+n)=2^n\cdot 1\cdot 3\cdot 5\cdot\ldots\cdot(2n-1)$;

б) $1-\frac{1}{2}+\frac{1}{3}-\ldots+\frac{1}{2n-1}-\frac{1}{2n}=\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}$;

в) $\left(1-\frac{1}{4}\right)\cdot\left(1-\frac{1}{9}\right)\cdot\ldots\cdot\left(1-\frac{1}{(n+1)^2}\right)=\frac{n+2}{2n+2}$.

Указание. Все пункты легко доказываются при помощи метода математической индукции.

Задача 9. Решите в целых числах уравнения:

а) $7x+5y=1$; б) $27x-24y=1$; в) $12x-33y=9$;

г) $-56x+91y=21$; д) $344x-215y=86$; е) $3x+5y+7z=1$.

Указание. Следует воспользоваться решением задачи 12 из листка «Алгоритм Евклида» для нахождения частного решения и задачей 13 для нахождения общего решения.

Ответ. а) $x=-2+5t$, $y=3-7t$;

б) нет решений, так как левая часть всегда делится на 3;

в) $x=9+11t$, $y=3+4t$;

г) $x=-15+13t$, $y=-9+8t$;

д) $x=-1+5t$, $y=-2+8t$;

е) $x=2-14l+5t$, $y=-1+7l-3t$, $z=l$.

Задача 10. Верно ли, что для любого натурального n числа $10n+7$ и $10n+5$ взаимно просты?

Решение. Верно. Оба числа нечетные, то есть не делятся на 2. Если бы они не были взаимно простыми, то оба бы делились на одно и то же число, большее 2, но тогда и их разность — 2 — должна делиться на это число, чего быть не может.

Задача 11. Найдите такие числа a и b, что $ax+by=1$ при
а) $x=7$, $y=9$; б) $x=17$, $y=19$; в) $x=27$, $y=29$;
г) $x=37$, $y=39$; д) $x=47$, $y=49$.

Решение. Заметим, что в этой задаче вовсе не обязательно находить все решения. Достаточно предъявить какие-то частные решения. Продемонстрируем технику нахождения частного решения для уравнения такого сорта, например, для пункта б).

Распишем алгоритм Евклида для чисел 17 и 19: $(19, 17) \to (17, 2) \to$ $\to (2, 1)$. Отсюда получаем: $1 = 2 - 1 = 2 - (17 - 2 \cdot 8) = (19 - 17) -$ $- (17 - (19 - 17) \cdot 8) = 19 \cdot 9 - 17 \cdot 10$, то есть $a = -10$, $b = 9$.

Ответ. а) $a = -5 + 9t$, $b = 4 - 7t$;
б) $a = -10 + 19t$, $b = 9 - 17t$;
в) $a = -15 + 29t$, $b = 14 - 27t$;
г) $a = -20 + 39t$, $b = 19 - 37t$;
д) $a = -25 - 49t$, $b = 24 + 47t$.

Задача 12. Определим последовательность чисел $u(n)$ по правилу: $u(0) = 0$, $u(1) = 1$, $u(n) = u(n-1) + u(n-2)$ (*числа Фибоначчи*).
а) Докажите, что $u(1) + \ldots + u(n) = u(n+2) - 1$.
б) Докажите, что $(u(1))^2 + \ldots + (u(n))^2 = u(n) \cdot u(n+1)$.
в) (*формула Бине*) Как связаны числа $u(n)$ и

$$\delta(n) = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n ?$$

Указание. Пункты а) и б) легко доказываются индукцией по n. Доказательство того факта, что числа $u(n)$ и $\delta(n)$ равны, также можно провести индукцией по n (самое сложное, на наш взгляд, — догадаться, что эти числа равны; именно этим обусловлено такое странное условие задачи).

Теория групп

листок 12 / март 2005

В этом листке впервые появляется понятие (абстрактной) группы. Отметим, что уже в этом листке рассматривается *категория* групп — практически сразу возникают понятия подгруппы и изоморфизма групп (впрочем, обсуждение произвольных гомоморфизмов отложено до следующего листка по теории групп). В частности, обсуждается задача классификации групп небольших порядков. Главным формальным результатом листка является теорема Лагранжа.

Чтобы изложение не было слишком абстрактным, в начале листка мы просим школьников для большого числа уже изученных объектов установить, являются ли они на самом деле группами, а в конце листка теорема Лагранжа применяется к теории чисел.

Важно, что изучение свойств абстрактных групп происходит уже *после* рассмотрения их на конкретных примерах (группы подстановок и группы остатков по модулю) в предыдущих листках.

Соглашение. Все числа в этом листке предполагаются целыми, а число p — простым.

Определение 1. *Бинарной операцией* $\cdot$ на множестве M называется отображение из множества упорядоченных пар $M^2 = \{(a, b) \mid a \in M, b \in M\}$ в множество M, то есть способ поставить каждой паре элементов множества M единственный элемент этого множества. Образ b пары (a, b) обозначается $a \cdot b$.

Определение 2. Пара $(G, \cdot)$, состоящая из множества G и бинарной операции $\cdot$ на нем, называется *группой*, если выполнены следующие свойства:

1) $\forall a, b, c \in G\colon a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ассоциативность);
2) $\exists e \in G\ \forall a \in G\colon e \cdot a = a \cdot e = a$ (существование единицы);
3) $\forall a \in G\ \exists a^{-1} \in G\colon a^{-1} \cdot a = a \cdot a^{-1} = e$ (существование обратного).

Если в G содержится конечное число элементов, то G называется *конечной группой*. Число элементов конечной группы G называется *порядком* группы G и обозначается $|G|$.

Все три аксиомы в определении группы имеют прозрачный смысл. Ассоциативность — это фактически то, что в начальной школе называют «сочетательным законом» сложения и умножения. Существование единицы — это существование в группе нейтрального по операции элемента, такого как ноль в группе целых чисел по сложению или тождественная подстановка в группе подстановок. Наконец, обратный элемент в группе — это, например, число, противоположное

данному в группе целых чисел по сложению или число, обратное данному, в группе ненулевых рациональных чисел по умножению.

Важно отметить еще и то, что операция в произвольной группе не обязана быть коммутативной (т. е. $a \cdot b$ не всегда равно $b \cdot a$), хотя для сложения и умножения обычных чисел это верно.

> **Соглашение.** Условие ассоциативности означает, что в произведении нескольких сомножителей расстановка скобок не влияет на ответ. Поэтому впоследствии скобки в произведении нескольких сомножителей не ставятся.

Задача 1. Является ли группой:

а) $(\mathbb{Z}, +)$; б) $(\mathbb{Z}, -)$; в) $(\mathbb{N}, \cdot)$; г) $(S_n, \cdot)$;

д) множество четных чисел с операцией сложения;

е) множество нечетных чисел с операцией сложения;

ж) множество отображений $f : X \to X$ с операцией взятия композиции;

з) множество $P(A)$ всех подмножеств множества A с операцией $\cup$;

и) $(P(A), \cap)$; к) $(P(A), \setminus)$;

л) $(P(A), \triangle)$, где $A \triangle B = (A \cup B) \setminus (A \cap B)$;

м) $(\mathbb{Z}/n\mathbb{Z}, +_n)$, где $\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}$, $a +_n b$ — остаток от деления числа $a + b$ на число n;

н) $(\mathbb{Z}/n\mathbb{Z}, \cdot_n)$, где $a \cdot_n b$ — остаток от деления числа ab на число n;

о) $(\mathbb{N}, \cdot)$, где $a \cdot b = a^b$;

п) $(\mathbb{Z}/n\mathbb{Z} \setminus \{0\}, \cdot_n)$;

р) $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot_n)$, где $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \text{НОД}(a, n) = 1\}$?

Если нужно выяснить, является ли множество A с некоторой операцией на нем группой, это можно сделать двумя способами. Первый — напрямую проверить все три аксиомы. Здесь нужно быть осторожными, поскольку операция, на первый взгляд нормальная, может быть вообще не определена или может выводить за пределы множества. Например, множество нечетных чисел с операцией «сложение» группой не является — сумма двух нечетных чисел не является нечетной.

Второй способ — проверить, не является ли данное множество A подгруппой уже имеющейся группы B с той же операцией. Типичный пример — подгруппа четных чисел в группе целых чисел. Про подгруппы будет более подробно сказано в одном из следующих комментариев.

Решение. а) Да, здесь все три аксиомы выполнены. Роль единицы группы играет ноль в целых числах, а обратный элемент к каждому числу — это его противоположное.

б) Не является; не выполнена самая первая аксиома — ассоциативность. Например, $1-(1-2)$ не равно $(1-1)-2$.

в) Натуральные числа не являются группой ни по умножению, ни по сложению, так как не выполняется аксиома об обратном элементе. Если рассмотреть самое обычное натуральное число 2, то ни -2, ни $1/2$ в натуральных числах не лежат. Хотя в случае умножения выполняются первые две аксиомы.

Объекты, в которых выполняются все аксиомы группы, кроме существования обратного, называются *моноидами*.

г) Да, является. Единичным элементом в этом случае будет тождественная подстановка. Группа S_n — это первый пример некоммутативной группы, то есть группы, в которой неверно, что всегда $a \cdot b = b \cdot a$. Пример: рассмотрим группу S_3, а в ней две подстановки — транспозицию (12) и цикл (123). Тогда (12)(123) равно (23), а (123)(12) равно (13).

д) Да, четные числа являются группой. Все три аксиомы выполняются, это проверяется аналогично пункту а).

Это первый пример подгруппы — подмножества, на котором структура группы наследуется от множества, его содержащего. В данном случае структура группы наследуется от целых чисел. Вообще, если подмножество H группы G таково, что умножение его элементов друг на друга и взятие обратного не выводят за пределы H, то эти операции задают на H структуру группы.

е) В этом случае у нас даже не определена операция на множестве. Сумма двух нечетных чисел нечетной не является.

ж) Это множество будет группой, если и только если в множестве X ровно один элемент. Во всех остальных случаях для отображений выполняется ассоциативность и есть единица — тождественное отображение, но не для всех отображений найдется обратное. Например, обратного нет для отображения всего множества в какой-то один элемент.

Если же рассматривать только биективные отображения, то получается группа перестановок элементов этого множества (см. листки «Подстановки 1, 2»). Отметим, что аксиомы группы — это фактически свойства взаимно однозначных отображений множества в себя. А именно: существование тождественного и обратного отображений, а также ассоциативность взятия композиции.

з) Если множество A — непустое, то $P(A)$ группой не является. Единицей в этом случае может быть только пустое множество, но тогда для остальных не выполняется аксиома об обратном элементе.

и) Если множество A — непустое, то $P(A)$ группой не является. Единицей должно быть все множество A, но тогда не у всех элементов будет обратный.

к) Если множество A — непустое, то $P(A)$ группой не является. Единицей должно быть пустое множество, но тогда не выполняется аксиома об обратном элементе. Более того, в этом случае не выполняется и ассоциативность.

л) Да, в этом случае $P(A)$ всегда будет группой. Выполнение ассоциативности следует из тождества $A \triangle (B \triangle C) = (A \triangle B) \triangle C$, которое доказывалось в листке «Теория множеств 1». Единицей группы будет пустое множество, а обратным к каждому элементу будет он сам. Эта структура на множестве подмножеств называется *булевой алгеброй*.

м) Является. Асоциативность выполняется, поскольку остатки от деления чисел $(a+b)+c$ и $a+(b+c)$ на n совпадают. Единица группы — это остаток 0, а обратный элемент к данному — это остаток, соответствующий противоположному числу. Этот пункт дает еще один важный пример группы — группы вычетов по модулю n.

Группа вычетов — один из важнейших примеров коммутативной группы (где $ab = ba$ для любых a и b), наряду с $\mathbb{Z}$. С теорией коммутативных групп мы уже фактически сталкивались в листках про целые числа и остатки.

н) Не является. Для остатка 0 мы не сможем найти обратный, поэтому не выполняется третья аксиома.

о) Нет, в этом случае не выполнена ассоциативность.

п) Если n — простое, то является, в противном случае — нет. Рассмотрим сначала случай, когда n — составное. Тогда найдутся числа $0 < a < n$, $0 < b < n$ такие, что $a \cdot b = n$. Следовательно, в этом случае наше множество даже не будет замкнутым относительно введенной операции.

Если же n — простое, то, как доказывалось в листке «Целые числа 2», для любого числа $0 < a < n$ найдется такое b, что $ab \equiv 1$ по модулю p. Значит, если мы положим единичный остаток за единичный элемент, то все три аксиомы группы будут выполнены.

р) Да, является при любых n. Если $0 < a < n$ и $\text{НОД}(a, n) = 1$, то найдется $0 < b < n$ такое, что $ab \equiv 1$ по модулю n (это следует из того, что уравнение $ax + by = \text{НОД}(a, b)$ всегда имеет решение в целых числах). Ясно, что тогда и b будет взаимно просто с n. Значит, все

три аксиомы выполнены (истинность первых двух мы уже проверяли в предыдущих задачах).

Эта задача дает запас примеров групп. Разные утверждения о группах бывает полезно проверять сначала на каких-нибудь из этих примеров. Проще всего обычно проверка для коммутативных групп $\mathbb{Z}$ и $\mathbb{Z}/n\mathbb{Z}$, а случай S_n часто позволяет полностью разобраться в происходящем.

Определение 3. Группа G называется *коммутативной* (или *абелевой*), если для любых $a, b \in G$ выполнено $ab = ba$.

Задача 2. Какие из групп задачи 1 коммутативны?

Ответ. Все кроме группы перестановок.

В качестве еще одного полезного примера некоммутативной группы приведем группу движений плоскости или пространства. К примеру, композиция двух осевых симметрий на плоскости относительно прямых, пересекающихся под углом α, является поворотом на угол 2α с центром в точке пересечения прямых, направление которого зависит от порядка, в котором берется композиция.

Задача 3. Докажите, что:
а) единица единственна; б) обратный элемент единственен;
в) $ba = e \Rightarrow b = a^{-1}$; г) $ba = a \Rightarrow b = e$; д) $(a^{-1})^{-1} = a$.

Решение. а) Докажем от противного. Предположим, что существует две единицы e и e'. Тогда по определению единицы, $e = ee' = e'$, следовательно, $e = e'$.

б) Опять предположим, что для данного a существуют два таких элемента b и c, что $ba = ca = ab = ac = e$. Умножим равенство $ab = ac$ слева на b. Получим, что $b = bab = bac = c$, то есть $b = c$.

в) Здесь нужно доказать, что также и $ab = e$. Умножим равенство $ba = e$ справа на b, а слева на b^{-1}. Получим, что $ab = b^{-1}bab = b^{-1}b = e$.

г) Умножив обе части равенства $ba = a$ на a^{-1} справа, получим, что $b = baa^{-1} = aa^{-1} = e$.

д) Так как $aa^{-1} = e$, согласно пункту в) $a = a^{-1}$.

Задача 4*. Докажите, что если в определении 2 свойства существования единицы и существования обратного заменить на свойства
1°) $\exists e \in G\ \forall a \in G\colon ea = a$ (левая единица);
2°) $\forall a\ \exists a^{-1}\colon a^{-1}a = e$ (левый обратный),
то получится определение группы, эквивалентное определению 2.

Решение. Нужно доказать два утверждения: $\forall a \in G\ ae = a$ и $\forall a \in G\ aa^{-1} = e$. Докажем сначала первое. Запишем равенство $(a^{-1}a)e =$

$= ee = e = a^{-1}a$ и умножим его на $(a^{-1})^{-1}$ слева: $(a^{-1})^{-1}a^{-1}(ae) = (a^{-1})^{-1}a^{-1}a$. Обозначим $(a^{-1})^{-1}a^{-1}$ за b, тогда последнее равенство примет вид $bae = ba$. Домножая его слева на b^{-1}, получаем $ae = a$.

Теперь докажем, что $aa^{-1} = e$. Умножим равенство $a^{-1}aa^{-1} = ea = a^{-1}$ слева на $(a^{-1})^{-1}$, получим, что $(a^{-1})^{-1}a^{-1}aa^{-1} = (a^{-1})^{-1}a^{-1}$. Домножая обе части слева на обратное к $(a^{-1})^{-1}a^{-1}$, получаем $aa^{-1} = e$, что и требовалось доказать.

Аналогично доказывается, что в определении группы достаточно требовать существование правой единицы и правого обратного. Однако из существования только *левой* единицы и *правого* обратного не следует выполнение аксиом группы: контрпример дает произвольное множество с операцией $a * b = b$.

Определение 4. Отображение $f\colon G \to H$ из группы G в группу H называется изоморфизмом, если оно взаимно однозначно и сохраняет операцию, то есть $\forall x, y \in G \ \ f(x * y) = f(x) * f(y)$. Если такое отображение существует, то группы G и H называются изоморфными.

Задача 5. Выпишите все попарно неизоморфные группы из: а) 1, 2, 3; б) 4; в*) 13 элементов.

Указание. К пунктам б) и в) можно вернуться после доказательства теоремы Лагранжа.

Один из способов задавать группы — это «таблица умножения» — квадратная таблица, в которой строки и столбцы занумерованы элементами группы, а в каждой клетке записано произведение (в рассматриваемой группе) «номера» строки на «номер» столбца.

Ясно, что каждой такой таблице, строки и столбцы которой пронумерованы множеством G, соответствует ровно одна бинарная операция на G. Осталось понять, когда эта операция задает структуру группы. Для этого в таблице должны быть строка и столбец, соответствующие единичному элементу, должна выполняться ассоциативность (это условие на таблице проверять сложнее всего); наконец, элементы в одном столбце (в одной строке) не должны повторяться — это условие существования обратного.

Решение. а) Группы из одного элемента — это просто e. Далее, группы из двух элементов состоят из a и e и таблица умножения там такова: $aa = e$, $ae = ea = a$. Эти два пункта разбираются несложно. Группа из трех элементов содержит e, a и b, причем все они не равны друг другу. Рассмотрим элемент ab: он не может быть равен ни a, ни b, поэтому $ab = e$ и $b = a^{-1}$. Значит, a^2 не может быть равно ни a, ни e, поэтому b также равно a^2. Получаем, что любая группа из трех элементов

порождается степенями какого-то одного, то есть, как говорят, является циклической. Следовательно, группа из трех элементов также единственна.

б) Перейдем теперь к случаю группы из четырех элементов. Можно перебрать возможные таблицы умножения, но удобнее воспользоваться задачей 10 листка. Для каждого неединичного элемента x из группы верно либо то, что $x^2 = e$, либо то, что $x^4 = e$ и $x^2 \neq e$. Если для всех элементов $x^2 = e$, то эта группа изоморфна группе $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ пар остатков по модулю 2. Если же существует элемент x, такой что $x^2 \neq e$, то группа изоморфна циклической группе $\mathbb{Z}/4\mathbb{Z}$ (остатку k при этом изоморфизме соответствует x^k).

в) Рассмотрим какой-нибудь неединичный элемент x нашей группы G. Пусть $\langle x \rangle$ — множество его степеней. Заметим, что это подгруппа, значит, ее порядок делит порядок группы. Но порядок группы равен 13, а это число простое. Значит, $\langle x \rangle$ совпадает со всей подгруппой, т. е. $G \cong \mathbb{Z}/13\mathbb{Z}$.

Отметим, что при решении пункта в) было, в сущности, доказано, что любая группа простого порядка — циклическая.

Определение 5. Непустое подмножество H группы G, замкнутое относительно операций $\cdot$ и взятия обратного элемента, называется *подгруппой*.

См. комментарий к задаче 1д.

Задача 6. Верно ли, что:
а) если H — подгруппа G, то $e \in H$;
б) если H — подгруппа G, то H — группа;
в) если K — подгруппа H, а H — подгруппа G, то K — подгруппа G;
г) объединение двух подгрупп — подгруппа;
д) пересечение двух подгрупп — подгруппа?

Решение. а) Конечно же, верно: если $g \in H$, то и $g^{-1} \in H$, а тогда $e = gg^{-1} \in H$.

б) Да, по предыдущему пункту.

в) Верно, так как K замкнуто относительно операции и взятия обратного в H, а следовательно, и в G.

г) Нет, не верно. Это множество не обязательно будет замкнуто относительно операции. Пример — объединение множеств четных чисел и чисел, делящихся на 3, являющихся подгруппами $\mathbb{Z}$.

д) Да, верно. Если два множества замкнуты относительно операции и взятия обратного элемента, то и их пересечение обязано быть замкнутым. В самом деле, пусть B и C — произвольные подгруппы

произвольной группы A. Тогда, если $x, y \in B \cap C$, то $x * y \in B$, $x * y \in C$, $x^{-1} \in B$ и $x^{-1} \in C$, то есть $x * y \in B \cap C$ и $x^{-1} \in B \cap C$.

Задача 7. Верно ли, что:

а) $\mathbb{N}$ — подгруппа $\mathbb{Z}$;

б) A_n — подгруппа S_n, где A_n — множество четных подстановок на множестве из n элементов;

в) $S_n \setminus A_n$ — подгруппа S_n?

Решение. а) Нет, не верно: $\mathbb{N}$ не замкнуто относительно взятия обратного.

б) Верно. Это следует из того, что произведение двух четных подстановок — четная, и обратная к четной — также четная.

в) Неверно. В этом множестве даже не лежит единица группы. Но даже добавив к $S_n \setminus A_n$ тождественную подстановку e, мы не получили бы подгруппу, поскольку полученное множество не замкнуто относительно операции. Например, в группе S_3 выполнено $(1\,2)(2\,3) = (2\,3\,1)$, но подстановки $(1\,2)$ и $(2\,3)$ лежат в $S_3 \setminus A_3 \cup e$, а $(2\,3\,1)$ там не лежит.

Задача 8. Перечислите все подгруппы: а) S_3; б) $\mathbb{Z}$.

Указание. При перечислении подгрупп может помочь простая идея: если G — подгруппа H и $a \in G$, то $\forall n\ a^n \in G$.

Решение. а) В группе S_3 всего 6 элементов. Заметим сперва, что если в какой-то подгруппе S_3 есть и транспозиция, и цикл длины 3, то эта подгруппа совпадает со всей S_3, поскольку любой элемент S_3 можно получить, перемножая транспозицию и цикл длины 3.

Осталось заметить, что если в подгруппе лежат только циклы, и нет ни одной транспозиции, то она совпадает с A_3, а если нет циклов — то в этой подгруппе ровно два элемента, один из которых — тождественная подстановка, другой — транспозиция (так как подгруппа, содержащая две транспозиции, совпадает с S_3). Итак, получаем всего 6 подгрупп S_3: единичная подгруппа, три подгруппы, соответствующие транспозициям, подгруппа A_3 и сама S_3.

б) В решении этой задачи ключевой момент следующий: если два целых числа лежат в какой-то подгруппе $\mathbb{Z}$, то и остаток от деления одного числа на другое лежит в этой подгруппе.

Ответ: это либо нулевая подгруппа, либо подгруппа вида $n\mathbb{Z}$, где $n \neq 0$.

Действительно, пусть A — нетривиальная подгруппа $\mathbb{Z}$. Тогда в ней существует ненулевой элемент m с наименьшим модулем. Докажем теперь, что все $a \in A$ обязаны делиться на m нацело. Если какой-то

$a \in A$ не делится на m, то для него верно, что $a = bm + r$, где $0 < r < |m|$. Но тогда и $r \in A$, то есть модуль r меньше модуля m. Получили противоречие, поэтому элемент m порождает всю группу A. Заметим, что A совпадает с $\mathbb{Z}$ тогда и только тогда, когда $m = \pm 1$.

Определение 6. Наименьшее натуральное k, такое что для элемента $a \in G$ выполняется равенство $a^k = e$, называется *порядком элемента* a. Обозначение: $\operatorname{ord} a$. Если такого числа не существует, то говорят, что $\operatorname{ord} a = 0$.

Задача 9. Докажите, что в конечной группе $\operatorname{ord} a > 0$ для любого элемента a.

Решение. Начнем возводить a в положительную степень. Так как группа конечна, то $a^k = a^l$ для некоторых положительных k и l, $k < l$. Следовательно, $a^{l-k} = e$.

Задача 10. Докажите, что $a^n = e$ тогда и только тогда, когда $\operatorname{ord} a \mid n$.

Решение. Разделим n на $\operatorname{ord} a$ с остатком: $n = m \cdot \operatorname{ord} a + k$. Если остаток k не равен нулю, то тогда $k < \operatorname{ord} a$. Поскольку $a^n = e$ и $a^{\operatorname{ord} a} = e$, a^k также равно e. Это противоречит определению $\operatorname{ord} a$.

Определение 7. *Левым (правым) смежным классом* группы G относительно подгруппы H называется множество вида $aH = \{ax \mid x \in H\}$ (соответственно вида $Ha = \{xa \mid x \in H\}$).

Задача 11. Докажите, что левые (правые) смежные классы между собой либо не пересекаются, либо совпадают.

Иными словами, множество элементов группы всегда можно как минимум двумя способами разбить на классы эквивалентности — на левые и правые смежные классы. Вообще говоря, это разные разбиения.

Решение. Докажем это утверждение для левых смежных классов (для правых доказательство аналогично). Если два левых смежных класса aH и bH имеют непустое пересечение, то это значит, что $ah_1 = bh_2$ для каких-то элементов $h_1, h_2 \in H$. Следовательно, $b = ah_1(h_2)^{-1} = ah$, где $h \in H$. Пусть теперь x — произвольный элемент bH, тогда $x = bh_3 = (ah)h_3 = a(hh_3)$, откуда заключаем, что $x \in aH$. Поэтому классы aH и bH совпадают.

Задача 12. Найдите разбиение на левые и правые смежные классы группы по подгруппе: а) $\mathbb{Z}/2\mathbb{Z}$; б) S_4/A_4; в) $S_3/\langle(12)\rangle$.

Решение. а) Одним из смежных классов является сама подгруппа $2\mathbb{Z}$ (четные числа). Вторым же — все нечетные числа. Чтобы это увидеть,

можно взять какое-нибудь нечетное число (например, 1) и прибавить к нему все четные числа (нет разницы, справа или слева). Ясно, что таким образом можно получить все нечетные.

б) Здесь также всего два смежных класса (правые и левые опять совпадают). Это доказывается аналогично: один из смежных классов — A_4, а второй — все нечетные подстановки — можно получить умножением произвольной транспозиции на все подстановки из A_4.

в) Здесь правых и левых смежных классов будет по три. Но они не будут совпадать между собой, как в предыдущих пунктах. Левые смежные классы: $\{(e), (12)\}$, $\{(13), (132)\}$ и $\{(23), (123)\}$, а правые смежные классы — $\{(e), (12)\}$, $\{(13), (123)\}$ и $\{(23), (132)\}$.

Задача 13 (теорема Лагранжа). Докажите, что для любой конечной группы G подрядок любой ее подгруппы H делит порядок группы G ($|G| \vdots |H|$).

Решение. Из предыдущей задачи мы знаем, что группа G распадается на непересекающиеся подмножества — левые смежные классы по H. Заметим теперь, что отображение $h \mapsto ah$, где a — любой элемент смежного класса, задает биекцию из H в этот класс. Значит, в каждом подмножестве элементов столько же, сколько в подгруппе H. Отсюда получаем, что $|G|$ должен делиться на $|H|$.

Задача 14. Докажите, что порядок любого элемента конечной группы G делит порядок группы G ($|G| \vdots \operatorname{ord} a$).

Указание. Для каждого элемента a группы G мы можем рассмотреть множество $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$, которое обязательно будет подгруппой.

Решение. Рассмотрим подгруппу $\langle a \rangle$. Тогда ее порядок (число элементов) равен в точности $\operatorname{ord} a$, поскольку $a^0 = e$, $a^{\operatorname{ord} a} = e$ и $a^k \neq e$ ни при каком $0 < k < \operatorname{ord} a$. Но по предыдущей задаче порядок подгруппы делит порядок группы G.

Определение 8. Обозначим через $\varphi(n)$ число натуральных чисел, не превосходящих n и взаимно простых с n. Функция $\varphi(n)$ называется *функцией Эйлера*.

Другое определение функции $\varphi(n)$ — число обратимых по умножению элементов в группе остатков $\mathbb{Z}/n\mathbb{Z}$.

Задача 15. Найдите: а) $\varphi(2)$, $\varphi(6)$, $\varphi(30)$; б) $\varphi(p)$; в) $\varphi(p^n)$.

Решение. а) Эти задачи решаются прямым перебором $\varphi(2) = 1$, $\varphi(6) = 2$, $\varphi(30) = 8$.

б) Если число p — простое, то все натуральные числа, меньшие его, взаимно просты с p. Поэтому $\varphi(p) = p - 1$.

в) Натуральные числа, не превосходящие p^n и имеющие с ним общий делитель, обязаны делиться на p. Поэтому их всего p^{n-1}, включая само p^n. Поэтому $\varphi(p^n) = p^n - p^{n-1}$.

Задача 16. Докажите, что для любых взаимно простых чисел m и n выполнено равенство $\varphi(mn) = \varphi(m)\varphi(n)$.

Решение. Выпишем все числа от 1 до mn в таблицу из m столбцов и n строк. Тогда вычеркнуть в ней все числа, имеющие с n общий делитель, очень просто: это числа, стоящие в строках, имеющих номер, не взаимно простой с n. Рассмотрим оставшиеся строки — их всего $\varphi(n)$. Числа, стоящие в них, имеют вид k, $k+n$, $k+2n$, …, $k+(m-1)n$ — всего m штук. Поскольку m и n взаимно просты, все эти числа дают разные остатки при делении на m. Значит, среди них (а следовательно, и в каждой строке) всего $\varphi(m)$ взаимно простых с m.

Задача 17. Найдите $\varphi(p_1^{k_1} \cdot \ldots \cdot p_n^{k_n})$.

Решение. По уже доказанному

$$\varphi(p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}) = \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_n^{k_n}) = (p_1^{k_1} - p_1^{k_1-1}) \cdot \ldots \cdot (p_n^{k_n} - p_n^{k_n-1}).$$

Перепишем этот ответ в другой форме. Пусть $n = p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, тогда $\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_n}\right)$, где $p_1, p_2, \ldots, p_n$ — все различные простые делители n.

Задача 18 (теорема Эйлера). Докажите, что для любого числа a, взаимно простого с n, выполнено равенство $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Решение. Вспомним, что $\varphi(n)$ равно порядку группы $(\mathbb{Z}/n\mathbb{Z})^\times$. Но по теореме Лагранжа, если $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, то $\operatorname{ord} a$ делит $|(\mathbb{Z}/n\mathbb{Z})^\times|$. А так как $a^{\operatorname{ord} a} \equiv 1 \pmod{n}$, имеем $a^{|(\mathbb{Z}/n\mathbb{Z})^\times|} \equiv 1 \pmod{n}$.

Задача 19*. Опишите группы симметрий: а) правильного треугольника; б) квадрата; в) правильного n-угольника (*группа диэдра* D_n).

Решение. Группа симметрий данной фигуры — это группа, состоящая из движений плоскости, переводящих фигуру в себя. При доказательстве мы будем пользоваться следующим фактом из курса планиметрии: движение полностью задается образами трех точек, которые не лежат на одной прямой.

а) Найдем теперь группу симметрий правильного треугольника. Очевидно, что при движении вершины переходят в вершины, поэтому все движение задается образами трех вершин, то есть подстанов-

кой из группы S_3. Значит, наша группа преобразований является подгруппой S_3. Докажем, что она совпадает со всей S_3. Для этого достаточно проверить, что для любой перестановки вершин существует движение, которое ее реализует. Если перестановка меняет местами какие-то вершины A и B, оставляя на месте вершину C, то искомое движение — симметрия относительно биссектрисы угла ACB. Если же перестановка переводит A в B, B в C, а C в A, то искомое движение — поворот относительно центра треугольника на 120°, переводящий A в B (любой такой поворот переводит либо A в B, либо наоборот).

б) Пусть A, B, C, D — последовательно идущие вершины квадрата. Мы хотим описать все движения f, оставляющие квадрат на месте. Ясно, что по соседству с вершиной $f(A)$ находятся $f(B)$ и $f(D)$. Образы вершин A, B и D полностью задают движение f. Рассмотрим поворот g вокруг центра квадрата на угол, кратный 90°, переводящий $f(A)$ обратно в A. Тогда $g(f(A)) = A$, а для вершин B и D есть две возможности: либо $g(f(B)) = B$ и $g(f(D)) = D$, либо наоборот, $g(f(B)) = D$, $g(f(D)) = B$.

В первом случае движение $g \circ f$ имеет три неподвижные точки A, B, D, и следовательно, тождественно. Значит, и отображение $f = g^{-1}$ являлось поворотом на угол, кратный 90°. Во втором случае рассмотрим симметрию b относительно диагонали AC. Тогда движение $b \circ g \circ f$ также имеет три неподвижные точки и, как следствие, тривиально. Поэтому движение f является композицией симметрии относительно AC и поворота вокруг центра квадрата на угол, кратный 90°.

Опишем теперь получившуюся группу. Пусть a — поворот вокруг центра квадрата на 90° против часовой стрелки. Тогда все повороты, оставляющие квадрат на месте, имеют вид a, a^2, a^3, a^4 (тождественное преобразование). Пусть, далее, b — симметрия относительно прямой AC. Согласно доказанному мы знаем, что любой элемент группы симметрий представляется либо в виде a^k, либо в виде $b \cdot a^k$ для $k = 0, \ldots, 3$. Поэтому в группе симметрий квадрата всего 8 элементов. Для полного ответа осталось полностью описать умножение в этой группе, то есть найти, чему равно $a \cdot b$. Если $ab = a^k$ для какого-то k, то тогда $b = a^{k-1}$, что неверно, так как симметрия и поворот — разные движения. Поэтому $ab = ba^k$. Осталось найти это k. $ab = ba^k \;\Rightarrow\; a^k = b^{-1}ab$. Поскольку b — симметрия, $b = b^{-1}$. Теперь вычислим композицию $b \circ a \circ b$. Прямой проверкой получаем, что это поворот на 90° по часовой стрелке, то есть a^3. Значит, $ab = ba^3$.

в) Решение этого пункта аналогично предыдущему. Точкой A будет произвольная вершина n-угольника, точками B и D — ее соседи.

Симметрия в данном случае будет относительно прямой, соединяющей A с центром n-угольника, которая не обязательно является диагональю. Разница будет еще лишь в том, что повороты будут кратными не 90°, а $360°/n$.

Группа симметрий имеет $2n$ элементов и две образующие — a и b, соответствующие, опять же, повороту и симметрии. Порядок элемента a равен n, порядок элемента b равен 2, а умножение в группе удовлетворяет соотношению $ab = ba^{n-1}$.

Теория графов 2

листок 3д / март 2005

Как и в первом листке по теории графов, большинство задач в первой части листка не объединяет никакой общий сюжет (разве что многие из них формально связаны с путями в графах), но возникают разные небольшие группы задач, объединенные общей темой.

Среди отдельных задач стоит отметить теорему Кэли о числе деревьев и теорему Холла о совершенном паросочетании.

Конец листка посвящен планарным графам, т. е., по существу, началам комбинаторной топологии. Основные результаты здесь — знаменитая формула Эйлера и критерий планарности Понтрягина — Куратовского.

Задача 1. В турнире по олимпийской системе участвовали n команд. Сколько всего было сыграно матчей?

Решение. Раз соревнования проводились по олимпийской системе, из n команд ровно одна стала победителем, а все остальные отсеялись в турнире. При этом после каждого сыгранного матча уходила ровно одна команда — проигравшая. Значит, всего партий было сыграно $n-1$.

Задача 2. Докажите, что граф с n вершинами, степень каждой из которых не менее $\frac{n-1}{2}$, связен.

Решение. Предположим, что у графа как минимум две компоненты связности и выберем ту, в которой меньше всего вершин. По принципу Дирихле, их не больше чем $\frac{n}{2}$, а значит, степень каждой из них не больше $\frac{n}{2}-1$, что меньше $\frac{n-1}{2}$ — противоречие.

Задача 3. В связном графе все вершины имеют степень 100. Докажите, что после удаления любого из ребер он остается связным.

Указание. Воспользуйтесь тем, что в любой связной компоненте графа сумма степеней вершин четна, так как она равна удвоенному числу ребер в этой компоненте.

Решение. Предположим, что граф стал несвязным после удаления какого-то ребра и рассмотрим одну из получившихся связных компонент. Степени всех ее вершин равны 100, кроме одной, степень которой равна 99. Получаем, что сумма степеней вершин в этой компоненте нечетна, что не может быть верно. Значит, исходный граф после удаления любого ребра остается связным.

Задача 4. Докажите, что в любом связном графе есть подграф, являющийся деревом и содержащий все вершины (максимальное поддерево).

Решение. Доказательство проведем индукцией по числу ребер. База (когда ребро одно) очевидна, докажем шаг. Если рассматриваемый нами связный граф является деревом, то утверждение доказано. Если же нет, то в нем есть хотя бы один простой цикл (цикл, в котором каждое ребро встречается лишь один раз). Удалим произвольное ребро из этого цикла и заметим, что полученный граф останется связным, но будет иметь на одно ребро меньше. Теперь можно применить предположение индукции.

Задача 5. Докажите, что из любого связного графа можно выкинуть вершину и выходящие из нее ребра так, чтобы он остался связным.

Решение. Рассмотрим в этом связном графе максимальное поддерево и выкинем одну из его висячих вершин (то есть вершину, из которой выходит ровно одно ребро этого дерева) вместе со всеми выходящими из нее ребрами. Тогда оставшееся поддерево, а значит, и весь оставшийся граф, будут связными.

Задача 6*. В кубической коробке $n \times n \times n$ лежало n^3 единичных кубиков. Кубики высыпали, каждый просверлили по диагонали, затем все плотно нанизали на нить и связали в кольцо (соединили вершину первого кубика с вершиной последнего). При каких n получившееся «ожерелье» можно убрать обратно в коробку?

Указание. Расставим на диагоналях кубиков стрелки так, чтобы нить превратилась в ориентированный цикл и посмотрим, сколько стрелок идет вверх и сколько вниз.

Ответ. Если n нечетно, то уложить нельзя, если n четно — то можно.

Решение. Если n нечетно, то число кубиков также нечетно. Расставим на диагоналях кубиков стрелки так, чтобы они образовывали цикл и предположим, что «ожерелье» из кубиков удалось уложить в коробку. Тогда стрелки на диагоналях кубиков смотрят либо вверх, либо вниз, и число идущих вверх равно числу идущих вниз. Но всего стрелок столько же, сколько кубиков, то есть нечетное число — получаем противоречие.

В случае, если n четно, «ожерелье» из кубиков можно уложить в коробку, что показывается явно.

Задача 7*. Все 28 Петиных одноклассников имеют по различному числу друзей в этом классе. Сколько из них дружат с Петей? А если одноклассников n?

Ответ. Если число одноклассников n четно, то с Петей дружат $n/2$. Если же n нечетно, то возможны два ответа — $(n-1)/2$ или $(n+1)/2$.

Решение. Доказывать будем индукцией по n. База индукции проверяется явно, докажем шаг. Выберем двух Петиных одноклассников, у которых число друзей, соответственно, наибольшее и наименьшее. Имеется две возможности — число друзей у этих одноклассников равно 0 и 27 или 1 и 28 соответственно. В обоих случаях можно убедиться, что если исключить их из класса, то у всех оставшихся Петиных одноклассников снова будет по различному числу друзей. Кроме того, число Петиных друзей уменьшится на 1. Теперь можно применить предположение индукции и свести все к случаю, когда число одноклассников равно двум (четный случай) или трем (нечетный).

> **Задача 8* (теорема Кэли).** В графе с n вершинами каждая вершина соединена с каждой ребром (такой граф называется *полным*). Докажите, что существует ровно n^{n-2} способов выкинуть несколько ребер так, чтобы оставшийся граф являлся деревом.

Набросок решения. Опишем конструкцию, лежащую в основе доказательства. Занумеруем все вершины графа числами от 1 до n. Идея состоит в том, что нужно сопоставить каждому дереву в полном графе набор из $n-2$ чисел.

Делается это следующим образом. Если имеется дерево в полном графе с n вершинами, то мы выбираем в нем лист (висячую вершину) с наименьшим номером, выкидываем его и записываем номер той вершины, с которой он был соединен. Это повторяется $n-2$ раза, и утверждается, что полученные таким образом $n-2$ числа, в свою очередь, однозначно задают исходное дерево. Кроме того, нужно еще показать, что любой набор из $n-2$ чисел от 1 до n так получается.

> **Определение 1.** *Ориентированным графом* называется граф, на ребрах которого поставлены стрелки. Его ребра называются *дугами*. Более формально, ориентированный граф — это пара $\Gamma = (V, E)$ из конечного множества вершин V и множества дуг E, элементами которого являются упорядоченные пары вершин графа Γ.
>
> Заметим, что у нас в ориентированном графе разрешаются дуги из вершины в себя саму (*петли*), несколько дуг из одной вершины в другую (*кратные дуги*), «встречные» дуги (из A в B и из B в A).
>
> То, что раньше называлось графом, мы теперь будем называть *неориентированным графом*.

Выше мы даем два определения ориентированного графа — формальное и неформальное, призванные дополнять друг друга в том

смысле, что формальное определение нужно для строгих обоснований решений задач, а неформальное используется в процессе решения задачи и при описании сути дела.

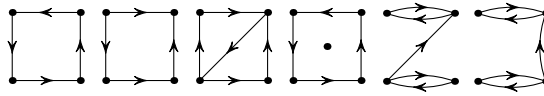
Задача 9. Дайте (формальные!) определения *пути* и *цикла* в ориентированном графе.

Решение. *Путем* в ориентированном графе Г называется последовательность ребер (упорядоченных пар $(a_1, b_1), \ldots, (a_n, b_n)$), такая что каждая пара (a_i, b_i) является подмножеством множества ребер E и, кроме того, вершины a_i и b_{i-1} совпадают для любого $i = 2, \ldots, n$.

Циклом в ориентированном графе Г называется путь $(a_1, b_1), \ldots, (a_n, b_n)$, в котором совпадают вершины a_1 и b_n.

Определение 2. Ориентированный граф называется *сильно связным*, если для любых двух его вершин существует путь как из первой во вторую, так и из второй в первую.

Задача 10. Какие из следующих графов сильно связны?

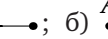
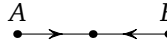


Ответ. Первый, третий и шестой, что видно из рисунка.

Определение 3. Ориентированный граф называется *связным*, если он окажется связным неориентированным графом после того, как мы сотрем стрелки с его дуг.

Задача 11. а) Приведите пример связного, но не сильно связного ориентированного графа.

б) Приведите пример связного ориентированного графа, в котором для некоторых двух вершин A и B нет пути ни из A в B, ни из B в A.

Ответ. а)  ; б) 

.

Задача 12. Докажите, что на ребрах связного неориентированного графа можно так расставить стрелки, чтобы из одной из вершин существовали пути во все остальные.

Решение. Рассмотрим в графе максимальное поддерево. Оно связно, так как исходный граф связен, и в нем есть висячая вершина A. Теперь расставим стрелки на ребрах так, чтобы все они вели «от» A (то есть, если ребро соединяет две вершины B и C, и B дальше от A, чем C, то стрелка ведет от C к B).

На оставшихся ребрах, не содержащихся в максимальном поддереве, можно расставить стрелки произвольным образом. Видно теперь, что из A есть пути во все остальные вершины.

> **Задача 13.** Можно ли так расставить на ребрах полного неориентированного графа стрелки, чтобы в полученном ориентированном графе не было циклов?

Решение. Можно. Занумеруем все вершины графа числами от 1 до n и расставим стрелки так, чтобы они вели из большей вершины в меньшую. Тогда в полученном графе циклов быть не может, так как вдоль любого пути номер вершины все время увеличивается.

> **Задача 14.** В полном неориентированном графе на ребрах как-то расставили стрелки. Докажите, что найдется вершина, из которой существуют пути во все остальные.

Решение. Докажем по индукции: база для $n = 2$ очевидна. Пусть теперь у нас есть полный граф с n вершинами, на ребрах которого произвольным образом расставлены стрелки. Удалим произвольную вершину A. В оставшемся графе с $n - 1$ вершиной есть вершина B, из которой существуют пути во все остальные. Если в исходном графе стрелка вела из B в A, то вершина B останется такой, какой нам надо. Если же стрелка вела из A в B, то получаем, что в исходном графе из вершины A существуют пути во все остальные.

> **Задача 15* (задача 17* из листка «Теория графов 1»).** В полном неориентированном графе на ребрах как-то расставили стрелки. Докажите, что полученный граф гамильтонов (т. е. существует путь, проходящий по каждой вершине ровно по одному разу).

Решение. Доказательство проведем индукцией по числу вершин. База очевидна, докажем шаг индукции. Выбросим произвольную вершину A из графа, тогда в оставшемся графе есть гамильтонов путь из вершины с номером 1 в вершину с номером $n - 1$. Разберем несколько случаев. Если из вершины A идет стрелка в вершину 1, добавим ее в гамильтонов путь в начало, и все доказано. Если в вершину A идет стрелка из вершины $n - 1$, добавим ее в гамильтонов путь в конец, и снова все доказано.

Поэтому осталось рассмотреть случай, когда стрелки ведут из 1 в A и из A в $n - 1$. Заметим, что тогда обязательно найдется вершина с таким номером k (в гамильтоновом пути), что стрелка ведет из k в A и из A в $k + 1$. Теперь нужно выкинуть из пути стрелку $k \to k + 1$ и добавить стрелки $k \to A$ и $A \to k + 1$. Все случаи нами разобраны, шаг индукции доказан.

Задача 16*. В полном неориентированном графе с не менее чем тремя вершинами на ребрах как-то расставили стрелки. Докажите, что можно заменить не более одной дуги на противоположную так, чтобы полученный граф стал сильно связным.

Решение. Воспользуемся решением предыдущей задачи. Найдем в графе гамильтонов путь и рассмотрим в нем первую и последнюю вершины. Если стрелка ведет из последней в первую, то путь можно дополнить до цикла, а граф, в котором есть гамильтонов цикл, является сильно связным. Если же стрелка ведет из первой в последнюю, то заменим ее на противоположную.

Определение 4. Количество дуг, входящих в вершину (ориентированного графа), называется *входной полустепенью* (или *полустепенью захода*) этой вершины. Количество выходящих дуг называется *выходной полустепенью* (или *полустепенью исхода*).

Задача 17. Найдите входные и выходные полустепени каждой вершины для всех графов из задачи 10.

Решение. Приведем лишь ответы. Степень вершины будем записывать в виде (a, b), где a — выходная полустепень, b — входная. В первом графе — у всех вершин $(1, 1)$. Во втором — $(2, 0)$, $(1, 1)$, $(1, 1)$, $(0, 2)$. В третьем — $(2, 1)$, $(1, 2)$, $(1, 1)$, $(1, 1)$. В четвертом — $(1, 1)$, $(1, 1)$, $(1, 1)$, $(1, 1)$, $(0, 0)$. В пятом — $(1, 1)$, $(1, 1)$, $(2, 1)$, $(1, 2)$. В шестом — $(1, 1)$, $(1, 1)$, $(2, 2)$, $(2, 2)$.

Задача 18. Что можно сказать о сумме всех входных полустепеней и сумме всех выходных полустепеней одного и того же ориентированного графа?

Решение. Эти суммы равны, так как каждой входящей в какую-то вершину дуге соответствует одна и только одна выходящая (из какой-то вершины) дуга.

Задача 19. Сформулируйте и докажите критерий эйлеровости ориентированного графа.

Решение. Напомним: эйлеровость графа означает, что в нем существует цикл, проходящий по всем ребрам ровно по одному разу. Будем считать, что в графе нет изолированных вершин.

Критерий эйлеровости ориентированного графа следующий: граф эйлеров, если и только если он связен и в каждую вершину входит столько же стрелок, сколько выходит, т. е. входная полустепень каждой вершины равна выходной полустепени.

Необходимость этих условий очевидна. Теперь докажем существование эйлерова цикла при указанных условиях. Доказывать будем индукцией по числу вершин. База очевидна, докажем шаг.

Выберем в графе произвольную вершину и пойдем из нее по какому-либо пути. В силу того, что входная полустепень каждой вершины равна выходной (это свойство называют законом Кирхгофа), мы рано или поздно попадем в вершину, в которой уже были. Таким образом, получаем замкнутый цикл $(A_1 \ldots A_n)$. Выкинем ребра этого цикла из графа. Останется одна или несколько связных компонент, к которым можно применить предположение индукции. Осталось склеить все получившиеся циклы в один, что мы можем сделать в силу предположения о связности исходного графа.

> **Задача 20 (цикл де Брюина).** Для того, чтобы открыть кодовый замок (с кнопками от 0 до 9), необходимо набрать код из четырех цифр, причем не важно, что было нажато до набора правильного кода. За какое наименьшее количество нажатий его можно гарантированно открыть?

Решение. Нарисуем граф, в котором вершинами являются трехзначные комбинации цифр, а стрелки ведут из вершин вида abc в вершины bcd, где a, b, c, d — произвольные цифры. Легко видеть, что ребра в этом графе соответствуют четырехзначным комбинациям на кодовом замке. Кроме того, граф удовлетворяет критерию из предыдущей задачи и, следовательно, является эйлеровым. Поэтому в нем существует цикл, проходящий по всем ребрам ровно по одному разу.

Всего трехзначных комбинаций 1000, полная степень каждой вершины равна 20 (обратите внимание на то, что наличие петли из вершины в себя увеличивает ее степень на 2). Таким образом, длина эйлерова пути равна $\frac{1}{2} \cdot 1000 \cdot 20 = 10000$. Чтобы получить ответ, осталось прибавить три первые цифры.

Ответ. 10003 нажатия.

> **Задача 21.** 20 школьников решали 20 задач. Каждый решил ровно две задачи, и каждую задачу решили ровно двое. Докажите, что можно устроить разбор задач так, чтобы каждый рассказал одну решенную им задачу.

Решение. Рассмотрим следующий граф: одна группа вершин — это школьники, вторая — задачи, а любое ребро соединяет какую-то задачу и решившего ее школьника. Тогда все вершины графа являются двухвалентными. Если выйти из произвольной вершины и пойти по произвольному пути, то легко видеть, что мы рано или поздно

вернемся в вершину, из которой начали, и при этом ни разу не пройдем по одному и тому же ребру дважды. Следовательно, наш граф разобьется на непересекающиеся циклы, а из этого уже легко следует утверждение задачи.

Определение 5. Граф называется *двудольным*, если его вершины можно разбить на две группы (называемые *долями*) так, чтобы все ребра (или дуги) были между различными долями.

Паросочетанием называется такой набор ребер графа, что каждая вершина графа является концом не более одного ребра из набора. Паросочетание называется *совершенным*, если каждая вершина является концом ровно одного ребра паросочетания.

Раскраска вершин графа называется *правильной*, если никакие две вершины одного цвета не соединены ребром. Граф называется *k-дольным*, если правильная раскраска его вершин возможна k цветами и не менее.

Задача 22. Какие графы из задач 1, 2 и 3 первого листка про графы являются двудольными? А сколькодольными являются остальные?

Решение. В двудольном графе обязательно четное число вершин — это поможет при разборе вариантов.

В задаче 1 все графы являтся трехдольными. В задаче 2 мы разберем для краткости лишь графы с четырьмя вершинами. Граф без ребер однодольный, граф с одним ребром и оба графа с двумя ребрами двудольные. Среди графов с тремя ребрами два двудольных и один трехдольный. Из графов с четырьмя ребрами один двудольный, а второй — трехдольный. Граф с пятью ребрами трехдольный, а с шестью — четырехдольный (все вершины разных цветов). В задаче 3 граф стран СНГ является трехдольным, граф чисел от 2 до 15 четырехдольный.

Задача 23. Равносильна ли двудольность неориентированного графа отсутствию циклов нечетной длины?

Решение. Равносильна. Если граф двудольный, то все циклы, очевидно, имеют четную длину. Докажем в другую сторону. Будем раскрашивать вершины графа в два цвета так, чтобы ребра были лишь между вершинами разных цветов (начав с произвольной вершины). Если какая-то вершина оказалась раскрашена таким образом в два цвета, то это означает, что в графе есть цикл нечетной длины, что неверно. Поэтому все вершины можно правильным образом раскрасить в два цвета, а это то же самое, что разбить на две доли.

Задача 24. Любое ли дерево двудольно?

Решение. Да, поскольку дерево — это граф, в котором нет никаких циклов вообще, там нет и циклов нечетной длины.

> **Задача 25* (теорема Холла).** В некой компании n юношей. При каждом $k = 1, 2, \ldots, n$ для любых k юношей в этой компании найдется не менее k девушек, знакомых хотя бы с одним из рассматриваемых k юношей. Можно ли просватать всех юношей за знакомых девушек? Является ли это условие необходимым?
>
> Иными словами, верно ли, что в двудольном неориентированном графе (с n вершинами в первой доле) существует паросочетание размера n тогда и только тогда, когда для каждого набора из k вершин первой доли с ними соединены хотя бы k вершин второй доли?

Решение. Докажем по индукции, что это верно. База ($n = 1$) очевидна, докажем шаг индукции. Если X — множество вершин из первой доли, то через $a(X)$ будем обозначать множество вершин, соединенных с X. Предположим сперва, что выполнено условие $|a(X)| > |X|$ для всех X, $0 < |X| < n$. Тогда выкинем из графа произвольную пару вершин A и B, соединенную ребром, и заметим, что для оставшегося графа также выполнены условия теоремы, а значит, можно применить предположение индукции.

Теперь предположим, что найдется такое X, что $|a(X)| = |X|$. Обозначим через $\bar{X}$ дополнение X в множестве вершин первой доли. Мы утверждаем, что для множеств $X \cup a(X)$ и $\bar{X} \cup a(\bar{X})$, рассматриваемых по отдельности, верны условия теоремы Холла.

Для X это является тавтологией, докажем для $\bar{X}$. Пусть $Y \subset \bar{X}$, тогда $|X \cup Y| \leqslant |a(X \cup Y)|$. Тогда $|X| + |Y| = |X \cup Y| \leqslant |a(X \cup Y)| \leqslant |a(X)| + |a(Y)|$. Но $|X| = |a(X)|$, поэтому $|Y| \leqslant |a(Y)|$, что и требовалось. Теперь можно применить предположение индукции. Все возможные случаи разобраны, теорема доказана.

> **Задача 26* (обобщение задачи 21).** Докажите, что в любом регулярном двудольном неориентированном графе есть совершенное паросочетание.

Решение. Решение задачи следует из теоремы Холла. Регулярность графа означает, что степени всех его вершин равны. Покажем, что $|X| \leqslant |a(X)|$ для любого множества X вершин из первой доли. Если $|X| < |a(X)|$ для какого-то множества $|X|$ и степень каждой вершины равна k, то число ребер, выходящих из $|a(X)|$, заведомо больше $k|X|$. Так как $|X| < |a(X)|$, степень как минимум одной вершины из $|a(X)|$ должна быть больше k, что неверно.

Теперь, поскольку $\forall X \ |X| \leqslant |a(X)|$, утверждение задачи следует из теоремы Холла.

Задача 27*. Верно ли, что при любой правильной раскраске k-дольного неориентированного графа в k цветов найдется путь из k разноцветных вершин?

Решение. Да, верно. Будем обозначать цвета, в которые раскрашены вершины, натуральными числами от 1 до k. Тогда любой вершине X можно поставить в соответствие число $l(X)$ — число путей, заканчивающихся в вершине X и таких, что номера цветов вершин строго возрастают вдоль пути.

Если $l(A) = k$ для какой-то вершины A, то все доказано. А если нет, и для всех вершин $l(X) \leqslant k-1$, то мы можем раскрасить вершины по-новому, поставив в соответствие каждой вершине цвет с номером $l(X)$. А это противоречит тому, что исходный граф является k-дольным.

Заметим, что мы доказали даже более сильное утверждение: что найдется путь, в котором цвета вершин идут в произвольном наперед заданном порядке.

Определение 6. Граф называется *планарным*, если его можно нарисовать на плоскости, изобразив вершины точками, а ребра (или дуги) — непересекающимися кривыми. Граф, который нарисован на плоскости указанным выше образом, называется *плоским*. Части, на которые плоский граф делит плоскость (включая внешнюю часть) называются его *гранями*.

Задача 28. Какие графы из задач 1, 2 и 3а первого листка про графы являются планарными?

Решение. Планарными являются все графы из задач 1, 2 и 3. Заметим, что планарность графа из задачи 3а доказывать не нужно — он уже нарисован на плоскости (карте мира).

Задача 29 (формула Эйлера). Пусть в неориентированном плоском связном графе B вершин, P ребер и Γ граней. Тогда $B+\Gamma-P=2$.

Решение. Предположим, что $\Gamma > 1$. Тогда возьмем произвольные две соседние грани и сотрем произвольное ребро между ними. Число ребер уменьшится на 1, и число граней уменьшится на 1, следовательно, сумма $B+\Gamma-P$ не изменится.

Таким образом, мы спустимся к случаю, когда $\Gamma = 1$. Заметим тогда, что в полученном графе не может быть циклов (иначе было бы хотя бы две разные грани), значит, он является деревом, и $B = P+1$. Следовательно, $B+\Gamma-P = (P+1)+1-P = 2$, что и требовалось доказать.

Задача 30. Чему равно $B+Г-P$ для несвязного неориентированного плоского графа?

Решение. Поскольку для каждой компоненты связности по отдельности $B+Г-P=2$, и одна грань у всех общая, имеем для всего графа $B+Г-P=1+K$, где K — число компонент связности.

Число $B+Г-P$ для связного графа, нарисованного на поверхности, зависит только от самой поверхности и не зависит от конкретного графа. Это число называют *эйлеровой характеристикой* поверхности. Например, для сферы с g ручками эйлерова характеристика равна $2-2g$. Понятие эйлеровой характеристики обобщается и на многомерный случай.

Задача 31. Пусть B, P и $Г$ — количества вершин, ребер и граней многогранника соответственно. Чему равно $B+Г-P$?

Ответ. $B+Г-P=2$.

Решение. Фактически эта задача уже решалась нами выше, здесь мы приведем два неформальных способа ее решения (которые на самом деле имеют далеко идущие обобщения).

Первое решение состоит в следующем: накачаем многогранник воздухом изнутри так, чтобы он превратился в сферу. Тогда сетка из вершин и ребер превратится в какой-то связный граф на поверхности сферы. Выкинем произвольную грань. Тогда та часть сферы, которая осталась, является (с точностью до деформации) диском. Если положить этот диск на плоскость, то возникнет обычный планарный граф, для которого все уже доказано выше.

Второе решение не использует растяжений и геометрических деформаций. Будем рассматривать пересечения многогранника в трехмерном пространстве с координатами $Oxyz$ с полупространствами вида $z \geqslant c$. Сначала, при c, близких к $-\infty$, пересечение совпадает с самим многогранником. Затем плоскость $z=c$ проходит через самую нижнюю вершину, и многогранник как-то меняется (нужно проследить, что величина $B+Г-P$ остается неизменной). Вообще, многогранник меняется только при прохождении плоскости через какие-то вершины, и в этом случае нужно отслеживать изменение величины $B+Г-P$.

Осталось заметить, что перед тем, как плоскость $z=c$ пройдет через последнюю вершину, наш многогранник был или тетраэром, или «косой призмой» — а в этом случае уже нетрудно убедиться в равенстве $B+Г-P=2$.

Задача 32. а) Докажите, что в плоском неориентированном графе $2P \geqslant 3Г$.

б) Докажите, что в плоском двудольном неориентированном графе $P \geqslant 2Г$.

Решение. а) Достаточно заметить, что к каждому ребру примыкает не более двух граней, а к каждой грани — не менее трех ребер, откуда и следует искомое неравенство.

б) Решение аналогично предыдущему случаю, но теперь, поскольку граф двудольный, к каждой грани примыкает уже не менее четырех ребер, поэтому оценку можно усилить.

Задача 33. Докажите, что следующие графы не планарны:

а) полный неориентированный граф с 5 вершинами. Этот граф обозначается K_5;

б) двудольный неориентированный граф с 3 вершинами в первой доле и 3 вершинами во второй доле, причем каждая вершина первой доли соединена с каждой вершиной второй (такой граф называется *полным двудольным*). Этот граф обозначается $K_{3,3}$;

в) произвольный неориентированный граф, у которого степени всех вершин не меньше шести.

Решение. Все три пункта решаются похожим перебором случаев. Мы приведем полное решение для графа K_5, для остальных оно будет аналогичным.

Предположим, что граф K_5 удалось вложить в плоскость. Тогда выберем в нем какой-нибудь гамильтонов цикл и обозначим вершины в нем буквами A, B, C, D, E (в порядке следования по циклу).

Вершины A и C соединены ребром. Оно может идти либо внутри, либо вне пятиугольника — пока мы без ограничения общности можем считать, что оно идет внутри.

Заметим, что вершину B теперь можно единственным образом соединить с вершинами D и E так, чтобы не появилось пересечений. А после проведения ребер BD и BE мы видим, что ребра AD и CE теперь обязательно пересекутся либо друг с другом, либо с уже проведенными ребрами.

Существует и другой способ решения, использующий задачу 32. Заметим, что если граф K_5 вложен в плоскость, то все грани обязаны быть треугольниками. Посчитав число граней и ребер графа K_5 и сопоставив их с задачей 32а, приходим к противоречию. Аналогично, если двудольный граф $K_{3,3}$ вложен в плоскость, то все грани обязаны быть четырехугольниками и можно применить задачу 32б.

Определение 7. *Подграфом* данного графа называется граф, который получается из данного выкидыванием некоторых вершин и ребер (дуг).

Два неориентированных графа называются *гомеоморфными*, если один можно получить из другого следующими операциями: взять ребро и добавить посередине этого ребра вершину; взять вершину степени 2 и заменить ее и выходящие из нее ребра на одно ребро (заметим, что эти две операции взаимно обратны).

Задача 34* (теорема Понтрягина — Куратовского). Докажите, что неориентированный граф планарен тогда и только тогда, когда у него нет подграфа, гомеоморфного K_5 или $K_{3,3}$.

Последняя задача является очень сложной и одновременно очень замечательной. Красивое доказательство этого факта придумано Юрием Макарычевым (когда он был школьником 10 класса 57 школы). См.: А. Б. Скопенков, Вокруг критерия Куратовского планарности графов // Математическое просвещение. Сер. 3. Вып. 9 (2005).

Графики функций

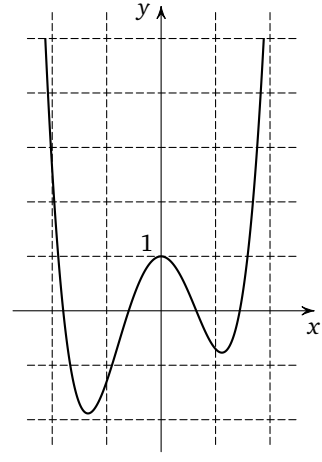
листок 13 / апрель 2005

В этом листке школьники учатся работать с графиками функций. Во-первых, они учатся считывать информацию с графика: находить значение в точке, решать графически уравнения $f(x)=c$ и $f(x)=g(x)$, находить промежутки возрастания и убывания функций. Область определения и область значений в этом листке не рассматриваются. Далее, школьники встречаются с разрывными функциями ($[x]$, $\{x\}$, $\operatorname{sign} x$) и их графиками, знакомятся с вертикальными и горизонтальными асимптотами. Кроме этого, в задаче 6 школьники знакомятся с преобразованиями графиков.

При этом обычно важно не столько поточечное приближение построенного графика к правильному, сколько различные качественные свойства строящегося графика (возрастание, убывание, пересечения с осями и т. д.).

Если у школьника не получается построить какой-то график, полезно построить этот график вместе с ним и дать ему решить аналогичную задачу.

Задача 1. Функция f задана графиком. Найдите $f(0)$ и $f(1)$, решите графически уравнения $f(x)=0$, $f(x)=1$ и $f(x)=x$; найдите все c, для которых уравнение $f(x)=c$ имеет ровно одно, ровно два и ровно три решения.



Ответ. $f(0)\approx 1$; $f(1)\approx -0{,}5$; $f(x)=0$ при $x\approx -1{,}8$; $-0{,}5$; $0{,}7$; $f(x)=x$ при $x\approx -1{,}5$; $-0{,}7$; $0{,}5$; $1{,}6$.

Уравнение $f(x)=c$ имеет ровно одно решение при $c=-1{,}9$, ровно два решения при $c\in(-1{,}9;\,-0{,}8)\cup(1;\,5)$ и ровно три — при $c\in\{-0{,}8;\,1\}$.

Определение 1. *Целой частью* числа x называется наибольшее целое число, не превосходящее x. Обозначение: $[x]$.

Определение 2. *Дробной частью* числа x называется число $\{x\}=x-[x]$.

Определение 3. $\operatorname{sign} x=\begin{cases}1, & \text{если } x>0;\\ 0, & \text{если } x=0;\\ -1, & \text{если } x<0.\end{cases}$

Задача 2. а) Найдите $[3{,}5]$, $[-2{,}2]$, $\{1{,}1\}$, $\{-2{,}7\}$, $[0]$, $\{0\}$, $[5]$, $\{5\}$, $\operatorname{sign}(5{,}6)$, $\operatorname{sign}(-2{,}4)$, $\operatorname{sign}(0)$.

б) Верно ли, что $\operatorname{sign} xy=\operatorname{sign} x\cdot\operatorname{sign} y$, $[xy]=[x][y]$, $\{xy\}=\{x\}\{y\}$?

в) Верно ли, что $\operatorname{sign}(x+y)=\operatorname{sign} x+\operatorname{sign} y$, $[x+y]=[x]+[y]$, $\{x+y\}=\{x\}+\{y\}$?

г) Докажите, что $x=|x|\cdot\operatorname{sign} x$, $x=[x]+\{x\}$.

Решение. а) $[3{,}5]=3$, $[-2{,}2]=-3$, $\{1{,}1\}=0{,}1$, $\{-2{,}7\}=0{,}3$, $[0]=0$, $\{0\}=0$, $[5]=5$, $\{5\}=0$, $\operatorname{sign}(5{,}6)=1$, $\operatorname{sign}(-2{,}4)=-1$, $\operatorname{sign}(0)=0$.

б) Первое утверждение верно и доказывается простым разбором случаев, а остальные ложны: $1=[0{,}8\cdot 1{,}5]\neq[0{,}8]\cdot[1{,}5]=0$ и $0{,}2=\{0{,}8\cdot 1{,}5\}\neq\{0{,}8\}\cdot\{1{,}5\}=0{,}4$.

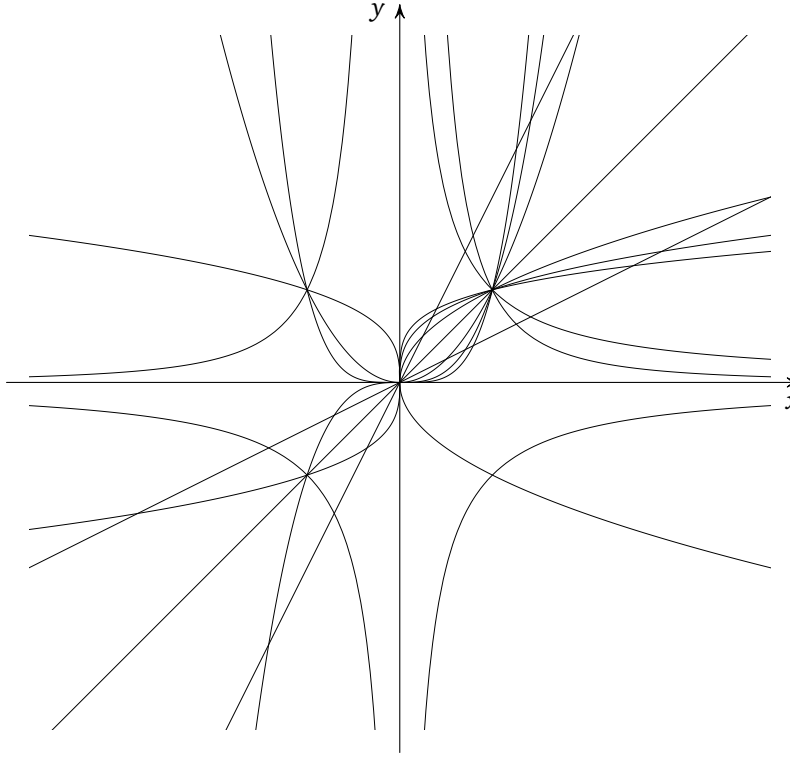
в) Все утверждения этого пункта ложны: $\operatorname{sign}(1+1)\neq\operatorname{sign}(1)+\operatorname{sign}(1)$, $[0{,}9+0{,}9]\neq[0{,}9]+[0{,}9]$, $\{0{,}9+0{,}9\}\neq\{0{,}9\}+\{0{,}9\}$.

г) Второе равенство получается из определения $\{x\}$ переносом $[x]$ в правую часть равенства. Докажем, что $x=|x|\cdot\operatorname{sign} x$. Действительно, при $x>0$ имеем $|x|=x$, $\operatorname{sign} x=1$, $|x|\cdot\operatorname{sign} x=x\cdot 1=x$, при $x<0$ имеем $|x|=-x$, $\operatorname{sign} x=-1$, $|x|\cdot\operatorname{sign} x=(-x)\cdot(-1)=x$, а при $x=0$ доказываемое равенство превращается в $0=0\cdot 0$.

Задача 3. Постройте графики функций $2x+3$, x^2, $1/x$, $[x]$, $\{x\}$, $\operatorname{sign} x$, $\dfrac{|x|}{x}$, $|x|$.

Решение. Для построения графика функции $\dfrac{|x|}{x}$ полезно заметить, что она равна $\operatorname{sign} x$ при $x\neq 0$ и не определена при $x=0$.

Задача 4. На рисунке обведите разными цветами графики функций $x/2$, x, $2x$, x^2, x^3, x^4, x^6, $\sqrt{x}$, $\sqrt[3]{x}$, $\sqrt[4]{x}$, $1/x$, $1/x^2$.



Решение. Сначала заметим, что среди данных функций три линейных: $x/2$, x и $2x$. Их графики легко выделить: это прямые, проходящие через точку 0. Между собой эти графики различаются углом наклона.

Теперь мысленно «сотрем» уже определенные графики. Заметим, что только у графиков функций $1/x$ и $1/x^2$ есть вертикальные асимптоты. Ветви этих функций при $x<0$ различаются по знаку ($1/x<0$, $1/x^2>0$). При $x>0$ обе функции положительны, причем при $0<x<1$ выполнено $1/x^2>1/x$, а при $x>1$ — $1/x>1/x^2$. Таким образом, графики этих функций также определяются. При этом оказывается, что одна из нарисованных гипербол (лежащая в IV квадранте) — лишняя.

Для определения остальных ветвей графиков достаточно заметить, что

при $x<-1$ выполнено $x^3<\sqrt[3]{x}<0<x^6<x^2$, а функции $\sqrt{x}$ и $\sqrt[4]{x}$ не определены;

при $-1<x<0$ выполнено $\sqrt[3]{x}<x^3<0<x^6<x^2$, а функции $\sqrt{x}$ и $\sqrt[4]{x}$ не определены;

при $0<x<1$ выполнено $0<x^6<x^4<x^3<x^2<\sqrt{x}<\sqrt[3]{x}<\sqrt[4]{x}$;

при $x>1$ выполнено $x^6>x^4>x^3>x^2>\sqrt{x}>\sqrt[3]{x}>\sqrt[4]{x}>0$.

Задача 5. Для указанных преподавателем функций f и g нарисуйте графики функций $f(x)+g(x)$, $f(x)\cdot g(x)$, $f(x)-g(x)$, $\sqrt{f(x)}$, $\frac{1}{f(x)}$.

Указание. Как обычно, можно отметить несколько «выделенных» точек, а потом соединить их плавной линией.

При построении всех этих графиков полезно понять, как ведет себя график вблизи точек разрыва одной из функций.

а) В точках, в которых одна из функций обращается в ноль, график суммы пересекается с графиком другого слагаемого.

б) Произведение обращается в ноль во всех точках, в которых хотя бы одна из функций обращается в ноль. При этом в остальных точках легко определить знак произведения.

в) Разность положительна или отрицательна в зависимости от того, расположен график функции f выше или ниже графика функции g, а точки пересечения графиков функций f и g соответствуют нулям разности.

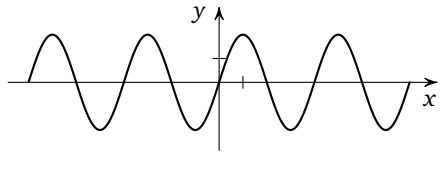
г) Функция $\sqrt{f(x)}$ определена только в точках, в которых $f(x)\geqslant 0$. При этом вблизи точек, в которых график функции $f(x)$ пересекает ось Ox, график функции $\sqrt{f(x)}$ ведет себя приблизительно как график функции $\sqrt{x}$, а вблизи точек касания графика функции f и оси Ox может вести себя по-разному: например, хотя графики функций x^2 и x^4 вблизи нуля сложно отличить «на глаз», графики их корней квадратных $|x|$ и x^2 уже отличаются очень сильно.

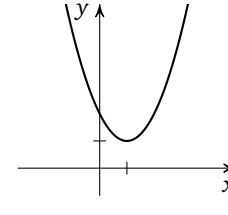
д) Нулям функции f соответствуют вертикальные асимптоты функции $\frac{1}{f(x)}$.

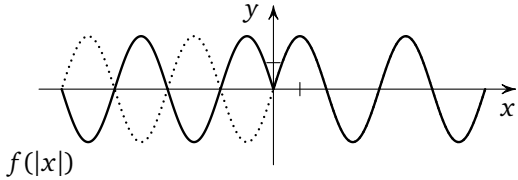
Задача 6. Нарисуйте графики функций

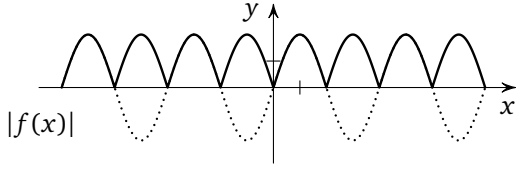
$f(|x|)$, $|f(x)|$, $f(x+1)$, $f(x-1)$, $f(x)+1$, $f(x)-1$, $f(2x)$, $3f(x)$, $f(x/3)$, $-f(x)$, $f(-x)$, $f([x])$, $f(\{x\})$, $[f(x)]$,

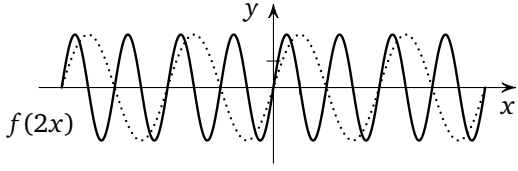
если график функции f изображен на рисунке.

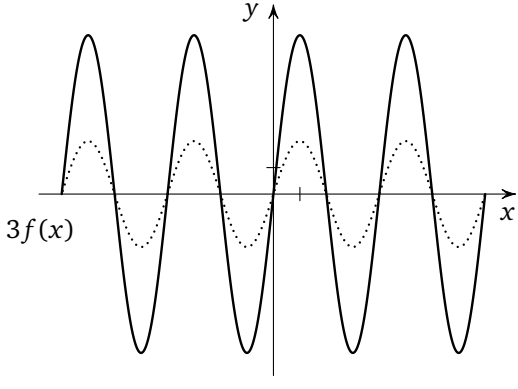


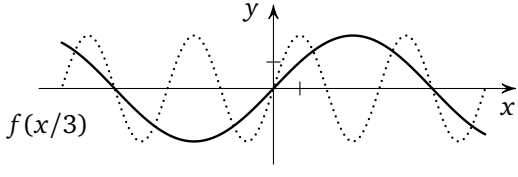


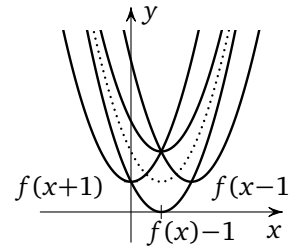


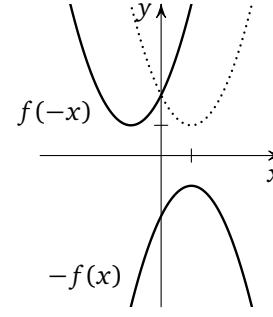


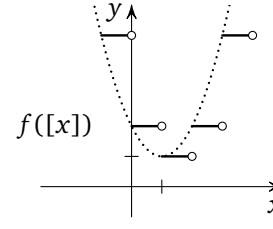


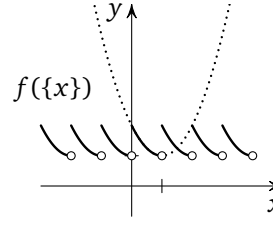


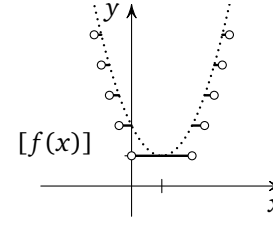












Вот некоторые из ответов к задаче 6.

Решение. График функции $f(|x|)$ получается следующим образом: часть графика, находящаяся слева от оси ординат, отбрасывается, а часть, находящаяся справа, отражается относительно этой оси (см. рисунок на следующей странице).

График функции $|f(x)|$ получается следующим образом: часть графика, находящаяся ниже оси абсцисс, отражается относительно этой оси, а часть, находящаяся сверху, не меняется.

График функции $f(x+a)$ получается из графика функции $f(x)$ параллельным переносом на a влево (соответственно, на $|a|$ вправо при отрицательных a).

График функции $f(ax)$ получается из графика функции $f(x)$ сжатием в a раз к оси ординат (если $a \geqslant 1$; растяжением в $1/a$ раз, если $0 < a < 1$; сжатием в $|a|$ раз и отражением относительно оси ординат, если $a \leqslant -1$; растяжением в $1/|a|$ раз и отражением относительно оси ординат, если $-1 < a < 0$).

График функции $af(x)$ получается из графика функции $f(x)$ растяжением в a раз от оси абсцисс (если $a \geqslant 1$; отражением относительно оси абсцисс и растяжением в $|a|$ раз, если $a \leqslant -1$ и т. д.).

Наконец, прежде чем рисовать последние три графика, полезно вспомнить, как выглядят графики функций $\{x\}$ и $[x]$.

Выполнение всех этих правил полезно проверить, вычислив значение функции в какой-нибудь точке. Кроме того, если школьник построил какой-нибудь график неправильно, ему полезно найти какую-нибудь конкретную точку, в которой значение построенной функции неправильно.

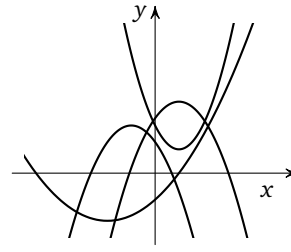
Задача 7. Нарисуйте графики функций
а) x^2+2x+3; б) $-2x^2+3x-1$; в) $x^2-2|x|+1$.

Решение. а) $x^2+2x+3=(x+1)^2+2$, поэтому можно взять график функции x^2 и сдвинуть его на 1 влево и на 2 вверх.

б) $-2x^2+3x-1=-2(x-0{,}75)^2+0{,}125$, поэтому можно взять график функции x^2, отразить относительно оси абсцисс, растянуть в два раза по вертикали, сдвинуть на 0,75 вправо и на 0,125 вверх.

в) $x^2-2|x|+1=(|x|-1)^2$, поэтому можно взять график функции x^2, сдвинуть его на 1 вправо и применить преобразование, переводящее график $f(x)$ в график $f(|x|)$.

Задача 8. На рисунке изображены графики квадратичных функций вида $y=ax^2+bx+c$. Найдите $\operatorname{sign} a$, $\operatorname{sign} b$ и $\operatorname{sign} c$ для каждой из этих функций.

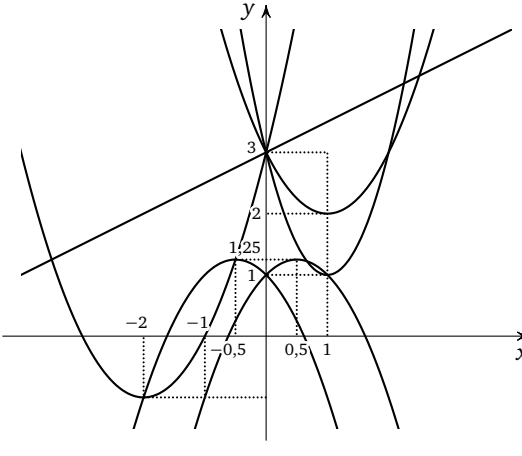


Решение. Опишем, как можно находить знаки коэффициентов квадратного трехчлена по его графику. Во-первых, знак коэффициента a отвечает за то, в какую сторону направлены ветви параболы: при $a>0$ ветви направлены вверх, а при $a<0$ — вниз.

Далее, $c=a\cdot 0^2+b\cdot 0+c$, то есть знак c можно определять по точке пересечения графика с осью ординат.

Осталось учесть, что абсцисса вершины параболы равна $-\frac{b}{2a}$, и найти знак коэффициента b.

Задача 9. На рисунке изображены графики функций x^2-2x+3, $2x^2-4x+3$, x^2+4x+3, $-x^2+x+1$, $x/2+3$. Определите, какой функции соответствует каждый из графиков.



Решение. Заметим сначала, что среди данных функций ровно одна линейная, а именно $x/2+3$. Ее графиком является единственная изображенная на рисунке прямая. Среди остальных квадратичных функций только функции x^2-2x+3 и $2x^2-4x+3$ не отличаются знаками коэффициентов. Следовательно, графики остальных функций можно определить, воспользовавшись предыдущей задачей, а

эти два графика различить по коэффициенту при x^2: ветви параболы $2x^2-4x+3$ «круче», чем ветви параболы x^2-2x+3.

Задача 10. На координатной плоскости изобразите множество точек (p, q), для которых уравнение $x^2+px+q=0$: а) не имеет корней; б) имеет ровно один корень; в) имеет два корня.

Решение. Как известно, уравнение $x^2+px+q=0$ не имеет корней при $p^2-4q<0$, имеет ровно один корень при $p^2-4q=0$ и имеет два корня при $p^2-4q>0$. Соответствующие множества точек плоскости изображены на рисунке.

Задача 11*. По изображенному преподавателем графику движения автобуса нарисуйте график скорости этого автобуса.

В этой задаче мы впервые наглядно знакомимся с понятием производной. При этом полезно подсказать школьнику, что скорость движения автобуса в некоторый момент времени — это угловой коэффициент касательной к графику его движения.

Как обсуждалось в начале листка, важно не столько поточечное приближение построенного графика к правильному, сколько понимание различных соотношений между качественными свойствами графика движения автобуса и графика его скорости. Рисуя график движения автобуса, полезно выделить несколько элементов, на которых наблюдаются такие соотношения. Перечислим несколько таких эффектов:

- если график движения автобуса на некотором промежутке постоянен, то скорость на этом промежутке равна нулю;
- если график движения линеен, то скорость постоянна;
- если функция движения автобуса возрастает (то есть автобус едет в положительном направлении), то скорость положительна, если убывает, то отрицательна, в максимумах и минимумах (соотетствующих развороту автобуса) — ноль;
- если график движения автобуса — выпуклый вверх, то скорость убывает, а если выпуклый вниз, то возрастает.

Кроме этих достаточно простых эффектов, есть несколько существенно более сложных. Например, можно «вклеить» в график движения автобуса график функции $y=x\sin\frac{1}{x}$.

Теория групп 2. Гомоморфизмы

листок 4д / май 2005

В последнем в 8 классе листке мы возвращаемся к теории групп. В двух первых разделах развиваются две возникшие в листке «Теории групп 1» темы: категория групп — обсуждаются гомоморфизмы групп, их ядра и образы; а также классы смежности — обсуждаются факторгруппы.

А в последней части обсуждаются действия групп на множествах, что позволяет отождествить (см. теорему Кэли) абстрактные группы с группами преобразований и открывает возможности для применения теории групп в других областях математики. В качестве примера в конце листка рассматривается применение леммы Бернсайда в комбинаторике.

1. Гомоморфизмы

Определение 1. Отображение $f\colon G\to H$ группы $(G,*)$ в группу $(H,\circ)$ называется *гомоморфизмом*, если для любых $a,b\in G$ выполнено равенство $f(a*b)=f(a)\circ f(b)$. Множество всех гомоморфизмов из G в H обозначается $\mathrm{Hom}(G,H)$.

Биективный гомоморфизм называется *изоморфизмом*. Изоморфизм на себя называется *автоморфизмом*. Множество всех автоморфизмов группы G обозначается $\mathrm{Aut}(G)$.

Группы G и H называются *изоморфными*, если между ними существует изоморфизм. Обозначение: $G\cong H$. Неформально говоря, изоморфными называются группы, отличающиеся «переобозначением элементов».

Задача 1. Докажите, что отношение «$G\cong H$» является отношением эквивалентности (формально говоря, это верно на любом множестве групп, но множества всех групп не существует).

Наименее тривиальная часть задачи — проверка того, что если f — изоморфизм G на H, то f^{-1} — изоморфизм H на G.

Задача 2. Какие из следующих отображений являются гомоморфизмами? А какие — изоморфизмами?

а) Тождественное отображение произвольной группы;
б) отображение произвольной группы в единицу;
в) $f\colon\mathbb{Z}\to\mathbb{Z}$, $f(n)=2n$; г) $f\colon\mathbb{Z}\to\mathbb{Z}$, $f(n)=n+1$;
д) $f\colon\mathbb{Z}\to\mathbb{Z}$, $f(n)=n^2$; е) $f\colon\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}/p\mathbb{Z}$, $f(n)=-n$;
ж) $f\colon(\mathbb{Z}/p\mathbb{Z})^\times\to(\mathbb{Z}/p\mathbb{Z})^\times$, $f(n)=n^{-1}$;
з) $f\colon(\mathbb{Z}/p\mathbb{Z})^\times\to(\mathbb{Z}/p\mathbb{Z})^\times$, $f(n)=n^{10}$;
и) $f\colon S_n\to S_n$, $f(x)=ax$; к) $f\colon S_n\to S_n$, $f(x)=x^{-1}$;
л) $f\colon S_n\to S_n$, $f(x)=axa^{-1}$; м) $\mathrm{sign}\colon S_n\to\mathbb{Z}/2\mathbb{Z}$.

Решение. а), б), в) Являются гомоморфизмами. Изоморфизмом является только гомоморфизм из пункта а), а также из пункта б) для единичной группы.

г) Не является гомоморфизмом: $f(0)+f(0)=2\neq 1=f(0+0)$.

д) Не является гомоморфизмом: $f(1)+f(1)=2\neq 4=f(1+1)$.

е) Является гомоморфизмом и даже изоморфизмом: равенство $-(a+b)=(-a)+(-b)$ выполняется для целых чисел, а значит остается верным и при приведение по модулю p.

ж) Является гомоморфизмом; вообще, взятие обратного $x\mapsto x^{-1}$ является автоморфизмом для любой абелевой группы (действительно, из $aba^{-1}b^{-1}=aa^{-1}bb^{-1}=e$ получаем, что $a^{-1}b^{-1}=(ab)^{-1}$.

Коммутативность существенна, так как в общем случае $(ab)^{-1}=$ $=b^{-1}a^{-1}$ (обратите внимание на порядок).

з) Является гомоморфизмом, но не изоморфизмом. Вообще, возведение в степень является эндоморфизмом (то есть гомоморфизмом *в себя*) для любой абелевой группы. Например, $(ab)^2=abab=aabb=$ $=a^2b^2$; отметим, что абелевость здесь существенна (контрпример в неабелевом случае дает группа подстановок). Доказательство общего случая удобно вести индукцией по степени.

и) Чтобы f было гомоморфизмом, необходимо (и достаточно), чтобы для произвольных $x, y\in S_n$ выполнялось $axay=axy$; умножая обе части на y^{-1} справа и на a^{-1} слева получаем $xa=x$, а значит, $a=e$. Тождественное отображение изоморфизмом, конечно, является.

к) Является гомоморфизмом только при $n=2$. Вообще, для произвольной группы $(ab)^{-1}=b^{-1}a^{-1}$ (действительно, $(b^{-1}a^{-1})(ab)=1$), поэтому (так как взятие обратного — биективная операция) взятие обратного является гомоморфизмом только для абелевых групп. В этом случае он будет изоморфизмом (так как сам является своим обратным).

л) Является гомоморфизмом (для произвольной группы). Действительно,

$$f(x)f(y)=(axa^{-1})(aya^{-1})=axya^{-1}=f(xy).$$

Этот гомоморфизм является изоморфизом, так как у него есть обратное — гомоморфизм $x\mapsto a^{-1}xa$.

Автоморфизмы такого вида называют *внутренними*. Внутренние автоморфизмы образуют подгруппу $\mathrm{Inn}(G)$ в группе всех автоморфизмов $\mathrm{Aut}(G)$ (см. задачу 5), причем имеется естественный сюръективный гомоморфизм $G\to\mathrm{Inn}(G)$.

м) Да, как было доказано листке «Подстановки 2». Изоморфизмом это отображение (при $n\neq 2$) не является.

Задача 3. Докажите, что для любого гомоморфизма $f: G \to H$
а) $f(e_G) = e_H$; б) $f(x^{-1}) = f(x)^{-1}$; в) $f(x^n) = f(x)^n$.

Решение. а) Заметим, что $f(e)f(e) = f(ee) = f(e)$. Но в группе $x^2 = x$ только для $x = e$ (чтобы убедиться в этом, домножим исходное равенство на x^{-1}).

б) Действительно, $f(x^{-1})f(x) = f(xx^{-1}) = f(e) = e$.

в) Доказательство индукцией по n. Проверим шаг:

$$f(x^{n+1}) = f(x^n x) = f(x^n)f(x) = f(x)^n f(x) = f(x)^{n+1}.$$

Задача 4. Пусть G — произвольная группа, а H — абелева группа. Введите структуру группы: а) на $\mathrm{Hom}(G, H)$, б) на $\mathrm{Aut}(G)$.

Ответ. а) $(fg)(x) = f(x)g(x)$;
б) $(fg)(x) = f(g(x))$.

Вопрос. Что является единицей? Обратным элементом? Почему ответ первого пункта не подходит для второго (и наоборот)? Подходит ли решение пункта а) для неабелевой группы H?

Задача 5. Найдите все гомоморфизмы:
а) $f: \mathbb{Z} \to \mathbb{Z}$; б) $f: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$; в) $f: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Указание. Каждый из этих гомоморфизмов полностью задается образом элемента 1.

Решение. См. решение задачи 7.

Задача 6. а) Найдите все подгруппы в $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$.
б) Докажите, что любая подгруппа группы $\mathbb{Z}/n\mathbb{Z}$ изоморфна группе вида $\mathbb{Z}/m\mathbb{Z}$.

Группа G, порожденная степенями одного элемента g, называется *циклической*. Любая группа вида $\mathbb{Z}/n\mathbb{Z}$ — циклическая; рассматривая гомоморфизм $\mathbb{Z} \to G$, $k \mapsto g^k$, нетрудно убедиться, что верно и обратное. (Подробнее: ядро этого гомоморфизма — подгруппа в $\mathbb{Z}$, порожденная некоторым числом n; тогда этот гомоморфизм задает изоморфизм между $\mathbb{Z}/n\mathbb{Z}$ и G.)

Решение пункта б) показывает, что любая подгруппа циклической группы — снова циклическая. (Не следует при этом думать, например, что произвольная подгруппа группы, порожденной двумя элементами, порождена двумя элементами.)

Решение. а) Все подгруппы $\mathbb{Z}/4\mathbb{Z}$ суть $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ и $\{0\}$. У $\mathbb{Z}/7\mathbb{Z}$ нет нетривиальных (то есть отличных от $\{0\}$ и $\mathbb{Z}/7\mathbb{Z}$) подгрупп. Решение можно получить несложным перебором. См. также следующий пункт.

б) Докажем, что произвольная подгруппа H в $\mathbb{Z}/n\mathbb{Z}$ порождена одним элементом. Рассмотрим в H минимальный по модулю ненулевой элемент x. Предположим, что в H имеется элемент y, не представимый в виде nx. Тогда (при помощи алгоритма Евклида) можно представить y в виде $nx+r$, где r — некоторый элемент H, меньший (по модулю), чем x. Полученное противоречие доказывает, что H — конечная группа, порожденная одним элементом, а значит, изоморфна $\mathbb{Z}/m\mathbb{Z}$.

> **Задача 7*.** Сколько существует гомоморфизмов из группы: а) $\mathbb{Z}$; б) $\mathbb{Z}/p\mathbb{Z}$ в группу G?

Указание. Куда может переходить элемент 1?

Ответ. а) $\mathrm{Hom}(\mathbb{Z}, G) = G$; б) $\mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, G) = {}_{(p)}G := \{x \in G : x^p = e\}$.

Решение. а) По задаче 3 любой гомоморфизм из $\mathbb{Z}$ задается образом единицы: $f(n) = f(1)^n$ (причем любое отображение единицы в G продолжается до гомоморфизма $\mathbb{Z} \to G$), а потому гомоморфизм $\mathrm{Hom}(\mathbb{Z}, G) \to G$, $f \mapsto f(1)$ является биекцией (а значит, и изоморфизмом групп).

б) Так же, как и в предыдущем пункте, каждый гомоморфизм из $\mathbb{Z}/p\mathbb{Z}$ полностью задается образом единицы. Однако $f(1)$ уже не может быть произвольным элементом G: так как (в $\mathbb{Z}/p\mathbb{Z}$) $p \cdot 1 = 0$, должно выполняться равенство $f(1)^p = e$. Это необходимое условие.

Убедимся, что оно является достаточным, то есть для любого $g \in {}_{(p)}G$ имеется гомоморфизм с $f(1) = g$. Действительно, по предыдущей задаче имеется $\tilde{f} \in \mathrm{Hom}(\mathbb{Z}, G)$ с $\tilde{f}(1) = g$, а так как $\tilde{f}(pn) = e$, этот гомоморфизм «спускается» на $\mathbb{Z}/p\mathbb{Z}$ ($\mathbb{Z}/p\mathbb{Z}$ есть множество классов эквивалентности целых чисел; $\tilde{f}$ принимает одинаковое значение на этих элементах этих классов.)

> **Задача 8.** Какие из следующих групп изоморфны: $\mathbb{Z}/2\mathbb{Z}$, $(\mathbb{Z}/3\mathbb{Z})^\times$, S_2, $\mathbb{Z}/6\mathbb{Z}$, S_3, $(\mathbb{Z}/7\mathbb{Z})^\times$?

Указание. Два самых наивных способа различить неизоморфные группы — это посмотреть на количества элементов в них и коммутативность.

Ответ. Все перечисленные группы делятся на три класса: S_3, $\mathbb{Z}/2\mathbb{Z} \cong$ $\cong (\mathbb{Z}/3\mathbb{Z})^\times \cong S_2$, $(\mathbb{Z}/7\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z}$.

Можно показать, что для любого простого p группа $(\mathbb{Z}/p\mathbb{Z})^\times$ является циклической (а значит, изоморфна $\mathbb{Z}/(p-1)\mathbb{Z}$). Доказательство основывается на том, что в противном случае существовало бы $n < p$,

такое что $x^{n-1}=1$ для любого $x\in(\mathbb{Z}/p\mathbb{Z})^\times$; однако это невозможно, так как $\mathbb{Z}/p\mathbb{Z}$ — *поле*, а в поле уравнение степени $n-1$ не может иметь более $n-1$ корня.

Определение 2. Множество $f(G)$ называется *образом* гомоморфизма $f\colon G\to H$. Обозначение: $\operatorname{Im} f$.

Множество $f^{-1}(e_H)$ называется *ядром* гомоморфизма $f\colon G\to H$. Обозначение: $\operatorname{Ker} f$.

Задача 9. Найдите ядра и образы всех гомоморфизмов задачи 2.

Ответ. а) $\operatorname{Ker} f=\{e\}$, $\operatorname{Im} f=G$;
б) $\operatorname{Ker} f=G$, $\operatorname{Im} f=\{e\}$;
в) $\operatorname{Ker} f=0$, $\operatorname{Im} f=2\mathbb{Z}$;
г), д) не гомоморфизмы;
е) $\operatorname{Ker} f=0$, $\operatorname{Im} f=\mathbb{Z}/p\mathbb{Z}$;
ж) $\operatorname{Ker} f=0$, $\operatorname{Im} f=\mathbb{Z}/p\mathbb{Z}^\times$;
з) *можно показать* (см. комментарий к задаче 8), что $(\mathbb{Z}/p\mathbb{Z})^\times\cong$ $\cong\mathbb{Z}/(p-1)\mathbb{Z}$, откуда нетрудно извлечь ответ:

$$\operatorname{Ker} f\cong\begin{cases}\mathbb{Z}/10\mathbb{Z}, & 10\mid p-1;\\ 0, & p=2;\\ \mathbb{Z}/2\mathbb{Z}, & 10\nmid p-1;\end{cases}\qquad \operatorname{Im}\cong\begin{cases}\mathbb{Z}/\frac{p-1}{10}\mathbb{Z}, & 10\mid p-1;\\ \mathbb{Z}/p\mathbb{Z}, & p=2;\\ \mathbb{Z}/\frac{p-1}{2}\mathbb{Z}, & 10\nmid p-1.\end{cases}$$

и) не гомоморфизм (при $a\neq e$);
к) при $n\neq 2$ не гомоморфизм, при $n=2$ $\operatorname{Ker} f=0$, $\operatorname{Im} f=S_n$;
л) $\operatorname{Ker} f=0$, $\operatorname{Im} f=S_n$;
м) $\operatorname{Ker} f=A_n$ (четные подстановки), $\operatorname{Im} f=\mathbb{Z}/2\mathbb{Z}$.

Задача 10. Докажите, что $\operatorname{Im} f$ и $\operatorname{Ker} f$ — подгруппы в H и G соответственно.

Решение. Если $h_1,h_2\in\operatorname{Im} f$, то $h_1=f(g_1)$, $h_2=f(g_2)$ для некоторых $g_1,g_2\in G$; тогда $h_1h_2=f(g_1g_2)\in\operatorname{Im} f$. Если $g_1,g_2\in\operatorname{Ker} f$, то $f(g_1)=e=$ $=f(g_2)$; тогда $f(g_1g_2)=f(g_1)f(g_2)=0$, а значит, $g_1g_2\in\operatorname{Ker} f$. Итак, $\operatorname{Ker} f$ и $\operatorname{Im} f$ замкнуты относительно умножения.

Пользуясь тем, что $f(g^{-1})=f(g)^{-1}$ (см. задачу 3), несложно проверить, что $\operatorname{Ker} f$ и $\operatorname{Im} f$ замкнуты и относительно операции взятия обратного.

Остается заметить, что, так как $f(e)=e$ (снова см. задачу 3), $\operatorname{Ker} f$ и $\operatorname{Im} f$ содержат единицу.

Задача 11. Докажите, что гомоморфизм $f\colon G\to H$ является изоморфизмом тогда и только тогда, когда $\operatorname{Im} f=H$, $\operatorname{Ker} f=\{e_G\}$.

Решение. Так как изоморфизм биективен, приведенное условие заведомо является необходимым.

Покажем, что оно является и достаточным. Так как $\operatorname{Im} f = H$, гомоморфизм f сюръективен. Достаточно теперь убедиться, что $\operatorname{Ker} f = \{e\}$ влечет инъективность f. Но действительно, $f(g_1) = f(g_2)$ влечет $f(g_1 g_2^{-1}) = e$, то есть $g_1 g_2^{-1} \in \operatorname{Ker} f$.

Замечание. Видно из решения и то, что гомоморфизм инъективен тогда и только тогда, когда он имеет тривиальное ядро.

> **Задача 12.** Придумайте гомоморфизм из группы $\mathbb{Z}$, ядром которого является подгруппа четных чисел.

Ответ. Приведение по модулю 2 (из $\mathbb{Z}$ в $\mathbb{Z}/2\mathbb{Z}$). Среди сюръекций ответ единственен.

2. Смежные классы

> **Задача 13.** Существует ли гомоморфизм из группы S_3, ядром которого является подгруппа $\{e, (12)\}$?

Ответ. Нет, не существует.

Указание. Рассмотрите перестановку вида $a(12)a^{-1}$, где a — какая-нибудь перестановка, отличная от (12).

Решение. Ядро любого гомоморфизма является *нормальной* подгруппой, то есть

$$\forall h \in \operatorname{Ker} f \ \forall g \in G \quad ghg^{-1} \in \operatorname{Ker} f.$$

Действительно, так как $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)ef(g)^{-1} = e$, $ghg^{-1} \in \operatorname{Ker} f$.

Можно показать, что любую нормальную подгруппу H можно представить как ядро подходящего отображения — например, проекции $G \to G/H$ (необходимые определения см. далее).

Осталось заметить, что $\{e, (12)\}$ нормальной подгруппой не является, так как в виде $a(12)a^{-1}$ можно представить любую транспозицию.

Вообще, *сопряжение* (см. задачу 23) в группе перестановок соответствует «замене координат» — переобозначению переставляемых элементов. См. также комментарий к задаче 7 в листке «Отношения эквивалентности».

Задача 14. Докажите, что для любого $a \in G$ и любого гомоморфизма $f\colon G \to H$ выполнено равенство $a(\operatorname{Ker} f) = (\operatorname{Ker} f)a$.

Решение. Поскольку условие $a(\operatorname{Ker} f) = (\operatorname{Ker} f)a$ равносильно тому, что $a(\operatorname{Ker} f)a^{-1} = \operatorname{Ker} f$, достаточно воспользоваться решением предыдущей задачи.

Задача 15. а) Докажите, что школьное правило

$$\text{четное} + \text{четное} = \text{нечетное} + \text{нечетное} = \text{четное},$$
$$\text{четное} + \text{нечетное} = \text{нечетное} + \text{четное} = \text{нечетное}$$

задает структуру группы на множестве $\{\{2n \mid n \in \mathbb{Z}\}, \{2n+1 \mid n \in \mathbb{Z}\}\}$.

б) Докажите, что аналогичное правило задает структуру группы на множестве $\{A_n, S_n \setminus A_n\}$.

Содержательная часть задачи заключается в том, что эта структура группы согласована со структурой исходной группы.

Определение 3. Напомним, что левым *смежным классом* элемента g группы G относительно подгруппы H называется множество gH. Множество всех левых смежных классов обозначают G/H.

Множество правых смежных классов группы G относительно подгруппы H (множеств вида Hg) обозначают $H\backslash G$. (Не следует путать фактор с разностью множеств.)

Определение 4. Подгруппа H группы G называется *нормальной*, если для любого элемента $a \in G$ выполнено $aH = Ha$ (или, что то же самое, $aHa^{-1} = H$). Обозначение: $H \triangleleft G$).

Другими словами, нормальной называется подгруппа, содержащая вместе с любым элементом все сопряженные к нему.

Задача 16. Докажите, что любая подгруппа коммутативной группы нормальна.

Решение. Действительно, $aH = Ha$ для произвольного элемента a и подмножества H коммутативной группы G.

Задача 17. Какие из подгрупп задачи 12 листка «Теория групп 1» нормальны?

Решение. По предыдущей задаче любая подгруппа коммутативной группы нормальна. Отсюда следуют решения пунктов а) и д).

Как было установлено при решении задачи 13, подгруппа из пункта в) не является нормальной.

Наконец, подгруппа из пункта б) нормальна, так как (см. решение задачи 13) является по задаче 15 ядром отображения $\operatorname{sign}\colon S_n \to \{\pm 1\}$.

Задача 18. Докажите, что подгруппа H группы G нормальна тогда и только тогда, когда разбиение группы G на левые смежные классы относительно группы H совпадает с разбиением на правые смежные классы.

Решение. Пусть H нормальна. Тогда $aH = Ha$ для каждого $a \in G$ и разбиения на правые и левые классы относительно H совпадают.

Пусть теперь, наоборот, разбиения на правые и левые классы относительно H совпадают. Но для произвольного $a \in G$ классы aH и Ha пересекаются (по элементу $ae = a = ea$), а значит (так как по предположению это классы эквивалентности относительно *одного и того же* отношения эквивалентности), они совпадают. Ввиду произвольности выбора a заключаем, что H нормальна.

Задача 19. Перечислите все нормальные подгруппы группы S_3.

Ответ. A_3 (а также $\{e\}$ и сама группа S_3).

Решение. Предположим, что нормальная подгруппа содержит какую-либо транспозицию. Тогда в силу нормальности она содержит и все сопряженные ей элементы, то есть все транспозиции (см. комментарий перед задачей 16). Но произведения транспозиций порождают всю группу S_n. Таким образом, собственная (то есть не совпадающая со всей группой) нормальная подгруппа не может содержать транспозиций, но тогда она либо совпадает с $\{e\}$, либо содержит цикл (а значит, и оба цикла, то есть совпадает с A_3).

Задача 20. Докажите, что любая подгруппа H группы G, для которой $2|H| = |G|$, нормальна.

Набросок решения. Из условия следует, что G/H состоит ровно из двух классов — H и $G\backslash H$.

Рассмотрим элемент $h \in H$. Ясно, что $Hh = H$. Так как умножение h на различные элементы дает различные результаты, $(G\backslash H)h = Gh\backslash Hh = G\backslash H$ (вообще, если отображение f переводит различные элементы в различные, то $f(A\backslash B) = f(A)\backslash f(B)$). Таким образом, умножение на элемент из H сохраняет класс элемента.

Пусть теперь $x \in G\backslash H$. Тогда по ранее доказанному $xH \subset H$, а так как по условию $|xH| = |G\backslash H|$, они совпадают. Наконец, (аналогично предыдущей части) $(G\backslash H)x = Gx\backslash Hx = G\backslash(G\backslash H) = H$.

Таким образом, сопряжение любым элементом сохраняет класс, и, в частности, H — нормальна.

Задача 21. Назовем произведением левых смежных классов aH и bH класс $(ab)H$.

а) Докажите, что это определение корректно тогда и только тогда, когда подгруппа H нормальна.

б) Докажите, что в этом случае множество левых смежных классов образует группу относительно введенной операции.

Решение. а) Корректность означает (проверьте), что при замене $a \to ah$, $b \to bh'$ класс $(ab)H$ сохраняется, то есть $ab \to abh''$. Получаем условие

$$\forall a, b \in G\ \forall h, h' \in H\ \exists h'' \in H\colon ahbh' = abh'',$$

которое равносильно (умножим на a^{-1} слева и h'^{-1} справа) условию

$$\forall b \in G\ \forall h \in H\ \exists h_1 \in H\colon hb = bh_1,$$

то есть условию нормальности H.

б) Заметим, что множество смежных классов есть множество классов эквивалентности (по некоторому *одному* — см. задачу 18 — отношению) на G. Но ясно, что если «индуцированное» умножение на классах эквивалентности на группе корректно, то выполнение всех аксиом группы для него следует из их выполнения для G.

Определение 5. Пусть H — нормальная подгруппа группы G. Группа, построенная в предыдущей задаче, называется *факторгруппой* (группы G по подгруппе H). Обозначение: G/H.

Задача 22. Докажите, что для любого гомоморфизма $f\colon G \to H$ выполнено $\operatorname{Im} f \cong G/\operatorname{Ker} f$ (в частности, $\operatorname{Ker} f$ — нормальная подгруппа G).

Решение. Действительно, f задает корректно определенный (так как $f(ak) = f(a)f(k) = f(a)$ для любых $a \in G$, $k \in \operatorname{Ker} f$) сюръективный гомоморфизм из $G/\operatorname{Ker} f$ в $\operatorname{Im} f$. Проверим, что он инъективен: $f(x) = f(y)$ влечет $xy^{-1} \in \operatorname{Ker} f$, то есть $\operatorname{Ker} f \cdot x = \operatorname{Ker} f \cdot y$.

Из этого рассуждения (и задачи 21) следует и нормальность ядра. Можно, впрочем, проверить это и непосредственно — см. решение задачи 13.

3. Действия

Определение 6. Гомоморфизм f группы G в группу преобразований множества A (т. е. биективных отображений множества A в себя) называется *действием* группы G на этом множестве. (Таким образом f ставит в соответствие каждому элементу g группы G некоторую биекцию множества A в себя.) Если понятно, о каком действии идет речь, элемент $f(g)(a)$ обозначается ga.

Альтернативное определение. Действием группы G на множестве X называется отображение $G \times X \to X$, $(g, x) \mapsto gx$, такое что $ex = x$ и $g(hx) = (gh)x$. Нетрудно убедиться, что эти определения эквивалентны. (Это проявление эквивалентности $\mathrm{Map}(X \times Y, Z)$ и $\mathrm{Map}(X, \mathrm{Map}(Y, Z))$.)

Последним из определений удобно пользоваться при проверке того, является ли нечто действием группы. Первое же позволяет применить развитую технику работы с гомоморфизмами, например, для перечисления всех действий группы на данном множестве (см. задачу 25).

Задача 23. Какие из следующих отображений являются действиями группы на себе?

а) $f(g)(x) = gx$ (*левый сдвиг*); б) $f(g)(x) = g^{-1}x$;
в) $f(g)(x) = xg$ (*правый сдвиг*); г) $f(g)(x) = xg^{-1}$;
д) $f(g)(x) = gxg^{-1}$ (действие сопряжениями).

Ответ. Отображения а), г) и д) являются действиями всегда, б) и в) — только для коммутативной группы.

Для произвольной группы G отображения б) и в) являются действиями группы G^{op}, совпадающей как множество с G, но имеющей другое умножение: $x \times_{G^{op}} y = y \times_G x$. Такие отображения называют иногда правыми действиями (а то, что называлось у нас просто действиями, — левыми действиями).

Указание. Удобнее проверять аксиомы из «альтернативного определения».

Задача 24 (теорема Кэли). Докажите, что любая конечная группа изоморфна некоторой подгруппе группы S_n.

Указание. Рассмотрите действие группы на себе.

Решение. Рассмотрим действие группы G на себе левыми сдвигами. Это некоторый гомоморфизм $\rho : G \to S_{|G|}$. Осталось проверить, что у него тривиальное ядро. Но $\mathrm{Ker}\,\rho = \{g \in G \mid \forall h \in G\, gh = h\} = \{e\}$.

Задача 25. Перечислите все действия:

а) группы $\mathbb{Z}$ на множестве из двух элементов (одного элемента);

б) группы $\mathbb{Z}/n\mathbb{Z}$ на множестве из двух элементов (одного элемента);

в) группы $\mathbb{Z}/n\mathbb{Z}$ на множестве из трех элементов;

г) группы $\mathbb{Z}/2\mathbb{Z}$ на группе $\mathbb{Z}$ (на группе $\mathbb{Z}/4\mathbb{Z}$), такие что каждое преобразование $f(g)$ является изоморфизмом;

д) группы $\mathbb{Z}/n\mathbb{Z}$ на множестве вершин квадрата, такие что каждое преобразование $f(g)$ является поворотом.

Указание. По определению любая задача о перечислении действий группы G сводится к задаче о нахождении гомоморфизмов из G (в некоторую группу). Но, так как нас интересует только случай циклической группы G, полный ответ дает задача 7.

Решение. а), б) Действие на одноэлементном множестве есть гомоморфизм в группу из одного элемента. Он единственен.

Нетривиальное действие на двуэлементном множестве есть нетривиальный, а значит, сюръективный гомоморфизм в группу $S_2 \cong \mathbb{Z}/2\mathbb{Z}$. Ядро такого отображения должно быть подгруппой индекса 2. В циклической группе такая подгруппа (если она существует) единственна. Для $\mathbb{Z}$ это $2\mathbb{Z}$, а для $\mathbb{Z}/n\mathbb{Z}$ — $2\mathbb{Z}/n\mathbb{Z}$ при четном n (а при нечетном n такой подгруппы не существует, так как индекс подгруппы является делителем порядка группы).

в) Нас интересуют гомоморфизмы группы $\mathbb{Z}/n\mathbb{Z}$ в S_3. Каким может быть образ такого гомоморфизма? Нетрудно перечислить (см. задачу 19) все подгруппы S_3: это S_3, $\{e\}$, A_3 и три изоморфные $\mathbb{Z}/2\mathbb{Z}$ подгруппы, состоящие из e и одной транспозиции.

Если образ нашего гомоморфизма есть $\{e\}$ или $\mathbb{Z}/2\mathbb{Z}$, то задача сводится к предыдущей. Так как гомоморфный образ коммутативной группы коммутативен, со всей группой S_3 образ совпадать не может.

Осталось разобрать случай, в котором действие является сюръекцией на $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. Аналогично предыдущему пункту получаем, что $3|n$, а действие заключается в том, что элемент 1 действует циклической перестановкой.

г) Нас интересуют гомоморфизмы из группы $\mathbb{Z}/2\mathbb{Z}$ в группы $\mathrm{Aut}(\mathbb{Z})$ и $\mathrm{Aut}(\mathbb{Z}/4\mathbb{Z})$. Найдем последние: при автоморфизме образующая циклической группы должна перейти в образующую. Образующие для $\mathbb{Z}$ исчерпываются ± 1, а $\mathbb{Z}/n\mathbb{Z}$ — элементами, взаимно простыми с n, то есть для $n = 4$ снова ± 1. Таким образом, $\mathrm{Aut}(\mathbb{Z}) = \mathrm{Aut}(\mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ (а нетривиальный элемент есть смена знака). Таким образом, $\mathbb{Z}/2\mathbb{Z}$ может действовать на обсуждаемых группах либо тривиально, либо сменой знака.

д) Группа поворотов квадрата есть (убедитесь в этом) $\mathbb{Z}/4\mathbb{Z}$. Таким образом, нас интересуют гомоморфизмы из $\mathbb{Z}/n\mathbb{Z}$ в $\mathbb{Z}/4\mathbb{Z}$. Каждый такой гомоморфизм полностью задается образом элемента 1, причем 1 может переходить только в элемент, аннулируемый умножением на n (см. задачу 7), то есть в 0 при $n = 2k+1$, 0 или 2 при $n = 4k+2$, а при $n = 4k$ — в любой.

Определение 7. Множество $Ga = \{ga \mid g \in G\}$ называется *орбитой* точки $a \in A$.

Определение 8. Орбиты действия сопряжениями называются *классами сопряженных элементов*.

Задача 26. Докажите, что отношение «точка a принадлежит орбите точки b» является отношением эквивалентности.

Решение. Рефлексивность: $a \in Ga$, так как $ea = a$. Симметричность: если $a \in Gb$, то $a = gb$; но тогда $g^{-1}a = g^{-1}gb = eb = b$, а значит, $b \in Ga$. Транзитивность: если $a \in Gb$, $b \in Gc$, то $a = gb$, $b = g'c$; значит, $a = (gg')c$.

Задача 27. а) Опишите орбиты для действий из задачи 25.
б) Опишите орбиты действия левыми сдвигами.
в) Найдите классы сопряженных элементов в S_3 и A_3.
г) Найдите классы сопряженных элементов в S_n.
д*) Найдите классы сопряженных элементов в A_n.

Решение. а) Единственной орбитой действия группы на одноэлементном множестве является все это множество. Вообще, при тривиальном действии (таком, что каждый элемент действует тождественным отображением) орбита каждой точки состоит из нее самой.

При нетривиальном действии на двуэлементом множестве имеется ровно одна орбита, совпадающая со всем множеством.

У нетривиального действия циклической группы на трехэлементном множестве одна орбита, если образующая действует циклом длины 3, и две орбиты (состоящие из 2 и 1 элемента), если образующая действует транспозицией.

Для нетривиального действия из задачи 25г орбиты имеют вид $\{n, -n\}$.

б) Единственной орбитой при действии группы на себе левыми сдвигами является вся группа. Орбитами при действии подгруппы на группе левыми сдвигами являются смежные классы относительно этой подгруппы.

в), г) Как было доказано в листке «Подстановки 2», в группе S_n сопряжены в точности элементы, имеющие одинаковую циклическую структуру.

Группа A_3 коммутативна, поэтому $ghg^{-1} = h$ и класс сопряженности каждого элемента состоит из него одного.

д) Ясно, что любые две сопряженные в A_n подстановки сопряжены в S_n, то есть имеют одинаковую циклическую структуру. Причем две имеющие одинаковую циклическую структуру четные подстановки

сопряжены в A_n, если и только если сопрягающую их подстановку можно выбрать четной. Заметим, что при этом класс из S_n разбивается не более чем на два класса — действительно, если a и b и b и c сопряжены нечетными подстановками x и y, то a и c сопряжены *четной* подстановкой xy.

Отсюда видно, что для четной подстановки a возможны два варианта: либо существует коммутирующая с ней нечетная подстановка x — тогда класс сопряженности a относительно S_n совпадает с классом сопряженности относительно A_n (действительно, если $yay^{-1}=b$ и подстановка y нечетная, то $(yx)a(yx)^{-1}=b$, причем yx — подстановка четная), либо такой подстановки не существует — тогда этот класс разбивается на два (рассмотрим $b=yay^{-1}$, где y — нечетна; если все же существует четная подстановка z, такая что $zaz^{-1}=b$, то $x=yz^{-1}$ — коммутирующая с a нечетная подстановка).

Осталось переформулировать эти случаи в терминах циклической структуры подстановки σ. Пусть сначала подстановка σ содержит цикл a четной длины. Тогда $\sigma a=a\sigma$, и реализуется первый случай. Пусть теперь она содержит два цикла равной нечетной длины: $(a_1, \ldots, a_k)$ и $(b_1, \ldots, b_k)$. Тогда σ коммутирует с $(a_1b_1)\ldots(a_kb_k)$, и опять реализуется первый случай. Доказательство того, что в остальных случаях подстановка не коммутирует ни с какой нечетной, оставляется читателю в качестве упражнения (следует использовать то, как действует сопряжение на подстановку, представленную в виде произведения независимых циклов).

Определение 9. Множество $\operatorname{stab} a=\{g\in G \mid ga=a\}$ (другое обозначение: G_a) называется *стабилизатором* точки $a\in A$.

Нетрудно видеть, что G_a является подгруппой в G.

Задача 28. Укажите стабилизаторы для действий из предыдущих задач.

Ответ. У действия левыми (или правыми) сдвигами стабилизатор любой точки тривиален (состоит из единицы группы).

Стабилизатор точки g при действии сопряжениями состоит из элементов группы, коммутирующих с g.

Для тривиального действия стабилизатор любого элемента совпадает со всей группой.

Вообще, стабилизатор элемента x при действии, соответствующем гомоморфизму $\varphi: G\to S_n$, есть $\varphi^{-1}(S_{n-1})$ (где $S_{n-1}\subset S_n$ — подгруппа, оставляющая x на месте).

Задача 29. Докажите, что $|G_x|\cdot|Gx|=|G|$.

В частности, отсюда следует, что размер любой орбиты делит порядок группы (если оба они конечны).

Решение. Заметим, что $|G| = \sum_{y \in Gx} |\{g \in G \mid gx = y\}|$. Докажем, что для каждой точки y в орбите точки x множество $\{g \in G \mid gx = y\}$ равномощно стабилизатору точки x. Действительно, рассмотрим какой-нибудь конкретный $y \in Gx$; по определению можно выбрать g_y так, что $g_y x = y$; тогда отображение $g \mapsto g_y^{-1} g$ задает биекцию между $\{g \in G \mid gx = y\}$ и G_x. Значит, $|G| = \sum_{y \in Gx} |G_x| = |G_x| \cdot |Gx|$.

Задача 30. Докажите, что в группе из p^2 элементов (p — простое число) найдется хотя бы два класса сопряженных элементов из одного элемента.

Указание. Один такой класс — класс единицы.

Решение. По предыдущей задаче каждый такой класс содержит либо один элемент, либо p элементов: действительно, его размер должен делить порядок группы, то есть p^2 (а совпадать с p^2 он не может, так как класс единицы состоит из нее одной).

Подсчитывая общее число элементов в группе, получаем $p^2 = n_0 + \ldots + n_1 p$, где n_i — количество классов из p^i элементов. Значит, n_0 делится на p, что (так как $n_0 \neq 0$) влечет $n_0 \geqslant 2$.

Определение 10. Множество $\operatorname{Fix} g = \{a \in A \mid ga = a\}$ (другое обозначение: A^g) называется *множеством неподвижных точек* элемента g (вообще говоря, это множество зависит от действия, но когда ясно, о каком действии идет речь, наименование действия не указывается).

Задача 31. Укажите множества неподвижных точек всех элементов для действий группы $\mathbb{Z}/4\mathbb{Z}$ а) левыми сдвигами; б) сопряжениями.

Решение. а) Для действия произвольной группы G на себе левыми сдвигами

$$G^g = \begin{cases} G, & g = e; \\ \{e\}, & g \neq e. \end{cases}$$

б) Так как $\mathbb{Z}/4\mathbb{Z}$ коммутативна, ее действие на себе сопряжениями тривиально, а $(\mathbb{Z}/4\mathbb{Z})^g = \mathbb{Z}/4\mathbb{Z}$ для любого g.

Задача 32. Укажите множества неподвижных точек всех элементов для действий группы S_3 а) левыми сдвигами; б) сопряжениями.

Решение. а) См. предыдущую задачу.

б) Заметим, что G^g для действия сопряжениями есть множество элементов, коммутирующих с g. Теперь нетрудно проверить, что

$$\operatorname{Fix}\sigma = \begin{cases} S_3, & \sigma = e; \\ A_3, & \sigma \in A_3 \backslash \{e\}; \\ \{e, \sigma\}, & \sigma \in S_3 \backslash A_3. \end{cases}$$

Задача 33 (лемма Бернсайда). Группа $|G|$ действует на множестве X. Докажите, что число орбит этого действия равно

$$\frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix} g|.$$

Указание. Перепишите сумму по элементам G в виде суммы по точкам X.

Решение. Пусть $G_x = \{g \in G \mid gx = x\}$ — *стабилизатор* точки x. Заметим, что

$$\sum_{g\in G}|\operatorname{Fix} g| = |\{(g,x) \in G\times X \mid gx = x\}| = \sum_{x\in X}|G_x|,$$

а следовательно (учитывая, что $|G_x|\cdot|Gx| = |G|$),

$$\frac{1}{|G|}\sum_{g\in G}|\operatorname{Fix} g| = \sum_{x\in X}\frac{|G_x|}{|G|} = \sum_{x\in X}\frac{1}{|Gx|} = \sum_{A\in X/G}\sum_{a\in A}\frac{1}{|A|} = \sum_{A\in X/G}1 = |X/G|.$$

Типичной задачей комбинаторики является подсчет количества классов эквивалентности. Нередко эти классы эквивалентности являются орбитами при действии какой-то группы. Для решения таких задач естественно (попытаться) применить методы теории групп. Иллюстрирует эту идею следующая задача.

Задача 34. а) Найдите число способов раскрасить n-местную карусель в красный и синий цвета.

б) Найдите число способов раскрасить ожерелье из n бусинок в красный и синий цвета.

Ответ. а) $\frac{1}{n}\sum\limits_{m=0}^{n-1}2^{(m,n)}$;

б) $\begin{cases} 2^l + \frac{1}{2n}\sum\limits_{m=0}^{n-1}2^{(m,n)}, & n = 2l+1; \\ 3\cdot 2^{l-1} + \frac{1}{2n}\sum\limits_{m=0}^{n-1}2^{(m,n)}, & n = 2l. \end{cases}$

Решение. а) Нас интересует число орбит при действии $\mathbb{Z}/n\mathbb{Z}$ (циклическими перестановками) на множестве раскрасок n-элементного множества. Воспользуемся леммой Бернсайда. Для этого для каждого числа m нам нужно найти $|\mathrm{Fix}\, m|$ — число раскрасок, переходящих в себя при циклическом сдвиге на m. При такой раскраске каждая орбита сдвигов на m должна быть покрашена одним цветом, а значит, $|\mathrm{Fix}\, m| = 2^{\text{число орбит}}$. Так как каждая из этих орбит состоит из $n/(m,n)$ элементов (это следует из того, что $am \equiv 0 \pmod n \Leftrightarrow a = (m,n)k$), всего их (m,n). Следовательно, $|\mathrm{Fix}\, m| = 2^{(m,n)}$ и по лемме Бернсайда искомое число способов есть $\frac{1}{n}\sum\limits_0^{n-1} 2^{(m,n)}$.

б) Этот пункт аналогичен предыдущему, но *группа симметрий* ожерелья больше $\mathbb{Z}/n\mathbb{Z}$ — это *группа диэдра* D_n. Ее можно определить как группу движений плоскости, сохраняющих правильный n-угольник. Нетрудно заметить, что она состоит из n поворотов (образующих нормальную подгруппу, изоморфную $\mathbb{Z}/n\mathbb{Z}$) и n симметрий.

Для поворотов $|\mathrm{Fix}\, g|$ вычислено в предыдущем пункте. Вычислим $|\mathrm{Fix}\, g|$ для симметрий. Если n нечетно, то ось симметрии проходит ровно через одну вершину (и $|\mathrm{Fix}\, g| = 2^{(n+1)/2}$); если же n четно, то для половины симметрий ось проходит через две вершины (и $|\mathrm{Fix}\, g| = 2^{(n+2)/2}$), а для другой половины — не проходит через вершины (и $|\mathrm{Fix}\, g| = 2^{n/2}$).

Отсюда получаем, что искомое число есть

$$\begin{cases} 2^l + \frac{1}{2n}\sum\limits_{m=0}^{n-1} 2^{(m,n)}, & n = 2l+1; \\ 3\cdot 2^{l-2} + \frac{1}{2n}\sum\limits_{m=0}^{n-1} 2^{(m,n)}, & n = 2l. \end{cases}$$

В книге использованы шрифты
гарнитуры ITC Charter.

Татьяна Игоревна Голенищева-Кутузова
Александр Дмитриевич Казанцев
Андрей Александрович Кустарёв
Юрий Георгиевич Кудряшов
Григорий Александрович Мерзон
Иван Валериевич Ященко

ЭЛЕМЕНТЫ МАТЕМАТИКИ В ЗАДАЧАХ
(с решениями и комментариями)
Часть 1

Технический редактор *В. Ю. Радионов*

Тираж 2000 экз. Заказ

Издательство Московского центра
непрерывного математического образования
119002, Москва, Большой Власьевский пер., 11
Тел. (499) 241-74-83

Отпечатано в ППП «Типография „Наука“»
121099, Москва, Шубинский пер., 6