OSNABRÜCKER SCHRIFTEN
ZUR MATHEMATIK

Reihe V Vorlesungsskripten

E Heft 7 Sommersemester 1997

ELEMENTARE ZAHLENTHEORIE

H. Spindler

Fachbereich Mathematik/Informatik
Universität Osnabrück

OSM Osnabrücker Schriften zur Mathematik

Herausgeber	Selbstverlag der Universität Osnabrück Fachbereich Mathematik/Informatik 49069 Osnabrück
Geschäftsführer	Prof. Dr. W. Bruns
Berater:	Prof. Dr. P. Brucker (Angew. Mathematik) Prof. Dr. E. Cohors-Fresenborg (Didaktik der Mathematik) Prof. Dr. V. Sperschneider (Informatik) Prof. Dr. R. Vogt (Reine Mathematik)
Druck	Hausdruckerei der Universität Osnabrück

Copyright bei den Autoren

Weitere Reihen der OSM:

Reihe D	Mathematisch-didaktische Manuskripte
Reihe I	Manuskripte der Informatik
Reihe M	Mathematische Manuskripte
Reihe P	Preprints
Reihe U	Materialien zum Mathematikunterricht

Elementare Zahlentheorie
Vorlesung
von

Heinz Spindler

Sommersemester 1997

Inhaltsverzeichnis

Vorwort

Dies ist die Ausarbeitung meiner vierstündigen Vorlesung über Zahlentheorie im Sommersemester 1997. Sie soll den Hörerinnen und Hörern die Nacharbeitung erleichtern.

Die Stoffauswahl entspricht ungefähr dem allgemein üblichen Stoff einführender Vorlesungen über Zahlentheorie, in denen keine besonderen Kenntnisse in Algebra vorausgesetzt werden.

Als triviale Anwendung des Eulerschen Satzes habe ich, wie es momentan Mode ist, das RSA public key crypto-system vorgestellt. p-adische Zahlen werden etwas ausführlicher behandelt. Insbesondere wird das Henselsche Lemma bewiesen.

Fast alle Themen der elementaren Zahlentheorie lassen sich mit Computeralgebra illustrieren. Deshalb wird parallel zum Stoff eine kleine, auf die Belange der Vorlesung beschränkte, Einführung in das Computeralgebrasystem ***Mathematica*** (Version 3.0) gegeben. Sie soll die Möglichkeit eröffnen, selbst die Geheimnisse der Welt der Zahlen experimentell zu erforschen oder auch nur Lehrsätze an konkreten Beispielen zu prüfen.

Das quadratische Reziprozitätsgesetz von Gauß fehlt natürlich nicht. Es werden zwei der vielen Beweise vorgestellt.

Im letzten Kapitel über algebraische Methoden wird etwas mehr Vertrautheit mit abstrakter Algebra (lineare Algebra, Polynome, Ideale, Restklassenringe) vorausgesetzt. Es werden die Anfangsgründe der Theorie der algebraischen Zahlkörper entwickelt. Algebraische Zahlkörper sind diejenigen Unterkörper des Körpers der komplexen Zahlen, die als $\mathbb{Q}$-Vektorraum endlich dimensional sind. Diese Körper sind von der Form $\mathbb{Q}[\alpha]$, wobei $\alpha \in \mathbb{C}$ eine algebraische Zahl ist (Satz vom primitiven Element).

Als Beispiel habe ich die reell-quadratischen Körper $\mathbb{Q}[\sqrt{d}]$, $d \equiv 1 \bmod 4$, $d \in \mathbb{N}_+$ quadratfrei, behandelt. Hier kommen unendliche Kettenbrüche und die Pellsche Gleichung ins Spiel. Schließlich werden Ideale eingeführt und die Verallgemeinerung des Hauptsatzes der elementaren Zahlentheorie auf die Ringe ganzer Zahlen in algebraischen Zahlkörpern bewiesen. Die Vorlesung schließt mit einer Behandlung der endlichen Körper. Jeder Abschnitt endet mit einer Liste von Übungsaufgaben, die zum Teil in den zweistündigen Übungen zur Vorlesung bearbeitet wurden.

Als Anhang gibt es ein ***Mathematica***-Notebook mit Programmen und Übungen zur Vorlesung. Wenn man ***Mathematica*** 3.0 nicht besitzt, kann man dieses Notebook mit dem von *Wolfram Research* kostenlos zu beziehenden Programm *MathReader* lesen.

Für die perfekte TEX-arbeit danke ich Frau Dünheuft sehr herzlich.

Heinz Spindler

Kapitel 1

Teilbarkeit

1.1 Der euklidische Algorithmus

Mit $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ bezeichnen wir den **Ring der ganzen Zahlen**. Weiter sei $\mathbb{N} = \{0, 1, 2, \dots\}$ die Menge der **natürlichen Zahlen** einschließlich der Zahl Null und $\mathbb{Z}_+ = \mathbb{N}_+ = \{1, 2, 3, \dots\}$ die Menge der positiven ganzen Zahlen. Für ganze Zahlen $a, b \in \mathbb{Z}$ gilt

$$a \leq b :\Longleftrightarrow \exists\, c \in \mathbb{N} : a + c = b \Longleftrightarrow b - a \in \mathbb{N}.$$

Es gelten die Regeln:

(1) $a \leq b \Longrightarrow a + c \leq b + c$ für alle $c \in \mathbb{Z}$

(2) $a \leq b \Longrightarrow ac \leq bc$ für alle $c \in \mathbb{N}$

Die Relation $\leq$ ist eine **Wohlordnung** auf $\mathbb{N}$, d.h. es gilt der **Satz vom kleinsten Element:**

> Jede nichtleere Teilmenge $M \subset \mathbb{N}$ besitzt ein kleinstes Element.

Hieraus kann man den Satz über die **vollständige Induktion** ableiten:

Satz 1.1.1 Ist $M \subset \mathbb{N}$ eine Teilmenge mit den Eigenschaften

$$\text{(a)} \quad 0 \in M, \qquad \text{(b)}\ \forall\, n \in \mathbb{N} : n \in M \Longrightarrow n + 1 \in M,$$

so gilt $M = \mathbb{N}$.

Beweis: Wir müssen zeigen, daß die Menge $N = \mathbb{N} \backslash M$ leer ist. Annahme: $N \neq \emptyset$. Nach dem Satz vom kleinsten Element existiert ein $n \in N$ mit $n \leq m$ für alle $m \in N$. Da $0 \in M$, ist $0 \notin N$, also $n > 0$, und somit ist $n - 1 \in \mathbb{N}$. Da $n - 1 < n$, ist $n - 1 \notin N$, d.h. $n - 1 \in M$. Nach (b) folgt jetzt $n = (n-1)+1 \in M$ im Widerspruch zu $n \in N$. $\square$

Satz 1.1.2 (Division mit Rest)
$\forall\, a, b \in \mathbb{Z},\ b > 0\, \exists!\ q \in \mathbb{Z},\ r \in \mathbb{Z}$, so daß

$$a = qb + r \text{ und } 0 \leq r < b.$$

Beweis:

(1) Existenz: Es sei

$$M := \{r \in \mathbb{N} \mid \exists\, q \in \mathbb{Z} : r = a - qb\} \subset \mathbb{N}.$$

Da $b > 0$, ist $b \geq 1$, also gilt für $q_0 := -|a| : q_0 b \leq q_0 1 \leq a$ und somit $a - q_0 b \geq 0$, also $a - q_0 b \in M$. Damit ist $M \neq \emptyset$, und es gibt ein kleinstes Element r in M. Es sei

$$r = a - qb.$$

Um zu sehen, daß $r < b$ gilt, untersuchen wir $r - b$. Es gilt $r - b = a - qb - b = a - (q+1)b$. Da aber $r - b < r$, muß wegen $r = \min M$ notwendigerweise $r - b < 0$ gelten, also $0 \leq r < b$.

(2) Eindeutigkeit: Es seien $q, q' \in \mathbb{Z},\ r, r' \in \mathbb{N}$ mit $0 \leq r < b,\ 0 \leq r' < b$ und $a = qb + r = q'b + r'$. Dann folgt $(q - q')b = r' - r$. Da nun $|r' - r| < b$, folgt $|q - q'| < 1$, also $|q - q'| = 0$, d.h. $q = q'$ und somit auch $r = r'$. □

Beispiel 1.1.3 In dem Computeralgebrasystem ***Mathematica*** (siehe [23]) gibt es die Funktionen

$$\text{Mod}[a, b] \ \text{ und } \ \text{Quotient}[a, b]$$

mit der Eigenschaft

$$a = \text{Quotient}[a, b]b + \text{Mod}[a, b].$$

$\text{Quotient}[a, b] \in \mathbb{Z}$ ist der ganze Anteil von a/b. a und b dürfen beliebige reelle Zahlen sein mit $b \neq 0$.
Man kann auch eine eigene Definition von $\text{Mod}[a, b]$ geben. Zur Unterscheidung heiße sie $\text{r}[a, b]$.
Die Definition erfolgt durch ein kleines Programm.

$$\begin{aligned} r[a\_, b\_] := \text{Module}[&\{r\},\\ &r = a; \text{While}[r >= b, r = r - b]; r] \end{aligned}$$

Hier wird innerhalb von Module [ ] eine lokale Variable r eingeführt durch die Zeile

$$\{r\},$$

Dann wird r der Startwert a zugewiesen:

$$r = a;$$

Solange $r \geq b$ ist, wird r um den Wert b vermindert:

$$\text{While}[r >= b,\ r = r - b];$$

am Schluß wird der Wert r angezeigt.
Allerdings ist dies sehr viel langsamer als die implementierte Funktion Mod. Ein Beispiel:

Mod[12345678, 3417]// Timing

und

r[12345678, 3417]// Timing

ergeben den Wert 57. Aber r[,] braucht zur Berechnung 1.01 Sekunden, während es Mod[,] in 0.00 Sekunden schafft.

Definition 1.1.4 Seien $a, b \in \mathbb{Z}$.

$$b \text{ teilt } a(\text{ in Zeichen: } b|a) :\Longleftrightarrow \exists\, q \in \mathbb{Z} : a = qb.$$

Dies gilt offensichtlich genau dann, wenn

$$\text{Mod}[a, b] = 0.$$

Man sagt dann auch:

"b ist **Teiler** von a" oder
"a ist **Vielfaches** von b".

Eine einfache Übung ergibt:

Lemma 1.1.5 $\forall\ a, b, c, \in \mathbb{Z}$ gilt:

(1) $a|a,\ a|-a,\ a|0,\ 1|a,\ -1|a$

(2) $0|a \Longleftrightarrow a = 0$

(3) $b|a$ und $a > 0 \Longrightarrow b \leq a$

(4) $a|b$ und $b|c \Longrightarrow a|c$

(5) $a|b \Longrightarrow a|bc$

(6) $a|b$ und $b|a \Longrightarrow a = \pm b$

(7) $a|b$ und $a|c \Longrightarrow\ \forall\ x, y \in \mathbb{Z} : a|bx + cy$

(8) $a|b \Longrightarrow ac|bc$ □

Aus (1), (4) und (6) folgt, daß die Teilerrelation "$a|b$" eine Ordnungsrelation auf $\mathbb{N}_+$ ist. Diese Relation ist aber keine lineare Ordnungsrelation: Sind $a, b \in \mathbb{N}_+$, so braucht weder $a|b$ noch $b|a$ zu gelten.
Eigenschaft (7) kann man auch allgemeiner aussprechen:

Lemma 1.1.6 Sind $a, b_1, \ldots, b_n, x_1, \ldots, x_n \in \mathbb{Z}$ und gilt $a|b_1, \ldots, a|b_n$, so gilt auch $a|\sum\limits_{k=1}^{n} b_k x_k$.

Beweis: $b_k = c_k a \Longrightarrow \sum\limits_{k=1}^{n} b_k x_k = \Big(\sum\limits_{k=1}^{n} c_k x_k\Big) a.$ □

Definition und Satz 1.1.7 Seien $a, b \in \mathbb{Z}$. Dann gilt: $\exists!\, d \in \mathbb{N}$, so daß gilt

(1) $d|a$ und $d|b$.

(2) Ist $c \in \mathbb{N}$ mit $c|a$ und $c|b$, so gilt $c|d$.

Diese Zahl d heißt der **größte gemeinsame Teiler** von a und b und wird mit $\mathrm{ggT}(a, b)$ oder kürzer mit (a, b) bezeichnet.

Beweis: Wir geben zwei Beweise. Der erste Beweis ist abstrakt.
1. Beweis:

a) Eindeutigkeit: Gelten (1) und (2) auch für $d' \in \mathbb{N}$, so folgt $d'|d$ und $d|d'$ und somit $d = d'$. □

b) Existenz: Es sei $M = \{ax + by | x, y \in \mathbb{Z}\}$.
Ist $M = \{0\}$, so ist $a = b = 0$ und $d = 0$ erfüllt (1) und (2).

Sei also $M \neq \{0\}$. Ist $c \in M$, so ist offensichtlich auch $-c \in M$ und somit folgt $M \cap \mathbb{N}_+ \neq \emptyset$.

Es sei d das kleinste Element von $M \cap \mathbb{N}_+$. Dann ist $d > 0$, und wir beweisen (1) und (2). Zu (1): Sei $a = qd + r$ mit $0 \leq r < d$. Dann ist $r = a - qd \in M$, denn: Ist $d = ax + by$, so ist auch r ganzzahlige Linearkombination von a und b:

$$r = a - q(ax + by) = a(1 - qx) - b(qy) \in M.$$

Aus der Minimalität von d folgt $r \leq 0$, also $r = 0$ und $a = qd$, d.h. $d|a$. Genauso folgt $d|b$. □

Zu (2): Ist c ein gemeinsamer Teiler von a und b, so ist c auch Teiler von $d = ax + by$. □

2. Beweis: (Euklidischer Algorithmus)
Wir betrachten folgendes ***Mathematica***-Programm:

```
ggT[a_, b_] :=
Module[{d, r},
d = r;
r = b;
While[r! = 0, {d, r} = {r, Mod[d, r]}];
d]
```

Es seien $a, b \in \mathbb{Z}$ und $b > 0$. Dann tut das Programm ggT$[a, b]$ folgendes: Zunächst setzt man

$$d_0 = a, \ r_0 = b$$

und führt Division mit Rest aus:

$$d_0 = q_1 r_0 + r_1, \ 0 \leq r_1 < r_0.$$

Ist $r_1 \neq 0$, so setzt man

$$\begin{aligned} d_1 &= r_0, \text{ und bildet} \\ d_1 &= q_2 r_1 + r_2 \text{ mit } 0 \leq r_2 < r_1. \end{aligned}$$

Ist $r_2 \neq 0$, so fährt man fort:

$$\begin{aligned} d_2 &:= r_1 \\ r_3 &:= \mathrm{Mod}(d_2, r_2), \text{ usw.} \end{aligned}$$

Da $\ldots < r_3 < r_2 < r_1 < r_0 = b$, wird nach k Schritten $r_{k+1} = 0$ gelten.
...
$d_{k-1} = r_{k-2}, \ d_{k-1} = q_k r_{k-1} + r_k, \ r_k > 0, \ d_k = r_{k-1}, \ d_k = q_{k+1} r_k, \ r_{k+1} = 0.$

$$d_{k+1} = r_k.$$

$d := d_{k+1}$ wird als Ergebnis ausgegeben.
Wegen $d_k = q_{k+1} r_k$ und $d = r_k$ gilt

$$d | d_k \text{ und } d | r_k.$$

Ist nun schon

$$d | d_i \text{ und } d | r_i$$

gezeigt für ein $i > 0$, so folgt aus

$$d_{i-1} = q_i r_{i-1} + r_i \text{ und } d_i = r_{i-1}$$

auch

$$d | d_{i-1} \text{ und } d | r_{i-1},$$

und somit folgt

$$d | d_0 \text{ und } d | r_0,$$

d.h.: d ist gemeinsamer Teiler von a und b.
Sei nun c ein beliebiger gemeinsamer Teiler von a und b. Dann gilt also

$$c | d_0 \text{ und } c | r_0.$$

Ist schon

$$c | d_i \text{ und } c | r_i \text{ für ein } i > 0$$

gezeigt und ist $r_i > 0$, so folgt aus

$$d_{i+1} = r_i \text{ auch } c|d_{i+1}$$

und aus

$$d_i = q_{i+1} r_i + r_{i+1}$$

(d.h. $r_{i+1} = d_i - q_{i+1} r_i$) auch

$$c|r_{i+1}.$$

Induktiv folgt somit $c|d$. Damit ist gezeigt, daß das Programm den größten gemeinsamen Teiler von a und b berechnet. □

Beispiel 1.1.8 Wir wollen die charakteristische Funktion der Relation "$a|b$" definieren.

$$\text{teilbar: } \mathbb{Z} \times \mathbb{Z} \longrightarrow \{\text{True}, \text{False}\}$$
$$\text{teilbar } [a\_, b\_] := \text{Mod}[a, b] == 0.$$

$\text{Mod}[a, b] == 0$ ergibt den Wert 'True', wenn b ein Teiler von a ist.

Wir geben ein weiteres ***Mathematica***-Programm zur Berechnung des größten gemeinsamen Teilers an, das die Funktion 'teilbar' verwendet. Zur Unterscheidung heiße es GGT:

```
GGT[0, a_] := a;
GGT[a_, 0] := a;
 GGT[a_, b_] :=
  Module[{c},
  c = Min[a, b];
  While[!(teilbar[a, c]&&teilbar[b, c]),
  c--];
  c]
```

In diesem Programm verkleinert man die Anfangszahl $c = \min(a, b)$ solange um 1 bis sie ein gemeinsamer Teiler von a und b wird. Zur Syntax:

$!A$ bedeutet die Negation der Aussage A.
$A\&\&B$ ist die Aussage "A und B".

Die Wahrheitstafeln sind:

A	B	A&& B
True	True	True
True	False	False
False	True	False
False	False	False

A	$!A$
True	False
False	True

c^{--} ist der Wert $c-1$ (decrement c).

Der größte gemeinsame Teiler ist durch folgende Regeln beschrieben, wie der 1. Beweis von Satz 1.1.7 zeigt:

$$\begin{aligned}(a,0) &= a\\ (a,b) &= (b,r),\end{aligned}$$

wobei $r = a - qb$ der Rest beim Teilen von a durch b ist. In ***Mathematica*** kann man diese Regeln programmieren. Dies führt uns zu folgendem regelbasierten Programm zur Berechnung des größten gemeinsamen Teilers. Zur Unterscheidung wählen wir die Bezeichnung $\mathrm{ggTr}[a,b]$.

$$\begin{aligned}\mathrm{ggTr}[a\_,0] &:= a\\ \mathrm{ggTr}[a\_,b\_] &:= \mathrm{ggTr}[b,\mathrm{Mod}[a,b]]\end{aligned}$$

Mit dem Befehl Trace kann man die Rechenschritte verfolgen. Ein Beispiel:

$$\begin{gathered}\mathrm{ggTr}[6,11] = 1\\ \mathrm{Trace}[\mathrm{ggTr}[6,11],\mathrm{ggTr}[\_\_\mathrm{Integer}]]\ //\mathrm{Table\ Form} =\\ \mathrm{ggTr}[17,11],\\ \mathrm{ggTr}[11,6],\\ \mathrm{ggTr}[6,5],\\ \mathrm{ggTr}[5,1],\\ \mathrm{ggTr}[1,0].\end{gathered}$$

Definition und Satz 1.1.9 Es sei $n \geq 1$ und $a_1, \ldots, a_n \in \mathbb{Z}$.

$$M = \{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in \mathbb{Z}\} \subset \mathbb{Z}$$

sei die Menge aller ganzzahligen Linearkombinationen von $a_1, \ldots, a_n$. Ist $M = \{0\}$, so sei $d := 0$. Ist $M \neq \{0\}$, so sei d die kleinste Zahl in $M \cap \mathbb{N}_+$. Dann gilt

(1) $d|a_1, \ldots, d|a_n$ und

(2) ist $c \in \mathbb{Z}$ mit $c|a_1, \ldots, c|a_n$, so gilt $c|d$.

Durch (1) und (2) ist $d \in \mathbb{N}$ eindeutig bestimmt. d heißt der **größte gemeinsame Teiler** von $a_1, \ldots, a_n$ und wird mit

$$\mathrm{ggT}(a_1, \ldots, a_n)$$

oder auch kurz mit $(a_1, \ldots, a_n)$ bezeichnet.

Beweis: wie 1.1.7 □

Bemerkung 1.1.10 In ***Mathematica*** ist der größte gemeinsame Teiler implementiert als

$$\mathrm{GCD}[a_1, \dots , a_n].$$

Beispiele: $\mathrm{GCD}[11, 88, 33, 550] = 11$, $\mathrm{GCD}[100/135] = \dfrac{20}{27}$.

Korollar 1.1.11 Seien $a_1, \dots , a_n \in \mathbb{Z}$, $d = (a_1, \dots , a_n)$.
Dann gilt

(1) $\exists\, x_1, \dots , x_n \in \mathbb{Z}$, so daß $d = a_1x_1 + \cdots + a_nx_n$.

(2) Ist c eine ganzzahlige Linearkombination von $a_1, \dots , a_n$, so ist c ein Vielfaches von d.

Beweis: Sei $M = \{a_1y_1 + \cdots + a_ny_n \mid y_1, \dots , y_n \in \mathbb{Z}\}$ und $d\mathbb{Z} = \{dm \mid m \in \mathbb{Z}\}$. Wir zeigen $M = d\mathbb{Z}$.

a)$M \subset d\mathbb{Z}$: Ist $y = a_1y_1 + \cdots + a_ny_n \in M$, so gilt $d|y$, weil $d|a_1, \dots , d|a_n$.

b)$d\mathbb{Z} \subset M$: Nach dem Beweis von 1.1.7 ist $d = 0$, falls $M = \{0\}$ und $d = \min(M \cap \mathbb{N}_+)$, falls $M \neq \{0\}$. Also ist $d \in M$ und somit $d = a_1x_1 + \cdots + a_nx_n$ für geeignete $x_1, \dots , x_n \in \mathbb{Z}$. Es folgt für alle $m \in \mathbb{Z}$:

$$dm = a_1(x_1m) + \cdots + a_n(x_nm) \in M$$

$\square$

Lemma 1.1.12 Seien $a, b, c \in \mathbb{Z}$. Dann gilt

(1) $(a, b) = (b, a)$, $(a, 0) = |a|$, $(a, b) = (a, -b)$

(2) $a|c$ und $b|c \Longrightarrow ab|c \cdot (a, b)$

(3) $a|b \Longleftrightarrow (a, b) = |a|$, $(a, 1) = 1$

(4) $(a, b) = d \Longrightarrow \frac{a}{d}, \frac{b}{d} \in \mathbb{Z}$ und $(\frac{a}{d}, \frac{b}{d}) = 1$

(5) $(ac, bc) = (a, b) \cdot |c|$

(6) $(a, b) = (a, b - ac)$

(7) $(a, c) = 1$ und $(b, c) = 1 \Longrightarrow (ab, c) = 1$

Beweis:

(1) trivial

(2) $c = am$, $c = bn$, $d = (a, b) = ax + by \Longrightarrow cd = cax + cby = bnax + amby = ab(nx + my) \Longrightarrow ab|cd$

(3) Sei $d = (a, b) = ax + by$. Es gilt also: $a|b \Longleftrightarrow a|d \Longleftrightarrow d = |a|$

(4) $d|a$ und $d|b \Longrightarrow \frac{a}{c}, \frac{b}{d} \in \mathbb{Z}$.
$d = ax + by \Longrightarrow 1 = \frac{a}{d}x + \frac{b}{d}y \Longrightarrow (\frac{a}{d}, \frac{b}{d}) = 1$.

(5) Da $d = (a,b) = \max\{m \in \mathbb{Z} | \, m|a \text{ und } m|b\}$, gilt
$d \cdot |c| = \max\{m \cdot |c| \mid m|a \text{ und } m|b|\} = \max\{n \mid n|(a|c|) \text{ und } n|(b|c|)\}$

(6) n ist $\mathbb{Z}$-Linearkombination von a und $b \Longleftrightarrow$
n ist $\mathbb{Z}$-Linearkombination von a und $b - ac$, denn:

$$\begin{aligned} n = ax + by &= ax + (b - ac)y + acy \\ &= a\underbrace{(x + cy)}_{\in \mathbb{Z}} + (b - ac)y. \end{aligned}$$

(7) $ax_0 + cy_0 = 1 = bx_1 + cy_1 \Longrightarrow 1 = (ax_0 + cy_0)(bx_1 + cy_1) =$
$ab(x_0x_1) + cy$ mit $y \in \mathbb{Z} \Longrightarrow (ab, c) = 1$. □

Definition 1.1.13

$$\begin{aligned} a \text{ und } b \text{ sind } \textbf{teilerfremd} &:\Longleftrightarrow (a,b) = 1 \\ a_1, \ldots, a_n \text{ sind } \textbf{teilerfremd} &:\Longleftrightarrow (a_1, \ldots, a_n) = 1 \\ a_1, \ldots, a_n \text{ sind } \textbf{paarweise teilerfremd:} &\Longleftrightarrow \end{aligned}$$

$$(a_i, a_j) = 1 \text{ für } i \neq j.$$

Trickreich ist folgendes einfache

Lemma 1.1.14 Seien $a, b, c \in \mathbb{Z}$. Dann gilt

$$a|bc \text{ und } (a,b) = 1 \Longrightarrow a|c.$$

Beweis: $a|bc \Longrightarrow \; \exists \; q \in \mathbb{Z} : bc = aq$.
$(a,b) = 1 \Longrightarrow \; \exists \; x, y \in \mathbb{Z} : 1 = ax + by$. Es folgt:

$$c = cax + cby = cax + aqy = a(cx + qy),$$

also $a|c$. □

Notation 1.1.15 Damit keine Verwechslungen mit dem größten gemeinsamen Teiler möglich sind, wollen wir hier – wie in ***Mathematica*** – Elemente von $\mathbb{Z}^n$ in der Form $\{x_1, \ldots, x_n\}$ schreiben, d.h. wir setzen geordnete n-Tupel in geschweifte Klammern. Diese Konvention soll nur in diesem Kapitel gelten.

Satz 1.1.16 (lineare diophantische Gleichungen)
Seien $a, b, n \in \mathbb{Z}$, und es sei $d = (a,b) > 0$.

(1) Die lineare Gleichung
$$ax + by = n$$
besitzt genau dann eine Lösung $\{x, y\} \in \mathbb{Z}^2$, wenn d ein Teiler von n ist.

(2) Ist $\{x_0, y_0\} \in \mathbb{Z}^2$ eine spezielle Lösung von

$$ax + by = n,$$

so ist $\{x, y\} \in \mathbb{Z}^2$ mit

$$\begin{aligned} x &= x_0 + t\frac{b}{d} \\ y &= y_0 - t\frac{a}{d},\ t \in \mathbb{Z}, \end{aligned}$$

die allgemeine Lösung von $ax + by = n$ in $\mathbb{Z}^2$.

Beweis:

(1) Sei $M = \{ax + by \mid x, y \in \mathbb{Z}\}$.
Nach Korollar 1.1.11 gilt $M = d\mathbb{Z}$. Also folgt: $ax + by = n$ ist in $\mathbb{Z}^2$ lösbar $\iff n \in M \iff d|n$. □

(2) Sei $L = \{\{x, y\} \in \mathbb{Z}^2 \mid ax + by = n\}$.
Ist $\{x_0, y_0\} \in L,\ t \in \mathbb{Z}$, so ist auch

$$\{x_0, y_0\} + t\left\{\frac{b}{d},\ -\frac{a}{d}\right\} \in L,$$

weil $a\frac{b}{d} + b(-\frac{a}{d}) = 0$ ist.

Ist umgekehrt $\{x_0, y_0\}, \{x, y\} \in L$, so gilt

$$(*) \qquad \frac{a}{d}(x - x_0) + \frac{b}{d}(y - y_0) = 0.$$

Also folgt $\frac{a}{d} \mid \frac{b}{d}(y - y_0)$. Da aber $(\frac{a}{d}, \frac{b}{d}) = 1$ ist, folgt aus Lemma 1.1.14

$$\frac{a}{d} \,\Big|\, y - y_0.$$

Es gibt somit ein $t \in \mathbb{Z}$, so daß

$$y = y_0 - t\frac{a}{d}.$$

Einsetzen in (*) ergibt

$$\frac{a}{d}(x - x_0) - t\frac{b}{d}\frac{a}{d} = 0,$$

also folgt $a = 0$ oder $x = x_0 + t\frac{b}{d}$.

In jedem Fall ist

$$\{x, y\} = \{x_0, y_0\} + t\left\{\frac{b}{d},\ -\frac{a}{d}\right\}.$$

□

Der sogenannte **erweiterte euklidische Algorithmus** ist ein Lösungsverfahren.
Gegeben seien $a, b, n \in \mathbb{Z}$, und es sei $a > b > 0$.
(Der Fall $a = 0$ oder $b = 0$ ist trivial.)
Der euklidische Algorithmus ergibt die Tabelle

$$a = r_0,\ b = r_1$$

$$\begin{array}{lcllcll}
r_0 & = & q_1 r_1 + r_2 & , & 0 < r_2 < r_1 & , & q_1 > 0 \\
r_1 & = & q_2 r_2 + r_3 & , & 0 < r_3 < r_2 & , & q_2 > 0 \\
\vdots & & & & & & \\
r_{k-2} & = & q_{k-1} r_{k-1} + r_k & , & 0 < r_k < r_{k-1} & , & q_{k-1} > 0 \\
r_{k-1} & = & q_k r_k & , & r_{k+1} = 0 & , & q_k > 0
\end{array}$$

$d = r_k = (a, b)$.
Eine Lösung $\{x, y\} \in \mathbb{Z}^2$ von $ax + by = d$ erhält man aus

$$\begin{array}{rclcl}
r_2 & = & r_0 & - & q_1 r_1 \\
r_3 & = & r_1 & - & q_2 r_2 \\
\vdots & & & & \\
d = r_k & = & r_{k-2} & - & q_{k-1} r_{k-1}
\end{array}$$

durch Einsetzen: Im ersten Schritt ergibt sich

$$r_3 = r_1 - q_2(r_0 - q_1 r_1) = -q_2 r_0 + (1 + q_1 q_2) r_1.$$

Im nächsten Schritt stellt man durch Einsetzen $r_4 = r_2 - q_3 r_3$ als Linearkombination von r_0 und r_1 dar, usw.
Wir betrachten ein Beispiel:

$$533x + 117y = 65$$

$a = 533,\ b = 117,\ n = 65$

$$\begin{aligned}
533 &= 4 \cdot 117 + 65 \\
117 &= 1 \cdot 65 + 52 \\
65 &= 1 \cdot 52 + 13 \\
52 &= 4 \cdot 13
\end{aligned}$$

$\Longrightarrow 13 = (533,\ 117)$

$$\begin{aligned}
65 &= 533 - 4 \cdot 117 \\
52 &= 117 - 1 \cdot 65 \\
13 &= 65 - 1 \cdot 52.
\end{aligned}$$

Also gilt $65 = 533 - 4 \cdot 117 \Longrightarrow$

$$\begin{aligned}
52 &= 117 - 1 \cdot 65 = 117 - 533 + 4 \cdot 117 = 5 \cdot 117 - 533 \\
\Longrightarrow 13 &= 65 - 1 \cdot 52 = 533 - 4 \cdot 117 - 5 \cdot 117 + 533 \\
&= 2 \cdot 533 - 9 \cdot 117.
\end{aligned}$$

Somit ist $\{2, -9\}$ Lösung von

$$533x + 117y = 13.$$

Da $65 = 5 \cdot 13$, ist $\{10,\ -45\}$ Lösung von

$$533x + 117y = 65$$

und die allgemeine Lösung ist $\left(\dfrac{117}{13} = 9,\ \dfrac{533}{13} = 41\right)$

$$\{x, y\} = \{10 + 9t,\ -45 - 41t\},\ t \in \mathbb{Z}.$$

Ein ***Mathematica***-Programm für den erweiterten euklidischen Algorithmus lautet folgendermaßen:

Beispiel 1.1.17

$$
\begin{aligned}
&\mathrm{erwggT}[a\_,\ b\_] := \\
&\qquad \mathrm{Module}[\{d, r, s, t, u, v\}, \\
&\qquad\qquad \{d, r, s, t, u, v\} = \{a, b, 1, 0, 0, 1\} \\
&\qquad \mathrm{While}[r! = 0, \\
&\qquad \{d, r, s, t, u, v\} = \\
&\qquad \{r, \mathrm{Mod}[d, r], u, v, s - \mathrm{Quotient}[d, r]u,\ t - \mathrm{Quotient}[d, r]v\}]; \\
&\qquad \{d, \{s, t\}\}]
\end{aligned}
$$

Wie funktioniert das Programm? Am Anfang ist

$$\{d, r, s, t, u, v\} = \{a, b, 1, 0, 0, 1\},$$

also

$$
\begin{aligned}
d &= as + bt, \\
r &= au + bv.
\end{aligned}
$$

Diese Gleichungen bleiben beim Programmdurchlauf invariant. Beweis: Es gelte

$$d = as + bt \text{ und } r = au + bv\ , \quad r \neq 0.$$

Für die neuen Werte d', r', s', t', u', v' gilt:

$$d' = r,\ r' = \mathrm{Mod}[d, r],\ s' = u,\ t' = v,\ u' = s - qu,\ v' = t - qv,$$

wobei $q := \mathrm{Quotient}[d, r]$. Da

$$\mathrm{Mod}[d, r] = d - qr,$$

folgt somit

$$
\begin{aligned}
d' &= r = au + bv = as' + bt' \text{ und} \\
r' &= d - qr = as + bt - q(au + bv) \\
&= a(s - qu) + b(t - qv) = au' + bv'.
\end{aligned}
$$

□

Da bei jedem Programmschritt der Wert von r kleiner wird aber stets ≥ 0 ist, wird nach endlich vielen Schritten $r = 0$ eintreten.

d ist dann der größte gemeinsame Teiler von a und b und $\{x, y\} = \{s, t\}$ ist Lösung der Gleichung

$$ax + by = d.$$

Der erweiterte euklidische Algorithmus ist in ***Mathematica*** implementiert als

$$\mathrm{ExtendedGCD}[a, b].$$

Definition 1.1.18 Seien $a_1, \ldots, a_n \in \mathbb{Z}\backslash\{0\},\ b \in \mathbb{Z}$.
b heißt **gemeinsames Vielfaches** von $a_1, \ldots, a_n$

$$\Longleftrightarrow \forall\ i = 1, \ldots, n : a_i | b \Longleftrightarrow b \in a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z}.$$

Mit $[a_1, \ldots, a_n]$ wird das kleinste positive gemeinsame Vielfache von $a_1, \ldots, a_n$ bezeichnet oder auch mit $\mathrm{kgV}(a_1, \ldots, a_n)$.

In ***Mathematica*** heißt die Funktion

$$\mathrm{LCM}[a_1, \ldots, a_n].$$

Lemma 1.1.19 Seien $a_1, \ldots, a_n \in \mathbb{Z}\backslash\{0\}$, und sei $h = [a_1, \ldots, a_n]$. Dann gilt

$$a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z} = h\mathbb{Z}.$$

Beweis: "$\subset$": Sei $b \in \bigcap\limits_{i=1}^{n} a_i\mathbb{Z}$. Dann gilt $b = a_i q_i,\ q_i \in \mathbb{Z}$, für $i = 1, \ldots, n$.

Es sei $b = qh + r$ mit $q \in \mathbb{Z}$ und $0 \leq r < h$. Weiter sei $h = a_i h_i,\ h_i \in \mathbb{Z}$. Dann gilt auch

$$r = b - qh = a_i q_i - q a_i h_i = a_i(q_i - q h_i);$$

also ist r gemeinsames Vielfaches von $a_1, \ldots, a_n$. Wegen der Minimalität von h und $0 \leq r < h$ muß $r = 0$ gelten.

"$\supset$" ist trivial. □

Lemma 1.1.20 Für $a_1, \ldots, a_n \in \mathbb{Z}\backslash\{0\},\ a, b \in \mathbb{N}_+$ gilt:

(1) $[ba_1, \ldots, ba_n] = b[a_1, \ldots, a_n]$

(2) $ab = [a, b](a, b)$

Beweis:

(1) Sei $h = [a_1, \ldots, a_n]$. Dann ist bh gemeinsames Vielfaches von $ba_1, \ldots, ba_n$ also $bh \geq h' := [ba_1, \ldots, ba_n]$. Es folgt weiter: $\frac{h'}{b} \in \mathbb{Z}$, und $\frac{h'}{b}$ ist gemeinsames Vielfaches von $a_1, \ldots, a_n$. Also ist $\frac{h'}{b} \geq h$, d.h. $h' \geq hb$ und somit $h' = hb$. □

(2) 1. Fall: $(a, b) = 1$. Es gilt $h = [a, b] \leq ab,\ h = am$ mit $m \in \mathbb{N}_+$. Da $b | am$ und $(a, b) = 1$, folgt nach Lemma 1.1.14 $b | m$, und somit folgt $ab | h$, weil $h = am$. Es folgt $ab \leq h$, also $ab = h$.

2. Fall: $(a, b) = d$ beliebig $\Longrightarrow$
$[a, b]\dfrac{1}{d} = \left[\dfrac{a}{d}, \dfrac{b}{d}\right] = \dfrac{a}{d} \cdot \dfrac{b}{d} \Longrightarrow [a, d]d = ab.$ □

Übungen 1.1.21

(1) Es sei $n \geq 3$ und $a_1, \dots, a_n \in \mathbb{Z}$. Beweise:

$$(a_1, \dots, a_n) = ((a_1, \dots, a_k), (a_{k+1}, \dots, a_n)) \text{ für } k = 1, \dots, n-1.$$

(2) Beweise: Für alle $n \in \mathbb{N}_+$ gilt

(a) $6 | n(n+1)(2n+1)$,

(b) $20 | n(n^2-1)(n^2-4)$

(3) Beweise: Ist $n \in \mathbb{N}_+$ gleichzeitig Quadrat- und Kubikzahl (wie $64 = 8^2 = 4^3$), so ist $\mathrm{Mod}(n, 7) \in \{0, 1\}$.

(4) Beweis: Eine Zahl $n \in \mathbb{N}$, $n > 1$, deren Dezimaldarstellung nur aus Einsen besteht, ist keine Quadratzahl. Hinweis: Untersuche $\mathrm{Mod}(n, 4)$.

(5) Beweise: Für alle $n \in \mathbb{N}_+$ gilt

a) $7 | 2^{3n} - 1$, b) $8 | 3^{2n} + 7$, c) $3 | 2^n + (-1)^{n+1}$

(6) Beweise:

(a) $(a, b) = 1$ und $c | a \Longrightarrow (b, c) = 1$

(b) $(a, b) = 1 \Longrightarrow (ac, b) = (c, b)$

(c) $(a, b) = 1$ und $c | a + b \Longrightarrow (a, c) = (b, c) = 1$

(7) Bestimme sämtliche Lösungen $\{x, y\} \in \mathbb{Z}^2$ der linearen diophantischen Gleichung

(a) $56x + 72y = 40$

(b) $24x + 138y = 18$

(c) $107360x + 30866y = 2684$

(8) (a) Es seien $a_1, \dots, a_n \in \mathbb{Z}$ mit $d = (a_1, \dots, a_n) > 0$, und es sei $m \in \mathbb{Z}$. Beweise: Die Gleichung

$$a_1 x_1 + \cdots + a_n x_n = m$$

ist genau dann in $\mathbb{Z}^n$ lösbar, wenn d ein Teiler von m ist.

(b) Bestimme sämtliche Lösungen $\{x, y, z\} \in \mathbb{Z}^3$ von $15x + 12y = 30z = 24$.

(9) Bestimme sämtliche Lösungen $\{x, y\} \in \mathbb{N}^2$ (also $x, y \geq 0$) von

(a) $30x + 70y = 300$

(b) $123x + 360y = 99$

(c) $54x + 21y = 906$

(10) Es seien $a, b \in \mathbb{N}_+$, $b > 1$. Beweise: Es gibt genau ein $n \geq 0$ und eindeutig bestimmte Zahlen $c_0, \ldots, c_n \in \mathbb{N}$, so daß

$$a = c_n b^n + c_{n-1} b^{n-1} + \cdots + c_1 b + c_0,\ 0 \leq c_i < b \text{ für } i = 0, \ldots, n \text{ und } c_n > 0.$$

(11) Es seien $a, b \in \mathbb{N}_+$ mit $(a, b) = 1$. Ist $n \geq (a-1)(b-1)$, so besitzt $ax + by = n$ eine Lösung $\{x, y\}$ in $\mathbb{N}^2$.

(12) (Für ***Mathematica***-Fans) Schreibe ein ***Mathematica***-Programm zur Lösung linearer diophantischer Gleichungen (vgl. Beispiel 1.16).

1.2 Primzahlen und eindeutige Primfaktorzerlegung

Definition 1.2.1 Es sei $p \in \mathbb{Z},\ p > 1$. p heißt **Primzahl** (auch **unzerlegbar, irreduzibel**) $\Longleftrightarrow$ Es gibt keine Teiler a von p mit $1 < a < p$.
Eine Zahl $a \in \mathbb{Z},\ |a| \geq 2$, heißt **zerlegbar**, wenn $|a|$ keine Primzahl ist.

Lemma 1.2.2 Es sei $p \in \mathbb{Z},\ p > 1$. p ist genau dann Primzahl, wenn gilt

$$(*) \qquad \text{Aus } \ p|ab \text{ folgt } p|a \text{ oder } p|b.$$

Beweis: "$\Longrightarrow$": Es sei p eine Primzahl.
Es gelte $p|ab$ aber $p \nmid a$ (p teilt nicht a). Da p nur die Teiler 1 und p in $\mathbb{N}$ besitzt, ist $(p, a) = 1$. Nach Lemma 1.1.14 folgt also $p|b$. "$\Longleftarrow$": Es gelte (*). Wäre nun p zerlegbar, so gäbe es $a, b > 1$ mit $p = ab$. Insbesondere gilt also $p|ab$. Nach (*) folgt $p|a$ oder $p|b$. Sei etwa $a = pq$. Dann folgt $p = ab = pqb$ also $qb = 1$ und somit $b = 1$. Widerspruch! □

Lemma 1.2.3 Es gilt

a) $\forall\ a \in \mathbb{N},\ a \geq 2\ \exists$ Primzahl p mit $p|a$.

b) Jede Zahl $a \in \mathbb{N},\ a \geq 2$, ist das Produkt endlich vieler Primzahlen.

Beweis: Zu a): $a \geq 2 \Longrightarrow M = \{b \in \mathbb{N} \mid b|a, b > 1\}$ ist nichtleer, weil $a \in M$. Nach dem Satz vom kleinsten Element gibt es ein kleinstes Element p von M. p kann natürlich außer 1 und p keine positiven Teiler besitzen, ist also eine Primzahl. □
zu b): Ist $a \geq 2$, so gibt es einen Primteiler p_1, also $a = p_1 a_1,\ 1 \leq a_1 < a$. Ist $a_1 \geq 2$, so besitzt auch a_1 einen Primteiler p_2, also $a = p_1 p_2 a_2,\ 1 \leq a_2 < a_1$.
Nach endlich vielen Schritten erhält man eine 'Primfaktorzerlegung'

$$a = p_1 p_2 \cdots p_k.$$

□

Hieraus folgt

Lemma 1.2.4 Es gibt unendlich viele Primzahlen.

Beweis: Seien $p_1, \ldots, p_n$ verschiedene Primzahlen. Nach 1.2.3 a) gibt es einen Primteiler p der Zahl $n := 1 + p_1 \cdot \ldots \cdot p_n$. Wäre nun $p = p_i$ für ein i, so wäre p Teiler von $p_1 \cdot \ldots \cdot p_n$ und somit auch (1.1.5 (7)) von $1 = n - p_1 \cdot \ldots \cdot p_n$, was natürlich nicht der Fall ist. Also ist p eine neue Primzahl. □

Satz 1.2.5 (Hauptsatz der elementaren Zahlentheorie)
Jede Zahl $n \in \mathbb{N}_+$ besitzt eine bis auf die Reihenfolge der Faktoren eindeutige Zerlegung

$$a = p_1 \cdot \ldots \cdot p_k \qquad (k \geq 0)$$

in ein Produkt von Primzahlen $p_1, \ldots, p_k$.

Beweis: Nach Lemma 1.2.3 ist nur noch die Eindeutigkeit zu beweisen. Seien

$$a = p_1 \cdot \ldots \cdot p_k = q_1 \cdot \ldots \cdot q_l$$

zwei Primfaktorzerlegungen.
Behauptung: Es gilt $k = l$, und es gibt eine Permutation $(\nu_1, \ldots, \nu_k)$ von $(1, \ldots, k)$, so daß

$$p_j = q_{\nu_j} \text{ für } j = 1, \ldots, k.$$

Der Beweis dieser Behauptung wird durch Induktion nach k geführt:
Ist $k = 0$, so ist $a = 1$ (leeres Produkt), also auch $l = 0$.
Induktionsschluß $k - 1 \longrightarrow k$:
Aus $p_1 \cdots p_k = q_1 \cdots q_l$ folgt

$$p_1 \mid q_1 \cdots q_l.$$

Nach Lemma 1.2.2 teilt p_1 einen der Faktoren, sagen wir q_{ν_1}. Da q_{ν_1} Primzahl ist, folgt $p_1 = q_{\nu_1}$. Ohne Einschränkung sei $\nu_1 = 1$. Es folgt also

$$p_2 \cdots p_k = q_2 \cdots p_l.$$

Nach Induktionsvoraussetzung gilt nach eventuellem Umnumerieren $p_i = q_i$ für $i = 2, \ldots, k$ und $k = l$. □

Definition 1.2.6 Jede Primzahl p definiert die p-adische Bewertung

$$v_p : \mathbb{Z}\backslash\{0\} \longrightarrow \mathbb{N}$$

mit

$$v_p(n) := \max\{\alpha \in \mathbb{N} \mid p^\alpha | a\}.$$

$v_p(n)$ heißt auch die **Vielfachheit von** p **in** a (oder auch der p-**Exponent** von a).

Jede Zahl $a \in \mathbb{N}, a \geq 2$, kann man eindeutig in folgender Form darstellen:
(*) $\qquad a = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$
wobei $\alpha_i \geq 1$, p_i Primzahl, $p_1 < p_2 < \ldots < p_k$. (*) heißt die **kanonische Primfaktorzerlegung** von a. $p_1, \ldots, p_k$ sind die **Primfaktoren** von a.

$$\alpha_i = v_{p_i}(a)$$

ist die Vielfachheit, mit der p_i auftritt. Offensichtlich bedeutet $v_p(a) = 0$ für eine Primzahl p, daß p kein Primfaktor von a ist.
Für die Formel (*) kann man auch schreiben

$$a = \prod_p p^{v_p(a)},$$

wobei das Produkt über alle Primzahlen p gebildet wird. Die Faktoren $p^{v_p(a)}$ sind nur für die Primfaktoren p von a ungleich 1.
Da es nicht einfach ist, die Primfaktorzerlegung einer Zahl wirklich zu bestimmen, ist das folgende Lemma nur von theoretischem Interesse.

Lemma 1.2.7 Seien $a, b \in \mathbb{N}_+$ und p Primzahl. Dann gilt

$$\begin{aligned} v_p([a,b]) &= \max(v_p(a), v_p(b)) \\ v_p(\mathrm{ggT}(a,b)) &= \min(v_p(a), v_p(b)) \\ v_p(ab) &= v_p(a) + v_p(b) \end{aligned}$$

Insbesondere gilt $(a, b) = 1$ genau dann, wenn a und b keinen gemeinsamen Primfaktor besitzen.

Beweis: Übung $\square$

Lemma 1.2.8 Seien $a_1, \dots, a_n \in \mathbb{N}_+$.
$a_1, \dots, a_n$ sind genau dann paarweise teilerfremd, wenn $[a_1, \dots, a_n] = a_1 \cdot \ldots \cdot a_n$ gilt.

Beweis: $v_p([a_1, \dots, a_n]) = v_p(a_1 \cdot \ldots \cdot a_n)$

$$\iff \max_i v_p(a_i) = \sum_i v_p(a_i) \iff \exists\ i_p\ \forall\ i \neq i_p : v_p(a_i) = 0$$

$$\iff \forall\ i \neq j : \min(v_p(a_i), v_p(a_j)) = 0.$$

$\square$

Die Eindeutigkeit der Primfaktorzerlegung ist nicht selbstverständlich. Dazu ein Beispiel: Die Teilmenge

$$N = \{4n + 1 \mid n \in \mathbb{N}\} = \{1, 5, 9, 13, 17, 21, \dots\}$$

ist abgeschlossen gegenüber der Multiplikation auf $\mathbb{N}$, denn $(4n + 1)(4m + 1) = 4(4nm + n + m) + 1$.
$(N, \cdot)$ ist ein sogenanntes **kommutatives Monoid**, d.h. die Multiplikation ist assoziativ und kommutativ, und es gibt ein Einselement.
Ist nun $a \in N,\ a > 1$, so ist die Menge

$$M := \{b \in N \mid b > 1 \text{ und } a = bq \text{ für ein } q \in N\}$$

nichtleer, weil $a \in N$; das minimale Element von M ist unzerlegbar in N. Wie im Beweis zu 1.2.3 folgt: Jedes Element $a \in N$ ist Produkt von unzerlegbaren Elementen. Es gibt sehr viele unzerlegbare Elemente in N. Die unterstrichenen Zahlen sind unzerlegbar in N:

$$\underline{5}, \underline{9}, \underline{13}, \underline{17}, \underline{21}, 25, \underline{29}, \underline{33}, \underline{37}, \underline{41}, 45, \underline{49}, \underline{53}.$$

Man erhält zum Beispiel zwei wesentlich verschiedene Zerlegungen von 441

$$441 = 21 \cdot 21 = 9 \cdot 49.$$

Den Begriff der Primzahl und der Unzerlegbarkeit kann man auch in beliebigen Integritätsbereichen einführen. Dabei heißt bekanntlich ein kommutativer Ring R

mit Einselement ein **Integritätsbereich**, wenn $0 \neq 1$ (also $R \neq \{0\}$) gilt und wenn die Kürzungsregel

$$ab = ac \text{ und } a \neq 0 \Longrightarrow b = c$$

gilt. Zahlentheoretisch interessante Beispiele sind die Unterringe des Körpers $\mathbb{C}$ der komplexen Zahlen.

Definition 1.2.9 Es sei R ein Integritätsbereich

(1) $e \in R$ heißt **Einheit** $\Longleftrightarrow$ $\exists\ e' \in R$, so daß $ee' = 1$. Die Einheiten von R bilden mit der Multiplikation als Verknüpfung eine abelsche Gruppe $R^\times$.

(2) $q \in R$ heißt **irreduzibel** $\Longleftrightarrow$
$q \neq 0,\ q \notin R^\times$, und es gilt:
Ist $q = ab$ mit $a, b \in R$, so ist a oder b eine Einheit in R.

(3) $p \in R$ heißt **Primelement** $\Longleftrightarrow$
$p \neq 0,\ p \notin R^\times$, und es gilt:
Sind $a, b \in R$ und gilt $p|ab$, so folgt $p|a$ oder $p|b$.

Nach Lemma 1.2.2 stimmen in $\mathbb{Z}$ die Begriffe 'Primelement' und 'irreduzibles Element' überein.

Die Einheitengruppe von $\mathbb{Z}$ ist $\mathbb{Z}^\times = \{\pm 1\}$, so daß jedes Element $n \in \mathbb{Z}\backslash\{0\}$ durch Multiplikation mit einer Einheit positiv wird. Deshalb beschränkt man sich in $\mathbb{Z}$ auf **positive** Primelemente, die Primzahlen. In einem beliebigen Integritätsbereich R werden zwei Primelemente p_1 und p_2 als nicht wesentlich verschieden angesehen, wenn $p_2 = ep_1$ mit einer Einheit $e \in R^\times$.

Man nennt dann p_1 und p_2 **assoziiert**.

Lemma 1.2.10 Sei R ein Integritätsring.
Ist p ein Primelement in R, so ist p auch irreduzibel.

Beweis: Sei $p = ab$ mit $a, b \in R$. Dann gilt insbesondere $p|ab$, also folgt $p|a$ oder $p|b$, etwa $a = pq$. Es folgt $p = pqb$, also $qb = 1$, d.h. $b \in R^\times$. □

Die Umkehrung dieser Aussage ist im allgemeinen falsch.

Wir geben dazu ein Beispiel:

Beispiel 1.2.11 Es sei $\alpha = \sqrt{d}\,i \in \mathbb{C}$, wobei $d \in \mathbb{N}_+$.
$R_d = \{a + b\alpha \mid a, b \in \mathbb{Z}\}$ ist ein Unterring von $\mathbb{C}$. Der Ring $R_1 = \mathbb{Z}[i]$ heißt der Ring der **ganzen Gaußschen Zahlen** (in ***Mathematica*** :GaussianIntegers). Wir betrachten hier nur $d \geq 2$.

1. Behauptung: $R_d^\times = \{\pm 1\}$ für $d \geq 2$.

Beweis: Ist $a + b\alpha$ Einheit in R_d, so gibt es ein $a' + b'\alpha \in R_d$, so daß

$(a + b\alpha)(a' + b'\alpha) = 1$. Also gilt dann

$$1 = |a + b\alpha|^2 \mid a' + b'\alpha|^2 = (a^2 + db^2)(a'^2 + db'^2).$$

Da $d \geq 2$ ist, folgt $b = 0$ und $a^2 = 1$. □

2. Behauptung: 2 ist irreduzibel in R_d falls $d \geq 3$.

Beweis: Aus $2 = (a + b\alpha)(a' + b'\alpha)$ folgt $4 = (a^2 + db^2)(a'^2 + db'^2)$. Ist $d \geq 3$, so folgt sofort $a + b\alpha = \pm 1$ oder $a' + b'\alpha = \pm 1$, d.h. 2 ist irreduzibel in R_d, $d \geq 3$. (In R_2 ist $2 = \alpha\bar{\alpha}$ natürlich nicht irreduzibel.)

3. Behauptung: 2 ist kein Primelement in R_d, falls d ungerade ist, $d \geq 3$.

Beweis: $(1 + \alpha)(1 - \alpha) = |1 + \alpha|^2 = 1 + d = 2 \cdot \frac{1+d}{2}$. Also ist 2 ein Teiler von $(1 + \alpha)(1 - \alpha)$; aber 2 ist weder Teiler von $1 + \alpha$ noch von $1 - \alpha$.

Im Ring R_d, d ungerade, $d \geq 3$, hat die Zahl $d + 1$ zwei wesentlich verschiedene Zerlegungen in irreduzible Elemente

$$d + 1 = 2 \cdot \frac{d+1}{2} = (1 + \alpha) \cdot (1 - \alpha).$$

In diesem Ring gilt also der Satz von der eindeutigen Primfaktorzerlegung nicht.

Ein Integritätsbereich R, in dem jedes Element $x \neq 0$, $x \notin R^\times$ eine bis auf Reihenfolge und Multiplikation mit Einheiten eindeutige Darstellung als Produkt von irreduziblen Elementen besitzt, heißt **faktorieller Ring**. Der Hauptsatz der elementaren Zahlentheorie sagt also:

$$\mathbb{Z} \text{ ist faktorieller Ring.}$$

Es gibt viele andere faktorielle Ringe. Ein wichtiges Beispiel ist der Polynomenring $K[x]$ der Polynome in einer Unbestimmten x mit Koeffizienten in einem Körper K (etwa $K = \mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$) (siehe [1] Kapitel 11).

Kehren wir zum Ring $\mathbb{Z}$ zurück.

Als eine Anwendung des Hauptsatzes der elementaren Zahlentheorie erwähnen wir

Satz 1.2.12 (Eulersche Produktdarstellung der Riemannschen Zetafunktion)
Für $s \in \mathbb{C}$ mit $\sigma = Re(s) > 1$ ist

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

absolut konvergent, und es gilt

$$\zeta(s) = \prod_{p \text{ Primzahl}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Beweis: $\displaystyle\sum_{n=1}^{\infty} |n^{-s}| = \sum_{n=1}^{\infty} n^{-\sigma} < \infty$ für $\sigma > 1$.

Also ist die Reihe absolut konvergent. Sei nun P die Menge aller Primzahlen. Wähle irgendeine aufsteigende Folge $P_1 \subset P_2 \subset \ldots$ von endlichen Teilmengen $P_k \subset P$ mit $P = \bigcup\limits_{k \geq 1} P_k$. Sei nun

$$N_k = \{n \in \mathbb{N}_+ \mid \text{ alle Primfaktoren von } n \text{ sind in } P_k\}.$$

Nach Satz 1.2.5 ist $\mathbb{N}_+ = \bigcup\limits_{k \geq 1} N_k$, und

$$\mathbb{N}^{P_k} \longrightarrow N_k,\ (\alpha_p)_{p \in P_k} \longmapsto n = \prod_{p \in P_k} p^{\alpha_p}$$

ist bijektiv.

Nach dem Umordnungssatz für absolut konvergente Reihen (siehe [7] Satz 7.8) ist nun

$$\zeta(s) = \lim_{k \to \infty} \sum_{n \in N_k} \frac{1}{n^s}$$

und weiter folgt aus der Bijektivität von $\mathbb{N}^{P_k} \longrightarrow N_k$

$$\begin{aligned}
\sum_{n \in N_k} \frac{1}{n^s} &= \sum_{\substack{(\alpha_p)_{p \in P_k} \\ \alpha_p \geq 0}} \prod_{p \in P_k} \frac{1}{p^{s\alpha_p}} \\
&= \prod_{p \in P_k} \left(\sum_{\alpha \geq 0} \frac{1}{p^{s\alpha}} \right) \\
&= \prod_{p \in P_k} \left(1 - \frac{1}{p^s} \right)^{-1}, \quad \text{also}
\end{aligned}$$

$$\zeta(s) = \lim_{k \to \infty} \prod_{p \in P_k} \left(1 - \frac{1}{p^s} \right)^{-1} = \prod_{p} \left(1 - \frac{1}{p^s} \right)^{-1}$$

$\square$

Bemerkung 1.2.13 Aus der Analysis ist bekannt, daß $\zeta(2) = \frac{\pi^2}{6}$ (siehe [7] Beispiel 21.8). Wir können dies und die Irrationalität von $\frac{\pi^2}{6}$ dazu benutzen, um einen weiteren Beweis für die Unendlichkeit der Menge der Primzahlen zu geben: Gäbe es nur endlich viele Primzahlen, so wäre das Eulersche Produkt $\prod\limits_{p}(1 - \frac{1}{p^2})^{-1}$ eine rationale Zahl!

$\zeta(s)$ ist die berühmte **Riemannsche Zetafunktion**. Sie ist zu einer meromorphen Funktion auf der komplexen Ebene $\mathbb{C}$ fortsetzbar. (In ***Mathematica*** : Zeta$[s] = \zeta(s)$.)

Ein uraltes Verfahren, alle Primzahlen unterhalb einer gegebenen Zahl zu finden, ist das **Sieb des Eratosthenes**.

In der Liste $\{2, 3, 4, 5, \dots\ n\}$ streicht man die Vielfachen $2k,\ k > 1$, von 2, dann die Vielfachen $3k,\ k \geq 3$, von 3. 5 ist die nächste noch nicht gestrichene Zahl. Man streicht dann die Vielfachen $5k,\ k \geq 5$, von 5 usw.

Ein ***Mathematica*** -Programm, das diese Arbeit verrichtet, lautet folgendermaßen:

```
eratosthenes [n_] :=
      Module [{ A = Range[2, n],  i = 1,  a = 2,
                  m = Quotient[n, 2]},
```

```
While[m >= a,
A = Complement[A, a Range[a, m]];
i++;
a = A[[i]];
m = Quotient[Last[A], a];];
A]
```

Dieses Programm funktioniert so:
Im ersten Schritt wird die Liste

$$A_1 = \{2, 3, \ldots, n\}$$

der Zahlen von 2 bis n betrachtet. A_1 wird durch den Befehl $A_1 = \mathrm{Range}[2, n]$ eingeführt. Es wird $a_1 = 2$ und $m_1 = [\frac{n}{2}] =$ ganzer Anteil von $\frac{n}{2}$ gesetzt. Ist $m_1 \geq a_1$, d.h. $n \geq 4$, so wird die Liste

$$a_1 \,\mathrm{Range}[a_1, m_1] = \{4, 6, \ldots, 2m_1\}$$

der Vielfachen ka_1 von a_1 bebildet, soweit sie relevant sind, d.h. für $k = a_1, \ldots, m_1$.
Man bildet dann

$$A_2 = A_1 \backslash a_1 \,\mathrm{Range}[a_1, m_1].$$

In A_2 fehlen die echten Vielfachen von 2.

$$A_2 = \{2, 3, 5, 7, 9, \ldots\}.$$

Nun erhöht man den Wert $i = 1$ um 1, also $i = 2$. Man wählt als neuen Multiplikator den zweiten Wert der Liste A_2 aus:

$$a_2 = A_2[[i]] = 3.$$

Man braucht die Vielfachen a_2k nur für $a_2 \leq k \leq [\mathrm{Last}[A_2]/a_2] = m_2$ zu betrachten. Dabei bedeutet $\mathrm{Last}[A_2]$ den letzten Wert in der Liste A_2. Nur wenn $m_2 \geq a_2$ gilt, ist noch etwas zu tun.
Man bildet

$$A_3 = A_2 \backslash a_2 \,\mathrm{Range}[a_2, m_2].$$

Nach endlich vielen Schritten enthält A_k nur noch Primzahlen. Offensichtlich werden weniger als $\sqrt{n}$ Schritte benötigt.
Für $n = 50$ ergibt sich folgender Ablauf:

i	A	a	m	$a\{a, \ldots, m\}$
1	$\{2, 3, \ldots, 50\}$	2	25	$\{4, 6, \ldots, 50\}$
2	$\{3, 5, 7, \ldots, 49\}$	3	16	$\{9, 12, 15, \ldots, 48\}$
3	$\{2, 3, 5, 7, 11, \ldots, 49\}$	5	9	$\{25, 30, \ldots, 45\}$
4	$\{2, 3, 5, 7, \ldots, 47, 49\}$	7	7	$\{49\}$
Ende	$\{2, 3, 5, 7, 11, \ldots, 47\}$	11	4	$\emptyset$, weil $a > m$

Für nicht zu große $n (n \leq 10^6)$ funktioniert das Programm ganz gut.

$$\pi(n) := \text{Length}[\text{eratosthenes}[n]]$$

ist die Anzahl der Primzahlen p mit $2 \leq p \leq n$. Ein wichtiges Ergebnis über die Verteilung der Primzahlen ist der berühmte **Primzahlsatz**

$$\lim_{x \to \infty} \pi(x) / \frac{x}{\log x} = 1,$$

d.h. für große x gilt annähernd

$$\pi(x) \approx \frac{x}{\log x}.$$

Die elegantesten Beweise unter den vielen Beweisen dieses Satzes benutzen Methoden der Funktionentheorie und die Eigenschaften der Riemannschen Zetafunktion.

Bemerkung 1.2.14

(1) Ein Paar von Primzahlen $\{p, q\}$ heißt **Primzahlzwilling**, wenn $q = p + 2$. Die ersten Beispiele sind

$$\{3, 5\},\ \{5, 7\},\ \{11, 13\},\ \{17, 19\}, \ldots$$

Ein riesiger Primzahlzwilling ist zum Beispiel

$$\{1691232 \cdot 1001 \cdot 10^{4020} \pm 1\},$$

was natürlich nicht einfach nachzuprüfen ist.

Der Primzahltest in ***Mathematica***

$$\text{Prime Q}[a] = \begin{cases} \text{True}, & \text{falls } a \text{ Primzahl} \\ \text{False}, & \text{sonst} \end{cases}$$

ist für so große Zahlen nicht anwendbar!

Die bisher ungelöste Vermutung ist, daß es unendlich viele Primzahlzwillinge gibt.

(2) Eine weitere ungelöste Vermutung ist die sogenannte **Goldbachsche Vermutung:** Jede gerade Zahl $n > 2$ ist die Summe zweier Primzahlen.

Einige Beispiele:

$$\begin{aligned}
10 \quad &= 3+7 &&= 5+5 \qquad \text{(2 Möglichkeiten)}\\
100 \quad &= 3+97 &&= 11+89 = 17+83 = 29+71\\
&= 41+59 &&= 47+53 \qquad \text{(6 Möglichkeiten)}\\
1000 \quad &= 3+997 &&= 17+983 = 23+977 = 29+971\\
&= 47+953 &&= 53+947 = 59+941\\
&= 71+929 &&= 89+911 = 113+887\\
&= 137+863 &&= 173+827 = 179+821\\
&= 191+809 &&= 227+773 = 239+761\\
&= 257+743 &&= 281+719 = 317+683\\
&= 347+653 &&= 353+647 = 359+641\\
&= 383+617 &&= 401+599 = 431+569\\
&= 443+557 &&= 479+521 = 491+509\\
& &&\text{(28 Möglichkeiten)}
\end{aligned}$$

Wir kommen zu einigen speziellen Primzahlen:

Lemma 1.2.15 Seien $a, n \in \mathbb{N},\ a, n \geq 2$.

(1) Ist n zerlegbar, so ist auch $a^n - 1$ zerlegbar.

(2) Ist $a \geq 3$, so ist $a^n - 1$ zerlegbar.

Beweis:

(1) Ist $n = mk$ mit $m, k \geq 2$, so ist

$$a^{mk} - 1 = (a^k - 1)(1 + a^k + a^{2k} + \cdots + a^{(m-1)k})$$

zerlegbar.

(2) Ist $a \geq 3$, so ist $a - 1 \geq 2$, also

$$a^n - 1 = (a - 1)(1 + a + \cdots + a^{n-1})$$

zerlegbar. □

Definition 1.2.16 Es sei p eine Primzahl.

$$M_p = 2^p - 1$$

heißt **Mersennesche Zahl** und Mersennesche Primzahl, falls M_p Primzahl ist.

Es ist unbekannt, ob es unendlich viele Mersennesche Primzahlen gibt. Die unvorstellbar große Zahl

$$2^{859433} - 1$$

ist die größte explizit bekannte Primzahl (Stand 1995).

Im Dezimalsystem ausgeschrieben würde diese Zahl ungefähr 60 Buchseiten füllen.

In ***Mathematica*** kann man leicht eine Tabelle der Mersenneschen Zahlen M_p nebst ihrer Primfaktorzerlegungen im Bereich $p \leq 67$ angeben.

$$M[n\_] := 2\text{^}\,\mathrm{Prime}[n] - 1$$

ist die n-te Mersennesche Zahl. Die gewünschte Tabelle erhält man durch

$$\mathrm{Table}\ \{\mathrm{Prime}[n],\ M[n],\ \mathrm{FactorInteger}\ [M[n]]\},\ \{n, 1, 19\}]\ //\mathrm{Table\ Form}$$

Nach dem Stand von 1995 ist $M_p = 2^p - 1$ für die folgenden Werte von p eine Primzahl:

2	61	2281	12701	859433
3	89	3217	23209	
5	107	4253	44497	
7	127	4423	86243	
13	521	9689	110503	
17	607	9941	132049	
19	1279	11213	216091	
31	2203	19937	756839	

Nähere Informationen findet man bei [15].

Lemma 1.2.17 Seien $a, n \in \mathbb{N}$, $a, n \geq 2$.

(1) Ist a ungerade, so ist $a^n + 1$ gerade, also keine Primzahl.

(2) Ist n keine Zweierpotenz, so ist $a^n + 1$ nicht prim.

Beweis:

(1) Ist $a = 2k + 1$, so ist

$$a^n + 1 = [(2k)^n + n(2k)^{n-1} + \cdots n(2k) + 1] + 1$$

gerade.

(2) Ist n keine Zweierpotenz, so hat n einen echten ungeraden Teiler; es gilt also $n = m(2k+1)$ mit $m \in \mathbb{N}$, $k > 0$. Es folgt:

$$a^n + 1 = a^{m(2k+1)} + 1 = (a^m + 1)(a^{m(2k)} - a^{m(2k-1)} \ldots - a^m + 1)$$

ist zerlegbar. □

Definition 1.2.18 $F_n := 2^{2^n} + 1$ heißt n-te **Fermatsche Zahl**.

Lemma 1.2.19 $(F_n, F_m) = 1$ für $n \neq m$.

Insbesondere treten unendlich viele Primzahlen als Primfaktoren in der Menge der Fermatschen Zahlen auf.

Beweis: Sei $a = 2^n$, $b = 2^m$, $n = m + k > m$.
$c = 2^k$, also $a = bc$. Es folgt

$$F_n - 2 = 2^a - 1 = 2^{bc} - 1 = (2^b + 1)(2^{b(c-1)} - 2^{b(c-2)} \ldots + 2^b - 1),$$

weil c gerade ist. $F_m = 2^b + 1$ ist also ein Teiler von $F_n - 2$ und somit gilt $(F_n, F_m) = (2, F_m) = 1$. $\square$

Beispiel 1.2.20 Euler hat gezeigt, daß die Primzahl 641 ein Teiler von F_5 ist. Das ist sehr trickreich:

$$\begin{aligned} 641 = 625 + 16 &= 25^2 + 4^2 = 5^4 + 2^4 \\ F_5 - 1 = 2^{32} &= 2^4 2^{28} = (641 - 5^4)2^{28} \\ &= 641 \cdot 2^{28} - (5 \cdot 2^7)^4 \\ &= 641 \cdot 2^{28} - (10 \cdot 2^6)^4 \\ &= 641 \cdot 2^{28} - 640^4 \\ &= 641 \cdot 2^{28} - (641 - 1)^4 \\ &= 641 \cdot (2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4) - 1 \end{aligned}$$

$$\Rightarrow F_5 = 641 \cdot (2^{28} - 641^3 + 4 \cdot 641^2 - 6 \cdot 641 + 4)$$

Ein berühmtes Theorem von Dirichlet besagt, daß für teilerfremde Zahlen a und b die Menge

$$\{an + b \mid n \in \mathbb{N}\}$$

unendlich viele Primzahlen enthält.

Der Beweis benutzt analytische Methoden und soll hier nicht geführt werden. Spezialfälle sind aber elementar. Ein Beispiel:

Lemma 1.2.21 Es gibt unendlich viele Primzahlen der Form $4n + 3$, $n \in \mathbb{N}$.

Beweis: Seien $q_1, \ldots, q_s$ Primzahlen von der Form $4n + 3$. Dann ist

$$N := 4q_1 \cdot \ldots \cdot q_s - 1 = 4(q_1 \cdot \ldots \cdot q_s - 1) + 3$$

ebenfalls von der Form $4n + 3$.

Seien $p_1, \ldots, p_t$ die Primfaktoren von N. Dann ist p_i von der Form $4n + 1$ oder $4n + 3$. Der Typ $4n + 3$ muß aber vorkommen, weil ein Produkt von Zahlen der Form $4n + 1$ ebenfalls von dieser Gestalt ist.

Es sei etwa $p_1 = 4n + 3$ für ein $n \in \mathbb{N}$. Da p_1 Teiler von N ist, ist $p_1 \neq q_i$ für alle $i = 1, \ldots, s$. $\square$

Lemma 1.2.22 Es sei $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ ein Polynom vom Grad $n > 0$ in der Unbestimmten x und Koeffizienten in $\mathbb{Z}$. Es sei

$$M = \{f(m) \mid m \in \mathbb{Z}\}.$$

Dann gilt

(1) $\{y \in M \mid y \text{ ist zerlegbar }\}$ ist unendlich

(2) $\{p \in \mathbb{N} \mid p \text{ Primzahl und } \exists\, y \in M : p|y\}$ ist unendlich.

Beweis:

(1) Nach der Binomischen Formel gilt

$$f(a+b) = f(a) + bg(a,b),$$

wobei $g \in \mathbb{Z}[x_1, x_2]$ ganzzahliges Polynom in zwei Veränderlichen ist.

Speziell gilt also

(*) $f(a + f(a)t) = f(a) + f(a)tg(a, f(a)t) = f(a)(1 + tg(a, f(a)t))$

für alle $a, t \in \mathbb{Z}$.

Wähle nun $a \in \mathbb{Z}$ so, daß $f(a) \notin \{0, 1, -1\}$. Dann ist $t \longmapsto a + f(a)t$ injektive Abbildung $\mathbb{Z} \longrightarrow \mathbb{Z}$ und somit ist (da ein Polynom vom Grad $n > 0$ höchstens n Nullstellen hat) die Menge

$$M' = \{f(a + f(a)t) \mid t \in \mathbb{Z}\} \setminus \{f(a), -f(a)\} \subset M$$

unendlich. Alle Elemente von M' sind nach (*) zerlegbar.

(2) 1. Fall: $a_0 = 0$. Dann gilt $p|f(p)$ für alle p.
2. Fall: $a_0 \neq 0$. Dann gilt für alle $m \in \mathbb{Z}$

$$f(a_0^2 m) = a_0(1 + a_0 a_1 m + a_0^3 a_2 m^2 + \dots)$$

m ist teilerfremd zu

$$\widetilde{f}(m) := 1 + a_0 a_1 m + a_0^3 a_2 m^2 + \dots$$

Sei nun p_i Primteiler von $f(m_i)$, $i = 1, \dots, s$. Sei dann $m := m' p_1 \cdot \ldots \cdot p_s$ so groß, daß $\widetilde{f}(m) \notin \{0, 1, -1\}$. p sei ein Primteiler von $\widetilde{f}(m)$. Dann ist p auch Teiler von $f(a_0^2 m)$, aber kein Teiler von m, also $p \neq p_1, \dots, p_s$. b) ist bewiesen.

□

Übungen 1.2.23

(1) Beweise: Es gibt unendlich viele Primzahlen von der Form $6n - 1$.

(2) Es sei $n! = 1 \cdot \ldots \cdot n$ für $n \in \mathbb{N}_+$ und $0! := 1$. Für $x \in \mathbb{R}$ sei $[x]$ die größte ganze Zahl n mit $n \leq x$. Beweise:
Für alle $n \in \mathbb{N}$ und für jede Primzahl p gilt

$$v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

(3) Für $k, n \in \mathbb{N}$, $k \leq n$ sei $\binom{n}{k} := \dfrac{n!}{k!(n-k)!}$.

(a) Zeige: $\binom{n}{k} \in \mathbb{N}_+$

(b) Es sei p eine Primzahl und $k \in \mathbb{N}_+$ mit $k < p$. Zeige $p | \binom{p}{k}$

(4) (a) Bestimme die größte Zahl $n \in \mathbb{N}$ mit

$$10^n \mid 1000000!$$

(b) Wie lautet die Primfaktorzerlegung des Produktes $1 \cdot 3 \cdot 5 \cdot \ldots \cdot 99$ der ersten 50 ungeraden Zahlen?

(5) Es sei $n \in \mathbb{N}_+$. Gibt es eine Zahl $a \in \mathbb{N}_+$, so daß alle Zahlen von a bis $a + n$ zerlegbar sind? Im Fall $n = 9$ bestimme gegebenenfalls das kleinstmögliche a.

(6) Ist $n \in \mathbb{N}$, $n \geq 2$, so ist $4^n + n^4$ keine Primzahl.

(7) Für $n \geq 2$ sei $S_n = \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$. Beweise: $S_n \notin \mathbb{Z}$.

(8) Zeige: $\forall\ x, y \in \mathbb{R} : [2x] + [2y] \geq [x] + [y] + [x + y]$. Folgere, daß

$$\frac{(2m)!(2n)!}{m!n!(m+n)!} \in \mathbb{Z}$$

(9) Es sei $u_0 = 0$, $u_1 = 1$ und $u_n = u_{n-1} + u_{u-2}$ für $n \geq 2$. Beweise: Für alle $n, m \in \mathbb{N}_+$ gilt

(a) $(u_n,\, u_{n+1}) = 1$

(b) $u_{n+m} = u_{n-1}u_m + u_n u_{m+1}$

(c) $d = (m, n) \Rightarrow (u_n, u_m) = d_d$

(d) Für $m > 2$ gilt: $u_m | u_n \Longleftrightarrow m | n$

(10) Seien α, β die Nullstellen von $x^2 - x - 1 = 0$, $\alpha > \beta$. Zeige: $u_n\sqrt{5} = \alpha^n - \beta^n$ für alle $n \in \mathbb{N}$.

(11) (a) Bestimme die Einheitengruppe $\mathbb{Z}[i]^\times$ im Ring der ganzen Gaußschen Zahlen.

(b) Beweise: Seien $\alpha, \beta \in \mathbb{Z}[i]$ und $\beta \neq 0$. Dann gibt es Elemente $\gamma, \rho \in \mathbb{Z}[i]$, so daß

$$\alpha = \gamma\beta + \rho \text{ mit } 0 \leq |\rho|^2 < |\beta|^2$$

(c) Beweise: Für $\alpha, \beta \in \mathbb{Z}[i]$ gibt es ein Element $\delta \in \mathbb{Z}[i]$ mit den Eigenschaften

(i) $\delta|\alpha$ und $\delta|\beta$, (ii) Ist $\gamma \in \mathbb{Z}[i]$ mit $\gamma|\alpha$ und $\gamma|\beta$, so gilt $\gamma|\delta$.

(Dabei heißt $\alpha|\beta$, daß $\beta = \gamma\alpha$ für ein $\gamma \in \mathbb{Z}[i]$.) δ ist bis auf Multiplikation mit Einheiten eindeutig bestimmt.

(d) Beweise: $\mathbb{Z}[i]$ ist ein faktorieller Ring.

(e) Finde die Primfaktorzerlegungen von 2,3,5,7 in $\mathbb{Z}[i]$.

(12) Für ***Mathematica*** -Fans

(a) Schreibe ein Programm, welches den n-ten Primzahlzwilling ermittelt.

(b) Schreibe ein Programm zur Primfaktorzerlegung.

1.3 Zahlentheoretische Funktionen

Definition 1.3.1 Sei R ein kommutativer Ring mit Eins.
Eine **zahlentheoretische Funktion** mit Werten in R ist eine Funktion

$$f : \mathbb{N}_+ \longrightarrow R.$$

$f : \mathbb{N}_+ \longrightarrow R$ heißt

(1) **multiplikativ** $\Longleftrightarrow \forall\, n, m \in \mathbb{N}_+$ mit $(n, m) = 1$ gilt $f(nm) = f(n)f(m)$

(2) **streng multiplikativ** $\Longleftrightarrow \forall\, n, m \in \mathbb{N}_+ : f(nm) = f(n)f(m)$

Lemma 1.3.2 Sei $f : \mathbb{N}_+ \longrightarrow R$ multiplikativ. Dann ist f durch die Werte $f(p^\alpha)$, p Primzahl, $\alpha \in \mathbb{N}$, festgelegt.

Beweis: Ist $n \in \mathbb{N}_+$ und $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ die Primfaktorzerlegung von n, so folgt induktiv wegen $(p_1^{\alpha_1} \dots p_{k-1}^{\alpha_{k-1}}, p_k^{\alpha_k}) = 1$

$$f(n) = f(p_1^{\alpha_1}) \cdot \ldots \cdot f(p_k^{\alpha_k}).$$

□

Beispiel 1.3.3 Es sei $R = \mathbb{Z}$.

(1) Sei $k \geq 0$; $f(n) = n^k$ ist vollständig multiplikativ, denn: $(nm)^k = n^k m^k$.

(2) Sei $k \geq 0$,

$$\sigma_k(n) := \sum_{d|n} d^k$$

heißt die k-te Teilerfunktion; speziell ist

$\sigma_0(n) = \tau(n) =$ Anzahl der Teiler von n.
$\sigma_1(n) = \sigma(n) =$ Summe der Teiler von n.

σ_k ist multiplikativ, wie gleich folgt.

Definition 1.3.4 Ist $f : \mathbb{N}_+ \longrightarrow R$ eine zahlentheoretische Funktion, so heißt

$$F : \mathbb{N}_+ \longrightarrow R \text{ mit } F(n) = \sum_{d|n} f(d)$$

die **summatorische Funktion** von f.

Satz 1.3.5 Ist f multiplikativ, so auch F.

Beweis: Sei $(m, n) = 1$. Ist d Teiler von mn, so gibt es eine eindeutig bestimmte Zerlegung $d = d_1 d_2$ mit $d_1|m$, $d_2|n$. Es folgt:

$$\begin{aligned}\sum_{d|mn} f(d) &= \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2) \\ &= \sum_{d|m} f(d) \sum_{d|n} f(d) = F(m)F(n).\end{aligned}$$

□

Korollar 1.3.6 σ_k ist multiplikativ, und für Primzahlpotenzen p^α gilt

$$\sigma_k(p^\alpha) = \sum_{\nu=0}^{\alpha} p^{k\nu}.$$

Beweis: σ_k ist die summatorische Funktion der multiplikativen Funktion $f(n) = n^k$. Nach 1.3.5 ist somit σ_k multiplikativ. Offensichtlich sind $1, p, \ldots, p^\alpha$ sämtliche Teiler von p^α. □

Satz 1.3.7

(1) Zu jeder Funktion $F : \mathbb{N}_+ \longrightarrow R$ gibt es genau eine Funktion $f : \mathbb{N}_+ \longrightarrow R$, so daß F die summatorische Funktion von f ist.

(2) Ist F multiplikativ, so auch f, und es gilt

$$f(n) = \prod_{i=1}^{k} (F(p_i^{\alpha_i}) - F(p_i^{\alpha_i - 1})),$$

wenn $n = \prod\limits_{i=1}^{k} p_i^{\alpha_i}$ die Primfaktorzerlegung von n ist.

Beweis:

(1) Durch Induktion nach n werden $f(1), \ldots, f(n)$ konstruiert.

a) $f(1) := F(1)$

b) Sind $f(1), \ldots, f(n-1)$ schon konstruiert, so daß $F(k) = \sum\limits_{d|k} f(d)$ für $k \leq n-1$, so setzt man

$$f(n) = F(n) - \sum_{\substack{d<n \\ d|n}} f(d).$$

□

(2) Sei F multiplikativ. Dann ist

$$F(p^\alpha) = \sum_{\nu=0}^{\alpha} f(p^\nu) = f(p^\alpha) + F(p^{\alpha-1}),$$

also

$$f(p^\alpha) = F(p^\alpha) - F(p^{\alpha-1}).$$

Für $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ setze nun

$$h(n) = \prod_{i=1}^{k} f(p^{\alpha_i}).$$

Dann ist h multiplikativ. Die summatorische Funktion H von h ist also auch multiplikativ. Da $H(p^\alpha) = \sum\limits_{\nu=0}^{\alpha} h(p^\nu) = \sum\limits_{\nu=0}^{\alpha} f(p^\nu) = F(p^\alpha)$, folgt $H = F$ und nach (1) gilt somit $h = f$, also ist f multiplikativ. □

Definition 1.3.8 Es sei $\varepsilon : \mathbb{N}_+ \longrightarrow R$ die Funktion

$$\varepsilon(n) := \begin{cases} 1 & \text{falls } n = 1 \\ 0 & \text{falls } n > 1, \end{cases}$$

und $\mu : \mathbb{N}_+ \longrightarrow R$ sei die Funktion mit ε als summatorischer Funktion. μ heißt die **Möbius-Funktion**.

Da ε multiplikativ ist, ist es auch μ und nach 1.3.7 (1) gilt für $n = \prod_{i=1}^{k} p_i^{\alpha_i}$

$$\mu(n) = \prod_{i=1}^{k} \left(\varepsilon(p^{\alpha_i}) - \varepsilon(p^{\alpha_i - 1})\right) = \begin{cases} 0 & \text{falls ein } \alpha_i \geq 2 \\ (-1)^k, & \text{falls } \alpha_1 = \ldots = \alpha_k = 1 \end{cases}$$

Es gilt also $\mu(n) \in \{-1, 0, 1\}$ und $\mu(n) \neq 0$ genau dann, wenn n **quadratfrei** ist, also n keine Quadratzahlen als Teiler besitzt.
Dann ist

$$\mu(n) = (-1)^{\text{Anzahl der Primfaktoren}}$$

Satz 1.3.9 (Möbiussche Umkehrformel)
Sei $f : \mathbb{N}_+ \longrightarrow R$ Funktion, $F : \mathbb{N}_+ \longrightarrow R$ ihre summatorische Funktion. Dann gilt

$$f(n) = \sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) = \sum_{d|n} F\left(\frac{n}{d}\right)\mu(d).$$

Beweis:

$$\sum_{d|n} F(d)\mu\left(\frac{n}{d}\right) = \sum_{\substack{d_1, d_2 \\ n = d_1 d_2}} f(d_1)\mu(d_2)$$

$$= \sum_{\substack{d_1, d_2 \\ n = d_1 d_2}} \sum_{d|d_1} f(d)\mu(d_2) = \sum_{\substack{d|n \\ d_2 | \frac{n}{d}}} f(d)\mu(d_2)$$

$$= \sum_{d|n} f(d)\varepsilon\left(\frac{n}{d}\right) = f(n).$$

□

Definition 1.3.10 (Eulersche φ-Funktion)
Für $n \in \mathbb{N}_+$ sei

> $\varphi(n)$ die Anzahl der Zahlen $a \in \mathbb{N}_+$ mit $1 \leq a \leq n$ und $(a, n) = 1$.
>
> φ heißt **Eulersche φ-Funktion**.

Satz 1.3.11
(1) $\varphi : \mathbb{N}_+ \longrightarrow \mathbb{N}_+$ ist multiplikativ und es gilt

$$\sum_{d|n} \varphi(d) = n.$$

(2) Ist $n = \prod_{i=1}^{r} p^{\alpha_i}$ die Primfaktorzerlegung von n, so gilt

$$\varphi(n) = \prod_{i=1}^{r}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \prod_{\substack{p|n \\ p \text{ Primzahl}}} \left(1 - \frac{1}{p}\right).$$

Beweis:

(1) Es sei $M_d^n = \{a \in \mathbb{Z} \mid 1 \leq a \leq n,\ (a,n) = d\}$.

Dann gilt

$$\{1, \ldots, n\} = \dot{\bigcup_{d|n}} M_d^n$$

und $M_d^n \longrightarrow M_1^{\frac{n}{d}}$, $a \longmapsto \dfrac{a}{d}$ ist bijektiv; also ist $\# M_d^n = \# M_1^{\frac{n}{d}} = \varphi(\frac{n}{d})$ und somit

$$n = \#\{1, \ldots, n\} = \sum_{d|n} \# M_d^n = \sum_{d|n} \varphi(\frac{n}{d})$$

□

(2) Dies folgt aus (1) und 1.3.7 (2) oder auch so: Für eine Primzahl p und für $1 \leq a \leq p^\alpha$ gilt entweder $p|a$ oder $(a, p^\alpha) = 1$. Es gibt aber genau $p^{\alpha-1}$ Vielfache von p in der Menge $\{a \mid 1 \leq a \leq p^\alpha\}$. Also ist

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

□

Offensichtlich gilt: $\varphi(n) = n - 1 \Longleftrightarrow n$ ist Primzahl.

Aus der Möbiusschen Umkehrformel folgt:

Lemma 1.3.12

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

□

Beispiel 1.3.13 Die Funktionen μ, φ, σ_k sind in ***Mathematica*** implementiert.

$\mu[n\_] =$ MoebiusMu$[n]$
$\varphi[n\_] =$ EulerPhi$[n]$
$\sigma_{k\_}[n\_] =$ DivisorSigma$[k, n]$

Weiter ergibt

Divisors $[n]$

die Liste aller Teiler von n.

Übungen 1.3.14

(1) (a) Beweise: Für alle $n \in \mathbb{N}_+$ gilt

$$\mu(n)\mu(n+1)\mu(n+2)\mu(2+3) = 0$$

(b) Beweise: Für $n \geq 3$ gilt

$$\sum_{k=1}^{n} \mu(k!) = 1.$$

(2) Es sei

$$\Lambda(n) := \begin{cases} \log p, & \text{falls } n = p^{\alpha}, \quad p \text{ Primzahl}, \\ & \qquad\qquad\quad \alpha \geq 1 \\ 0 & \text{sonst} \end{cases}$$

Beweise: $\Lambda(n) = \sum\limits_{d|n} \mu(\frac{n}{d}) \log d = -\sum\limits_{d|n} \mu(d) \log d$ und $\log n = \sum\limits_{d|n} \Lambda(d)$

(3) Es sei R ein kommutativer Ring mit Eins, $n \in \mathbb{N}_+$ und $n = \prod\limits_{i=1}^{r} p_i^{\alpha_i}$ sei die Primfaktorzerlegung von n.

(a) Beweise: Ist $f : \mathbb{N}_+ \longrightarrow R$ multiplikativ mit $f(1) = 1$, so gilt

$$\sum_{d|n} \mu(d) f(d) = \prod_{i=1}^{r} (1 - f(p_i))$$

(b) Berechne $\sum\limits_{d|n} \mu(d)\tau(d)$, $\sum\limits_{d|n} \mu(d)\sigma(d)$, $\sum\limits_{d|n} \mu(d) d^s$ $(s \in \mathbb{R})$.

(c) Beweise: $\sum\limits_{d|n} \dfrac{\mu^2(d)}{\varphi(d)} = \dfrac{n}{\varphi(n)}$

(4) (a) Beweise: Für $n, m \in \mathbb{N}_+$ gilt $\varphi(mn)\varphi(d) = d\varphi(m)\varphi(n)$, wobei $d = (m, n)$.

(b) Ist $n \geq 2$, so ist die Summe aller zu n teilerfremden Zahlen k mit $1 \leq k \leq n$ gleich $\frac{1}{2} n \varphi(n)$.

(5) (a) Seien $f, g : \mathbb{N}_+ \longrightarrow \mathbb{Z}$ Funktionen. Beweise:

$$\sum_{i=1}^{n} \left(f(i) \sum_{d|i} g(d) \right) = \sum_{d=1}^{n} \left(g(d) \sum_{j=1}^{[\frac{n}{d}]} f(d \cdot j) \right)$$

(b) Sei $F : \mathbb{N}_+ \longrightarrow \mathbb{Z}$ die summatorische Funktion von $f : \mathbb{N}_+ \longrightarrow \mathbb{Z}$. Beweise:

$$\sum_{i=1}^{n} F(i) = \sum_{i=1}^{n} f(i) \left[\frac{n}{i} \right]$$

(c) Berechne $\sum\limits_{i=1}^{n} \varphi(i) \left[\dfrac{n}{i} \right]$

(6) Es $k \geq 2$. Eine Zahl $n \in \mathbb{N}_+$ heißt k-vollkommen, wenn $\sigma(n) = kn$ gilt.

(a) Beweise: Eine gerade Zahl $n \in \mathbb{N}_+$ ist genau dann 2-vollkommen, wenn es eine Mersennesche Primzahl M_p gibt, so daß

$$n = 2^{p-1} M_p.$$

(b) Finde eine 3-vollkommene Zahl ≤ 150.

(7) Zwei Zahlen $a, b \in \mathbb{N}_+,\ a \neq b$, heißen befreundet, wenn $\sigma(a) = \sigma(b) = a + b$ gilt. Finde ein befreundetes Paar a, b mit $a, b < 300$.

(8) Beweise: $\det\Big(\big(\mathrm{ggT}(i,j)\big)_{i,j=1,\dots,n}\Big) = \prod_{k=1}^{n} \varphi(k)$

(9) Für $n \in \mathbb{N}_+$ sei $\deg n = \sum_{p \text{ Primzahl}} v_p(n)$ und $\lambda(n) := (-1)^{\deg n}$.

(a) Beweise: λ ist vollständig multiplikativ.

(b) Bestimme die summatorische Funktion von λ.

(c) Berechne $\sum_{d|n} \mu(d)\lambda(d)$

(10) Sei R ein kommutativer Ring mit Eins. Auf der Menge $S = R^{\mathbb{N}_+}$ der Funktionen $f : \mathbb{N}_+ \longrightarrow R$ wird folgende Multiplikation $*$ erklärt:

$$(f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

(a) Beweise: $(S, +, *)$ ist kommutativer Ring mit ε als Einselement.

(b) Sei $\chi_0 : \mathbb{N}_+ \longrightarrow R$ die Funktion $\chi_0(n) = 1$. Berechne $f*\chi_0,\ f*\chi_0*\mu,\ \chi_0*\mu$.

(c) Die multiplikativen Funktionen $f : \mathbb{N}_+ \longrightarrow R$ mit $f(1) = 1$ bilden eine Untergruppe von $S^\times$.

(d) Sei $(Lf)(n) := f(n)\log n$ (hier ist $R = \mathbb{R}$). Beweise:

$$L(f * g) = (Lf) * g + f * (Lg)$$

(11) Beweise: $\sqrt{n^{\tau(n)}} = \prod_{d|n} d$

(12) Für ***Mathematica*** -Fans

(a) Schreibe ein Programm zur Berechnung von φ, τ, σ.

(b) Schreibe ein Programm zum Auffinden von befreundeten Zahlen.

Kapitel 2

Kongruenzen, Restklassen

2.1 Lineare Kongruenzen, Eulerscher Satz

Definition 2.1.1 Seien $a, b \in \mathbb{Z}$ und $m \in \mathbb{N}_+$.

$$a \equiv b \bmod m :\Longleftrightarrow m|b-a$$

Man sagt dann: a und b sind **kongruent modulo** m. Offensichtlich ist dies genau dann der Fall, wenn

$$\mathrm{Mod}[a,m] = \mathrm{Mod}[b,m],$$

wenn also a und b beim Teilen durch m denselben Rest haben.

Lemma 2.1.2 Es sei $m \in \mathbb{N}_+$.

(1) Die Relation $a \equiv b \bmod m$ ist eine Äquivalenzrelation auf $\mathbb{Z}$.

(2) $a \equiv b \bmod m$ und $c \equiv d \bmod m \Longrightarrow a + c \equiv b + d \bmod m$ und $ac \equiv bd \bmod m$

(3) $a \equiv b \bmod m,\ d|m \Longrightarrow a \equiv b \bmod d$

(4) (Kürzungsregel)

$$ad \equiv bd \bmod m \text{ und } (d,m) = 1 \Longrightarrow a \equiv b \bmod m.$$

Beweis:

(1) Statt $a \equiv b \bmod m$ schreiben wir hier kurz $a \equiv b$. Es gilt

   (a) $a \equiv a$, weil $m|a-a$.

   (b) $a \equiv b \Longrightarrow m|b-a \Longrightarrow m|a-b \Longrightarrow b \equiv a$.

   (c) $a \equiv b$ und $b \equiv c \Longrightarrow m|b-a,\ m|c-b \Longrightarrow m|c-b+b-a \Longrightarrow a \equiv c$.
   Also ist $\equiv$ eine Äquivalenzrelation.

(2) $a \equiv b$ und $c \equiv d \Longrightarrow b - a = sm,\ d - c = tm$

$$\Longrightarrow b + d - (a + c) = (s + t)m \Longrightarrow a + c \equiv b + d.$$

Weiter folgt aus $b = a + sm,\ d = c + tm$

$$bd = ad + (at + cs)m + stm^2, \text{ also } ad \equiv bd.$$

(3) $a \equiv b \bmod m \Longrightarrow b - a = sm$

$$d|m \Longrightarrow m = m'd \Longrightarrow b - a = (sm')d \Longrightarrow a \equiv b \bmod d.$$

(4) $ad \equiv bd \bmod m \Longrightarrow m|(b - a)d$
Da $(m, d) = 1$, folgt $m|b - a$, also $a \equiv b \bmod m$. □

Definition 2.1.3 Sei $m \in \mathbb{N}_+$ fest gewählt. Für $a \in \mathbb{Z}$ sei

$$\begin{aligned} [a]_m &:= \{b \in \mathbb{Z} \mid b \equiv a \bmod m\} \\ &= \{mq + b \mid q \in \mathbb{Z}\} \end{aligned}$$

die Äquivalenzklasse von a in $\mathbb{Z}$ bezüglich der Äquivalenzrelation 'kongruent modulo m'. $[a]_m$ heißt auch die **Restklasse von a modulo m**. Mit $\mathbb{Z}/m\mathbb{Z} = \{[a]_m \mid a \in \mathbb{Z}\}$ wird die Menge der Restklassen modulo m bezeichnet. Die Abbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z},\ a \longmapsto [a]_m$$

heißt die **Restklassenabbildung** (modulo m).

Ist $x \in \mathbb{Z}/m\mathbb{Z}$ und $a \in \mathbb{Z}$ mit $x = [a]_m$, so heißt a **Repräsentant** von x. Jede zu a kongruente Zahl b ist dann ebenfalls ein Repräsentant von x.

Nach Lemma 2.1.2 (2) sind die folgenden Rechenoperationen für Restklassen wohldefiniert:

Seien $x, y \in \mathbb{Z}/m\mathbb{Z}$ mit Repräsentanten $a, b \in \mathbb{Z}$, also $x = [a]_m,\ y = [b]_m$. Man setzt

$$\begin{aligned} x + y &:= [a + b]_m \\ x \cdot y &:= [a \cdot b]_m \end{aligned}$$

Man erhält nun ohne Mühe

Satz 2.1.4 Sei $m \in \mathbb{N}_+$. Dann ist $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Eins. Die Restklassenabbildung

$$\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

ist ein surjektiver Ringhomomorphismus. $[1]_m$ ist das Einselement und $[0]_m$ ist das Nullelement in $\mathbb{Z}/m\mathbb{Z}$. □

$\mathbb{Z}/m\mathbb{Z}$ heißt der **Restklassenring modulo m**. Das Rechnen im Ring $\mathbb{Z}/m\mathbb{Z}$ heißt auch **modulare Arithmetik**.

Wir wollen dies in ***Mathematica*** programmieren. Dazu definieren wir zunächst

Definition 2.1.5 Eine Teilmenge $\{c_1, \ldots, c_m\} \subset \mathbb{Z}$ heißt **vollständiges Restsystem** modulo m, wenn $\mathbb{Z}/m\mathbb{Z} = \{[c_1]_m, \ldots, [c_m]_m\}$ gilt. $\{0, 1 \ldots, m-1\}$ heißt das **kleinste nichtnegative Restsystem** modulo m.

$$\{-\frac{m}{2}+1, \ldots -1, 0, 1, \ldots, \frac{m}{2}\}, \text{ falls } m \text{ gerade, bzw.}$$
$$\{-\frac{m-1}{2}, \ldots, -1, 0, 1 \ldots, \frac{m-1}{2}\}, \text{ falls } m \text{ ungerade,}$$

heißt das **absolut kleinste Restsystem** modulo m.

Beispiel 2.1.6 (Modulare Arithmetik mit ***Mathematica***) (vgl. [11] Kapitel 5)
Es sei $m \in \mathbb{N}_+$ und $n \in \mathbb{Z}$. Das Paar (n, m) definiert das Element $[n]_m$ in $\mathbb{Z}/m\mathbb{Z}$, welches wir jetzt mit

$$n \bmod m$$

bezeichnen wollen. Das Paar (n, m) versehen wir nun in ***Mathematica*** mit einem Kopf, sagen wir etwa 'modularezahl'. Der Ausdruck

$$\text{modularezahl}[n, m]$$

soll dann die Restklasse $[n]_m \in \mathbb{Z}/m\mathbb{Z}$ beschreiben. Es gibt jetzt den Variablentyp

$$x\_\,\text{modularezahl}\,.$$

Daß die Eingabe modularezahl$[n, m]$ in der Form

$$n \bmod m$$

ausgegeben wird, kann man in ***Mathematica*** durch den Befehl

$$\text{Format}[x\_\,\text{modularezahl}] := \text{Infix}[x, \text{"mod"}]$$

erreichen.

Jetzt stellen wir die Regeln auf:
rest$[n, m]$ sei dabei irgendeine noch festzulegende Funktion, die (n, m) den zu n modulo m kongruenten Rest r aus einem ausgezeichneten vollständigen Restsystem modulo m zuordnet. Wir wählen der Einfachheit halber den kleinsten nichtnegativen Rest:

$$\text{rest} = \text{Mod}\,.$$

Die Restklassenabbildung $\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ wird nun durch

$$q[n\_\text{Integer}, m\_\text{Integer?Positive}] := \text{modularezahl}[\text{rest}[n, m], m]$$

eingeführt. Nach Konstruktion gilt wie gewünscht: $q[n, m] = q[n', m'] \Longleftrightarrow m = m'$ und rest$[n, m] =$ rest$[n', m]$. Es gilt zum Beispiel

$$q[6, 5] = 1 \bmod 5,$$

Wir setzen nun weiter

$$\text{repräsentant}[x\_ \text{ modularezahl}] := x[\![1]\!],$$
$$\text{modul}[x\_ \text{ modularezahl}]] := x[\![2]\!].$$

Dabei ist modularezahl$[a_1, a_2][\![i]\!] = a_i$.
Durch die folgenden Befehle werden die Addition und Multiplikation definiert:

```
modularezahl/:
        x_ modularezahl +y_ modularezahl :=
        If [modul[x] == modul[y],
           q repräsentant[x]+repräsentant[y], modul[x]],
           Print["geht nicht"]]
modularezahl/:
        x_ modularezahl *y_ modularezahl :=
        If [modul[x] ==modul[y],
           q[repräsentant[x]* repräsentant[y], modul[x]],
           Print["geht nicht"]]
```

Wenn wir die Festlegung rest = Mod aufheben (das geht durch den Befehl Clear[rest]), so ergibt $q[3,5]+q[6,5]$ den Wert $q[\text{rest}[3,5]+\text{rest}[6,5],5]$ und wird nicht weiter ausgewertet, weil $\text{rest}[3,5]+\text{rest}[6,5]$ nicht als ganze Zahl betrachtet werden kann. Mit rest = Mod erhält man

$$q[3,5]+q[6,5] = 4 \bmod 5.$$

Definiert man aber zum Beispiel rest als den absolut kleinsten Rest, so ergibt sich

$$q[3,5]+q[6,5] = -1 \bmod 5.$$

Das Potenzieren modulo m ist in ***Mathematica*** durch den Befehl

$$\text{PowerMod}[n,k,m]$$

gegeben. Wir können dies in unsere modulare Arithmetik einbauen:

```
modularezahl/:
x_ modularezahl ^k_ Integer :=
q[PowerMod[repräsentant[x], k, modul[x]], modul[x]]
```

Auch die Verknüpfung $\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$ $(a, b \bmod m) \longmapsto (ab) \bmod m$ können wir einführen:

```
modularezahl/:
a_ Integer *b_ modularezahl :=
q[a * repräsentant[b], modul[b]]
```

Man kann daraus auch ein Programmpaket schnüren, ein sogenanntes **Package** (siehe [23] 2.6.10 und [11] 4.3).

Wir testen unsere Funktionen mit einigen Beispielen: Zunächst führen wir die modularen Zahlen a, b, c, d ein

$$\begin{array}{rcl c r}
a &=& q[7732, 37] &=& 36 \bmod 37 \\
b &=& q[44311, 37] &=& 22 \bmod 37 \\
c &=& q[2, 37] &=& 2 \bmod 37 \\
d &=& q[4, 12] &=& 4 \bmod 12
\end{array}$$

Dann ergibt sich zum Beispiel

$$\begin{array}{rcl rcl}
a\ b &=& 15 \bmod 37, & & & \\
c\text{^}3 &=& 8 \bmod 37, & c\text{^}100 &=& 12 \bmod 37, \\
c\text{^}(-1) &=& 19 \bmod 37, & c * c\text{^}(-1) &=& 1 \bmod 37, \\
(a+b)\text{^}3 &=& 11 \bmod 37. & & &
\end{array}$$

Aber

$$d\text{^}(-1) = \text{modularezahl}[\text{PowerMod}[4, -1, 12], 12]$$

wird nicht berechnet, weil d keine Einheit in $\mathbb{Z}/12\mathbb{Z}$ ist, denn

$$d \cdot q[3, 12] = 0 \bmod 12.$$

Das Multiplizieren mit ganzen Zahlen funktioniert auch:

$$3c = 6 \bmod 37,$$
$$3d = 0 \bmod 12$$

Die Additionstafel von $\mathbb{Z}/m\mathbb{Z}$ erzeugt man durch den Befehl

$$\begin{array}{l}
\text{Additionstafel}[m_\text{Integer?Positive}] := \\
\text{Table}[\text{rest}[a+b, m], \{a, 0, m-1\}, \{b, 0, m-1\}]//\text{TableForm}
\end{array}$$

Berechnete Beispiele findet man im ***Mathematica***-Anhang

Man sieht, daß $(\mathbb{Z}/m\mathbb{Z}, +)$ eine zyklische Gruppe der Ordnung m mit $[1]_m = 1 \bmod m$ als erzeugendem Element ist, denn

$$\mathbb{Z}/m\mathbb{Z} = \{n \cdot [1]_m \mid n \in \mathbb{Z}\}.$$

Die Multiplikationstafel von $\mathbb{Z}/m\mathbb{Z}$ wird durch den Befehl

$$\text{Table}[\text{rest}[a * b, m], \{a, 0, m-1\}, \{b, 0, m-1\}]//\text{TableForm}$$

erzeugt. Im Fall $m = 7$ sieht man, daß auch alle Elemente $[a]_m,\ a = 1, 2, 3, 4, 5, 6$ die additive Gruppe $(\mathbb{Z}/7\mathbb{Z}, +)$ erzeugen.

Anders ist es im Fall $m = 8$:

Hier sind nur $[1]_8, [3]_8, [5]_8, [7]_8$ Erzeuger der additiven Gruppe $(\mathbb{Z}/8\mathbb{Z}, +)$. Allgemein gilt folgender Satz:

Satz 2.1.7 Es sei $m \in \mathbb{N}$, $m \geq 2$. Weiter seien $a, b \in \mathbb{Z}$. Die lineare Kongruenz

$$(*) \qquad ax \equiv b \bmod m$$

ist genau dann lösbar, wenn (a, m) ein Teiler von b ist. Ist $x_0 \in \mathbb{Z}$ eine Lösung, so gibt es modulo m genau (a, m) verschiedene Lösungen. Es sind dies

$$x = x_0 + \frac{m}{(a,m)} t, \ t = 0, 1, \dots, (a, m) - 1.$$

Sind a und m teilerfremd, so hat die Gleichung (*) genau eine Lösung modulo m.

Beweis: $ax \equiv b \bmod m$ ist genau dann lösbar, wenn die lineare diophantische Gleichung

$$ax + my = b$$

lösbar ist; nach Satz 1.15 ist dies genau dann der Fall, wenn (a, m) Teiler von b ist, und

$$\{x_t = x_0 + t\frac{m}{(a,m)} \;\Big|\; t \in \mathbb{Z}\}$$

ist die Menge aller ganzzahligen Lösungen. Es gilt nun für $t, s \in \mathbb{Z}$:

$$x_t \equiv x_s \bmod m \Longleftrightarrow m \;\Big|\; (s-t)\frac{m}{(a,m)} \Longleftrightarrow (a,m) \;\Big|\; s-t \Longleftrightarrow t \equiv s \bmod (a,m).$$

Man erhält also die verschiedenen Lösungen x_t modulo m, wenn t ein vollständiges Restsystem modulo (a, m) durchläuft. □

Korollar 2.1.8 Sei $m \in \mathbb{N}, \ m \geq 2$.
Für $a \in \mathbb{Z}$ ist die lineare Kongruenz

$$ax \equiv 1 \bmod m$$

genau dann lösbar, wenn $(a, m) = 1$ gilt. Die Einheitengruppe

$$(\mathbb{Z}/m\mathbb{Z})^\times$$

von $\mathbb{Z}/m\mathbb{Z}$ besteht aus den Restklassen $[a]_m$ von Zahlen $1 \leq a \leq m$ mit $(a, m) = 1$. Die Ordnung von $(\mathbb{Z}/m\mathbb{Z})^\times$ ist $\varphi(m)$, d.h. $(\mathbb{Z}/m\mathbb{Z})^\times$ besitzt genau $\varphi(m)$ Elemente. □

Korollar 2.1.9 Ist p eine Primzahl, so ist $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ ein Körper. □

Definition 2.1.10 $\mathbb{F}_p$ heißt **Primkörper der Charakteristik** p.

Beispiel 2.1.11

(1) Ist $ax \equiv b \bmod m$ zu lösen, so kann man versuchen (etwa falls a klein ist) zunächst $my \equiv b \bmod a$ zu lösen. Ist y_0 eine Lösung von $my \equiv b \bmod a$, so ist $x_0 = \frac{b - my_0}{a}$ eine ganzzahlige Lösung von $ax \equiv b \bmod m$. Wir betrachten ein konkretes Beispiel:

$$3x \equiv 157 \bmod 311.$$

Wir untersuchen zunächst

$$311y \equiv 157 \bmod 3.$$

Diese Kongruenz ist natürlich äquivalent zu

$$-y \equiv 1 \bmod 3,$$

weil $311 \equiv -1 \bmod 3$ und $157 \equiv 1 \bmod 3$ gilt.

Eine Lösung ist also

$$y_0 = -1.$$

Damit ist $x_0 = \frac{b-my_0}{a} = \frac{157+311}{3} = \frac{468}{3} = 156$ eine Lösung unserer Ausgangskongruenz. Da $(3, 311) = 1$, ist die Lösung modulo 311 eindeutig bestimmt.

(2) Die Standardmethode ist durch den erweiterten euklidischen Algorithmus gegeben:

Um $ax \equiv b \bmod m$ zu lösen, löst man

$$ax + my = d \quad (\text{wobei } d = (a, m))$$

mit dem erweiterten euklidischen Algorithmus:

$$\text{erwggT}(a, b) = \{d,\ \{x_0, y_0\}\}.$$

Ist d Teiler von b, so ist

$$x_t = x_0 \cdot \frac{b}{d} + t\frac{m}{d}, \quad t = 0, \ldots, d-1$$

die allgemeine Lösung von $ax \equiv b \bmod m$.

Im Beispiel $3x \equiv 157 \bmod 311$ geht es um die diophantische Gleichung

$$3x + 311y = d, \quad d = (3, 311).$$

Man erhält das Schema:

$$\begin{aligned} 311 &= 103 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 \end{aligned}$$

(I) $\quad 311 - 103 \cdot 3 = 2$

(II) $\quad 3 - 1 \cdot 2 = 1$

(I) in (II) einsetzen $\Longrightarrow$

$$3 - 1(311 - 103 \cdot 3) = 1$$

$$\begin{aligned} &\Longrightarrow 1 = 104 \cdot 3 - 311 \\ &\Longrightarrow d = 1,\ x = 104,\ y = -1; \\ &\Longrightarrow x_0 = x \cdot b = 104 \cdot 157 \text{ ist die Lösung.} \end{aligned}$$

Reduktion modulo 311 ergibt

$$104 \cdot 157 = 52 \cdot 314 \equiv 52 \cdot 3 = 156$$

wie oben.

(3) Ist $(a,m)=1$, so besitzt $[a]_m$ ein Inverses in $\mathbb{Z}/m\mathbb{Z}$. Ist $x\in\mathbb{Z}$ Repräsentant von $([a]_m)^{-1}$, so gilt also
$$[a]_m\cdot[x]_m=[1]_m,$$
d.h.
$$ax\equiv 1 \bmod m.$$
Es gibt verschiedene Möglichkeiten x zu bestimmen. Ein Beispiel: Wir berechnen
$$[5]_{27}^{-1}\in\mathbb{Z}/27\mathbb{Z}.$$

(a) $5x\equiv 1 \bmod 27$ ist zu lösen. Es gilt:
$$\begin{aligned}
&27y\equiv 1 \bmod 5 \Longrightarrow 2y\equiv 1 \bmod 5 \Longrightarrow y\equiv 3 \bmod 5\\
&\Longrightarrow x=\frac{1-3\cdot 27}{5}=-\frac{80}{5}=-16\equiv 11 \bmod 27\\
&\Longrightarrow [5]_{27}^{-1}=[11]_{27}.
\end{aligned}$$

(b) Mit 'Bruchrechnung' in $\mathbb{Z}/27\mathbb{Z}$ ($[\ ]_{27}$ wird hier weggelassen) geht es so:
$$\begin{aligned}
&\frac{1}{5}=\frac{28}{5}=\frac{55}{5}=\frac{5\cdot 11}{5}=11.\quad\text{Analog:}\\
&\frac{1}{10}=\frac{1}{5}\cdot\frac{1}{2}=11\cdot\frac{1}{2}=\frac{11}{2}=\frac{38}{2}=19\Longrightarrow [10]_{27}^{-1}=[19]_{27}.
\end{aligned}$$
Im Nenner dürfen nur zu 27 teilerfremde Zahlen stehen. Unsinn ist etwa
$$\frac{1}{10}\stackrel{!}{=}\frac{3}{3\cdot 10}=\frac{3}{30}=\frac{3}{3}=1,$$
weil 3 keine Einheit modulo 27 ist.
$(\mathbb{Z}/27\mathbb{Z})^\times$ ist Gruppe der Ordnung $\varphi(27)=3^3-3^2=18$. Diese Gruppe ist ebenfalls zyklisch, und 5 ist ein Erzeuger:
$$(\mathbb{Z}/27\mathbb{Z})^\times=\{5^k \bmod 27 \mid k=1,\ldots,18\}.$$
Da $\varphi(18)=\varphi(2\cdot 3^2)=\varphi(2)\varphi(3^2)=6$, gibt es 6 verschiedene Erzeuger dieser Gruppe, nämlich
$$5,\ 5^5=-7,\ 5^7=13,\ 5^{11}=2,\ 5^{13}=-4,\ 5^{17}=11.$$

Satz 2.1.12 (Chinesischer Restsatz)
Seien $m_1,\ldots,m_k\geq 2$ paarweise teilerfremd und $m=m_1\cdot\ldots\cdot m_k$. Weiter seien $c_1,\ldots,c_k\in\mathbb{Z}$. Dann gilt: Das System von Kongruenzen
$$x\equiv c_j \bmod m_j,\ j=1,\ldots,k$$
hat modulo m genau eine Lösung $x\in\mathbb{Z}$.

Beweis:

(1) Existenz:

Setze $m_i' = m/m_i$. Dann ist $(m_i', m_i) = 1$ und nach Korollar 2.1.8 gibt es Zahlen $m_i'' \in \mathbb{Z}$ mit $m_i' m_i'' \equiv 1 \bmod m_i$. Es sei $e_i := m_i' m_i'' \in \mathbb{Z}$. Dann ist

$$\begin{aligned} e_i &\equiv 1 \bmod m_i \quad \text{und} \\ e_j &\equiv 0 \bmod m_i \quad \text{für } j \neq i, \end{aligned}$$

also ist $x = e_1 c_1 + \cdots + e_k c_k$ Lösung des Systems, denn für $i = 1, \ldots, k$ gilt

$$x \equiv 0 \cdot c_1 + \cdots 0 \cdot c_{i-1} + 1 \cdot c_i + 0 \cdot c_{i+1} + \cdots + 0 \cdot c_k = c_i \bmod m_i.$$

(2) Eindeutigkeit:

Seien $x, y \in \mathbb{Z}$ zwei Lösungen. Dann gilt

$$m_i \mid x - y \quad \text{für } i = 1, \ldots, k.$$

Da $m = m_1 \cdot \ldots \cdot m_k$ und $m_1, \ldots, m_k$ paarweise teilerfremd sind, folgt

$$m \mid x - y,$$

d.h. $x \equiv y \bmod m$. □

Beispiel 2.1.13 $1001 = 7 \cdot 11 \cdot 13$.

Es sei M eine endliche Menge mit höchstens 1000 Elementen. Wie bestimmt man die Anzahl x der Elemente von M ? Man bildet 7er-Bündel und erhält einen Rest c_1. Dann bildet man 11er und schließlich 13er-Bündel und erhält den Rest c_2 bzw. c_3. Jetzt löst man das System von Kongruenzen

$$\begin{aligned} x &\equiv c_1 \bmod 7, \\ x &\equiv c_2 \bmod 11, \\ x &\equiv c_3 \bmod 13. \end{aligned}$$

Sei etwa $c_1 = 3,\ c_2 = 4,\ c_3 = 5$. Zur Lösung geht man wie im Beweis des chinesischen Restsatzes vor:

$$\begin{aligned} m_1 = 7,&\ m_1' = 11 \cdot 13 = 143, \\ m_2 = 11,&\ m_2' = 7 \cdot 13 = 91, \\ m_3 = 13,&\ m_3' = 7 \cdot 11 = 77. \end{aligned}$$

Jetzt müssen wir $m_1'' \in \mathbb{Z}$ mit

$$143 m_1'' \equiv 1 \bmod 7$$

finden. Hierzu ist natürlich wegen $143 \equiv 3 \bmod 7$ die Kongruenz

$$3 m_1'' \equiv 1 \bmod 7$$

äquivalent, und

$$m_1'' = 5$$

ist eine Lösung. Nun ist m_2'' mit $91m_2'' \equiv 1 \bmod 11$, also mit $3m_2'' \equiv 1 \bmod 11$ zu bestimmen. $m_2'' = 4$ ist eine Lösung. Schließlich ist $m_3'' = -1$ eine Lösung von $77m_3'' \equiv 1 \bmod 13$. Es folgt:

$$\begin{aligned} e_1 &= m_1' m_2'' = 143 \cdot 5 = 715, \\ e_2 &= m_2' m_2'' = 91 \cdot 4 = 364, \\ e_3 &= m_3' m_3'' = -77. \end{aligned}$$

Die Zahlen e_1, e_2, e_3 sind für jedes Tripel c_1, c_2, c_3 verwendbar. In unserem Fall ist

$$\begin{aligned} x &\equiv c_1 \cdot e_1 + c_2 \cdot e_2 + c_3 \cdot e_3 \\ &\equiv 3 \cdot 715 + 4 \cdot 364 - 5 \cdot 77 \\ &\equiv 2145 + 1456 - 385 \\ &\equiv 143 + 455 - 385 = 598 - 385 = 213. \end{aligned}$$

213 ist die einzige Lösung zwischen 0 und 1000. Also hat die Menge M genau 213 Elemente.

Eine etwas abstraktere Formulierung des chinesischen Restsatzes lautet folgendermaßen:

Satz 2.1.14 Seien $m_1, \ldots, m_k$ paarweise teilerfremde positive ganze Zahlen, $m = m_1 \cdot \ldots \cdot m_k$. Dann ist die Abbildung

$$\Phi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$$

mit $\Phi(a \bmod m) = (a \bmod m_1, \ldots, a \bmod m_2)$ ein Ringisomorphismus.
Für $i = 1, \ldots, k$ sei $e_i \in \mathbb{Z}$ die ganze Zahl

$$e_i = \frac{m}{m_i} \cdot \text{ Repräsentant } \left(\left(\frac{m}{m_i} \bmod m_i \right)^{-1} \right).$$

Dann induziert die Abbildung

$$\Psi : \mathbb{Z}^k \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

mit $\Psi(x_1, \ldots, c_k) = \sum_{i=1}^{k} c_i e_i \bmod m$ die Umkehrabbildung

$$\Phi^{-1} : \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z}$$

von Φ.

Beweis: Der Satz ist nur eine Umformulierung von 2.1.12. Sind $R_1, \ldots, R_k$ kommutative Ringe mit Eins, so ist das cartesische Produkt $R_1 \times \cdots \times R_k$ mit den komponentenweise erklärten Verknüpfungen ein kommutativer Ring mit Eins, der **Produktring** von $R_1, \ldots, R_k$. $\square$

Bemerkung 2.1.15 Die Restklassen $e_i \bmod m$ der in 2.1.14 definierten Zahlen e_i sind **idempotente** Elemente in $\mathbb{Z}/m\mathbb{Z}$, d.h.

(1) $$e_i^2 \equiv e_i \bmod m.$$

Das folgt sofort aus

$$e_i \equiv 1 \bmod m_i \text{ und } e_i \equiv 0 \bmod m_j \text{ für } j \neq i.$$

Denn dann ist auch

$$e_i^2 \equiv 1 \bmod m_i \text{ und } e_i^2 \equiv 0 \bmod m_j \text{ für } j \neq i,$$

also

$$e_i^2 \equiv e_i \bmod m_j \text{ für } j = 1, \dots, k.$$

Weiter zeigt man analog, daß

(2) $$e_i e_j \equiv 0 \bmod m \text{ für } i \neq j,$$

(3) $$e_1 + \dots + e_k \equiv 1 \bmod m.$$

Allgemein kann man leicht zeigen: Ist R ein kommutativer Ring mit Eins und sind $e_1, \dots, e_k \in R \backslash \{0\}$ idempotente Elemente mit $\sum\limits_{i=1}^{k} e_i = 1$ und $e_i e_j = 0$ für $i \neq j,\ k \geq 2$, so ist

$$R_i = Re_i = \{ae_i \mid a \in R\}$$

ein Unterring von R mit e_i als Einselement (e_i ist nicht das Einselement von R!) und

$$\Phi : R \longrightarrow R_1 \times \dots \times R_k \text{ mit } \Phi(a) = (ae_1, \dots, ae_k)$$

ist Ringisomorphismus mit

$$\Psi : R_1 \times \dots \times R_k \longrightarrow R,$$
$$\Psi(x_1, \dots, x_k) = x_1 + \dots + x_k$$

als inverser Abbildung.

Beweis:

(1) $\Psi \circ \Phi(a) = \Psi(ae_1, \dots, ae_k) = ae_1 + \dots + ae_k = a(e_1 + \dots + e_k) = a1 = a.$

(2) $\Phi \circ \Psi(x_1, \dots, x_k) = \Phi(x_1 + x_2 + \dots + x_k) = \left(\sum\limits_{i=1}^{k} x_i e_1, \sum\limits_{i=1}^{k} x_i e_2, \dots \sum\limits_{i=1}^{k} x_i e_k\right).$

Da $x_i = c_i e_i$ für ein $c_i \in R$, folgt

$$\sum_{i=1}^{k} x_i e_j = \sum_{i=1}^{k} c_i e_i e_j = c_j e_j^2 = c_j e_j = x_j,$$

also $\Phi \circ \Psi(x_1, \dots, x_k) = (x_1, \dots, x_k).$ □

Aus Satz 2.1.14 folgt unmittelbar:

Korollar 2.1.16 Seien $m_1, \ldots, m_k, m, \Phi$ wie in Satz 2.1.14. Dann gilt: Φ induziert einen Gruppenisomorphismus

$$(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/m_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/m_k\mathbb{Z})^\times.$$

$\square$

Definition 2.1.17 Sei $m \geq 2$. Eine Teilmenge $\{c_1, \ldots, c_{\varphi(m)}\} \subset \mathbb{Z}$ heißt **primes Restsystem** modulo $m \Longleftrightarrow (c_i, m) = 1$ fr $i = 1, \ldots, \varphi(m)$ und

$$c_i \not\equiv c_j \bmod m \text{ für } i \neq j,$$

d.h. $(\mathbb{Z}/m\mathbb{Z})^\times = \{c_1 \bmod m, \ldots, c_{\varphi(m)} \bmod m\}$.

Satz 2.1.18 (Euler) Für $a, m \in \mathbb{Z}$ mit $(a, m) = 1$ und $m \geq 2$ gilt

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Beweis: Sei $\{c_1, \ldots, c_{\varphi(m)}\}$ ein primes Restsystem modulo m. Dann ist auch $\{ac_1, \ldots, ac_{\varphi(m)}\}$ ein primes Restsystem modulo m, denn:

$$ac_i \equiv ac_j \bmod m \Longrightarrow m \mid a(c_j - c_i).$$

Da $(m, a) = 1$, muß m Teiler von $c_j - c_i$ sein; also gilt $c_i \equiv c_j \bmod m$ und somit $i = j$.
Es folgt

$$\begin{aligned} c_1 \cdot \ldots \cdot c_{\varphi(m)} &\equiv (ac_1) \cdot \ldots \cdot (ac_{\varphi(m)}) \\ &= a^{\varphi(m)} c_1 \cdot \ldots \cdot c_{\varphi(m)} \bmod m, \end{aligned}$$

also $1 \equiv a^{\varphi(m)} \bmod m$. $\square$

Mit etwas elementarster Gruppentheorie kann man so argumentieren: Da $(\mathbb{Z}/m)^\times$ eine Gruppe der Ordnung $\varphi(m)$ ist, ist die Ordnung eines jeden Elementes von $(\mathbb{Z}/m)^\times$ ein Teiler von $\varphi(m)$, insbesondere gilt

$$a^{\varphi(m)} \equiv 1 \bmod m \text{ für } (a, m) = 1.$$

$\square$

Ist G eine multiplikativ geschriebene Gruppe, so wird bekanntlich die Ordnung eines Elementes $g \in G$ als die kleinste positive Zahl $n \in \mathbb{N}$ definiert, für die $g^n = 1$ gilt. Ist G endlich, so ist die Ordnung von g ein Teiler der Gruppenordnung.

Korollar 2.1.19 (kleiner Fermat) Ist p eine Primzahl, so gilt

$$a^p \equiv a \bmod p \text{ für alle } a \in \mathbb{Z}.$$

$\square$

Beispiel 2.1.20

(1) Mit dem Satz von Euler kann man schnell Potenzen modulo m berechnen, sofern man den Wert $\varphi(m)$ kennt.

Wir stellen etwa die Aufgabe, die letzten beiden Dezimalstellen von 3^{256} zu bestimmen. Wir haben also

$$3^{256} \bmod 100$$

zu bestimmen: Es gilt $\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2-2)(5^2-5) = 40$, also ist

$$\begin{aligned} 3^{256} = 3^{240+16} = (3^6)^{40} \cdot 3^{16} &\underset{[Euler]}{\equiv} 3^{16} \\ &\equiv 81^4 \equiv (-19)^4 \equiv 361^2 \equiv 61^2 \\ &\equiv 21 \bmod 100 \Longrightarrow \end{aligned}$$

2 ist die Zehnerziffer und 1 ist Einerziffer.

(2) Wir untersuchen die Gruppenstruktur von $(\mathbb{Z}/100\mathbb{Z})^\times$. Nach Korollar 2.1.16 gilt

$$(\mathbb{Z}/100\mathbb{Z})^\times \cong (\mathbb{Z}/25\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times.$$

Ist $(a,100) = 1$ und $0 \leq a < 100$, so ist $\Phi(a) = (a_1, a_2)$ mit $a_1 = \mathrm{Mod}(a, 25)$, $a_2 = \mathrm{Mod}(a, 4)$ das Bild von a unter dem Isomorphismus Φ.

Die Gruppe $(\mathbb{Z}/25\mathbb{Z})^\times$ ist zyklisch von der Ordnung $\varphi(5^2) = 5^2 - 5 = 20$ und $2 \bmod 25$ ist ein Erzeuger. $(\mathbb{Z}/4\mathbb{Z})^\times$ ist zyklisch von der Ordnung 2 mit $3 \bmod 4$ als Erzeuger.

Die Paare $(2 \bmod 25,\ 1 \bmod 4)$ und $(1 \bmod 25,\ 3 \bmod 4)$ sind somit Erzeuger der Produktgruppe

$$(\mathbb{Z}/25\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times.$$

Ihre Bilder unter dem Isomorphismus

$$\Phi^{-1} = \Psi : (\mathbb{Z}/25\mathbb{Z})^\times \times (\mathbb{Z}/4\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/100\mathbb{Z})^\times$$

erzeugen dann natürlich die Gruppe $(\mathbb{Z}/100\mathbb{Z})^\times$. Um Ψ zu berechnen, brauchen wir nur die idempotenten Restklassen $e_1 \bmod 100$ und $e_2 \bmod 100$ mit

$$\begin{aligned} e_1 + e_2 &\equiv 1 \bmod 100 \\ e_1 &\equiv 1 \bmod 25 \\ e_1 &\equiv 0 \bmod 4 \end{aligned}$$

zu bestimmen. Es ergibt sich $e_1 = 76,\ e_2 = 25$, also ist

$$\Psi(2 \bmod 25,\ 1 \bmod 4) = (2 \cdot 76 + 1 \cdot 25) \bmod 100 = 77 \bmod 100$$

und

$$\Psi(1 \bmod 25,\ 3 \bmod 4) = (1 \cdot 76 + 3 \cdot 25) \bmod 100 = 51 \bmod 100.$$

Es gilt somit

$$(\mathbb{Z}/100\mathbb{Z})^\times = \{77^k 51^l \bmod 100 \mid k = 0, \ldots, 19;\ l = 0, 1\}.$$

Insbesondere ist diese Gruppe nicht zyklisch. Später (in Abschnitt 4.4) werden wir allgemein die Struktur von $(\mathbb{Z}/m\mathbb{Z})^\times$ bestimmen.

Es ist kein Problem, mit ***Mathematica*** hohe Potenzen einer ganzen Zahl modulo einer großen Zahl m zu berechnen. Man beachte, daß es nicht so einfach ist, $\varphi(m)$ zu berechnen, wenn m sehr groß ist und wenn man die Primfaktorzerlegung von m nicht kennt. Solange man $\varphi(m)$ nicht kennt, kann man natürlich den Eulerschen Satz nicht anwenden um $c^k \bmod m$ im Fall $k > \varphi(m)$ auf eine Potenz $c^{k'} \bmod m$ mit $0 \leq k < \varphi(m)$ zu reduzieren.

Man kann aber zum Beispiel k als Summe von Zweierpotenzen schreiben,

$$k = 2^{n_1} + \cdots + 2^{n_t}, \ n_1 > n_2 > \ldots > n_t,$$

und durch sukzessives Quadrieren modulo m die Reste $0 \leq s_\nu < m$ mit

$$s_\nu \equiv c^{2^\nu} \bmod m, \ \nu = 0, 1, \ldots, n_1$$

bestimmen: Wegen $(c^{2^\nu})^2 = c^{2^\nu \cdot 2} = c^{2^{\nu+1}}$ ist nämlich

$$s_{\nu+1} \equiv s_\nu^2 \bmod m.$$

$r \equiv s_{n_1} \cdot \ldots \cdot s_{n_t} \bmod m$ ist dann der gesuchte Rest $r \equiv c^k \bmod m$. Es sind dazu höchstens $2n_1 \leq 2 \log_2 k$ Multiplikationen modulo m nötig.

Mit Hilfe des kleinen Fermats ergibt sich folgender einfache Primzahltest:

Beispiel 2.1.21 (Chinesischer Primzahltest)

Ist $n \in \mathbb{N}_+, \ a \in \mathbb{Z}\backslash\{0\}$ und gilt $a^{n-1} \not\equiv 1 \bmod n$, so ist n keine Primzahl.

Gilt dagegen $a^{n-1} \equiv 1 \bmod n$, so nennt man n **pseudoprim** bzgl. a. n braucht dann noch keine Primzahl zu sein, wie folgendes Beispiel von Sarrus zeigt: $341 = 11 \cdot 31$ ist pseudoprim bzgl. 2, denn

$$\begin{aligned} 2^{340} &= (2^{34})^{10} = 1 \bmod 11 \text{ und} \\ 2^{340} &= 2^{11 \cdot 30 + 10} \equiv 2^{10} \\ &\equiv (32)^2 \equiv 1^2 \equiv 1 \bmod 31 \end{aligned}$$

und somit ist

$$2^{340} \equiv 1 \bmod 341.$$

Eine weitere Anwendung des kleinen Fermat ist die Methode von Pollard zur Primfaktorzerlegung.

Beispiel 2.1.22 (Pollards $(p-1)$-Methode)

Es sei $n \in \mathbb{N}_+$ eine zerlegbare Zahl. Ist p ein Primfaktor von n und k ein Vielfaches von $p-1$, so gilt nach dem kleinen Fermat für $a \in \mathbb{N}$ mit $(a, p) = 1$ die Relation $p|(a^k - 1, n)$, denn $a^k = a^{l(p-1)} \equiv 1 \bmod p$. Hat nun n einen Primfaktor $p > 2$ derart, daß $p-1$ relativ kleine Primfaktoren besitzt, so wird $p-1$ für relativ kleines m ein Teiler von $k = \mathrm{kgV}(1, 2, 3, 4, \ldots, m)$ sein. Wir haben dann mit

$$d = (a^k - 1, n)$$

einen echten Teiler von n gefunden, falls n kein Teiler von $a^k - 1$ ist. Diese Beobachtung führt zu einer Methode einen echten Teiler von n zu finden.

n sei eine zerlegbare natürliche Zahl, was man mit einem Primzahltest prüft. Man setzt

$$a = 2,\ b = 1,\ k = 1,\ f = 0.$$

Solange $f = 0$, geht man nun so vor: Es sei

(1) $c = \mathrm{ggT}(a, n)$.

Ist $c \neq 1$, so hat man mit $f = c$ einen echten Faktor von n gefunden.

Ist $c = 1$, so bildet man

(2) $k = \mathrm{kgV}(k, b)$ und

(3) $d = \mathrm{ggT}(a^k - 1, n)$.

Ist $d = 1$, so erhöht man den Wert von b um 1 und beginnt wieder bei (1).

Ist $a < d < n$, so hat man mit $f = d$ einen echten Teiler von n gefunden. Es bleibt der Fall $d = n$.

Dann ist n ein Teiler von $a^k - 1$ und somit auch von $a^{kl} - 1$ für alle $l \in \mathbb{N}_+$.

Deshalb führt das Erhöhen von b nicht weiter. Stattdessen erhöht man in diesem Fall a um 1 und setzt die Werte von b und k auf die Anfangswerte $b = 1,\ k = 1$ zurück. Dann beginnt man wieder bei (1).

Behauptung: Nach endlich vielen Schritten liefert dieses Verfahren einen echten Teiler f von n.

Beweis: Es sei p der kleinste Primfaktor von n. Ist $p = 2$, so ergibt sich am Anfang

$$c = \mathrm{ggT}(a, n) = 2, \text{ weil } a = 2.$$

also $f = c$.

Wir können $p > 2$ annehmen.

Wir numerieren die Schritte des Verfahrens mit $t = 1, 2, \ldots$ Am Anfang ($t = 1$) ist

$$\begin{aligned} &k_1 = 1,\ a_1 = 2,\ b_1 = 1,\ f_1 = 0,\\ &c_1 = \mathrm{ggT}(a_1, n). \end{aligned}$$

Für $t \geq 1$ gilt: Ist $c_t = 1$, so setzt man

$$\begin{aligned} k_{t+1} &= \begin{cases} 1\ , & \text{falls } b_t = 1 \\ \mathrm{kgV}(k_t, b_t)\ , & \text{falls } b_t > 1 \end{cases} \\ d_{t+1} &= \mathrm{ggT}(a_t^{k_{t+1}} - 1, n) \end{aligned}$$

Dann setzt man

$$(a_{t+1}, b_{t+1}) = \begin{cases} (a_t, b_t + 1)\ , & \text{falls } d_{t+1} = 1 \\ (a_t + 1, 1)\ , & \text{falls } d_{t+1} = n \end{cases}$$

Ist $c_t \neq 1$, so ist $f = c_t$ ein Faktor von n. Ist $c_t = 1$ und $c < d_{t+1} < n$, so ist $f = d_{t+1}$ ein Faktor von n.

Die Folge $(a_t, b_t)_{t \geq 1}$ ist streng monoton wachsend bzgl. der lexikographischen Ordnung, denn

$$(a_t \leq a_{t+1} \text{ und } a_t = a_{t+1}) \Longrightarrow b_t < b_{t+1}.$$

Annahme: Die Folge (a_t, b_t) ist für alle $t \geq 1$ definiert, d.h. das Verfahren bricht nicht ab.

Dann gibt es zwei Fälle:

(1) $\forall\, l \in \mathbb{N},\ l \geq 2\ \exists\ t_0$ s.d. $a_{t_0} = l,\ b_{t_0} = 1$.

Insbesondere gilt dies für $l = p + 1$.

$$\begin{aligned} a_{t_0} &= p+1,\ b_{t_0} = 1 \Longrightarrow k_{t_0+1} = 1, \text{ also} \\ d_{t_0+1} &= \mathrm{ggT}((p+1)-1, n) = p. \end{aligned}$$

Damit stoppt das Verfahren hier entgegen der Annahme.

(2) $\exists\ t_0 \forall\, t \geq to : a_t = a_{t_0},\ b_t = (t - t_0) + b_{t_0}$ und $c_t = \mathrm{ggT}(a_t, n) = 1$.

Insbesondere gibt es ein $t \geq t_0$, so daß $(p-1)|b_t$; da $k_{t+1} = \mathrm{kgV}(k_t, b_t)$ folgt $(p-1)|k_{t+1}$. Nach dem kleinen Fermat ist somit $d_{t+1} = \mathrm{ggT}(a_t^{k_{t+1}} - 1, n)$ ein Vielfaches von p, also ist $d_{t+1} > 1$ im Widerspruch zu $a_{t+1} = a_t$.

Damit bricht das Verfahren wie behauptet ab. $\square$

Es ist leicht, ein ***Mathematica*** -Programm für dieses Verfahren zu schreiben. Wir nennen es 'faktor':

```
faktor [n_ Integer?Positive]:=
Module [{a = 2, b = 1, c, k = 1, f = 0},
If [PrimeQ[n] == False,
   While [f == 0,
            c =GCD[a, n];
            If [c == 1,
               k =LCM[k, b];
               d =GCD[PowerMod[a, k, n] - 1, n];
               If [d == 1,
                  b++,
                  If [d == n,
                     a++; b = 1; k = 1,
                     f = d]],
               f = c]],
   f = n];
f]
```

Als Beispiel wählen wir ein Produkt $n = pq$ von zwei Primzahlen. Sind p, q groß, so ist es sehr zeitaufwendig ohne die Kenntnis von p und q das Produkt $n = pq$ zu zerlegen. Für fünfstellige Primzahlen p, q funktioniert das Programm faktor[n] ganz gut, vorausgesetzt $p - 1$ und $q - 1$ haben relativ kleine Primfaktoren.

Aus der Primzahltabelle eratosthenes[100000] oder mit dem Befehl Prime[n], welcher die n-te Primzahl ausgibt, wählen wir zwei Primzahlen, etwa

$$\begin{aligned} p &= 48673 \\ q &= 48751 \end{aligned}$$

und bilden

$$n = pq = 2372857423.$$

Wir erhalten dann

faktor[n]//Timing =
{5.28333 Second, 48673}

Der Grund dafür, daß die Berechnung so schnell geklappt hat, sind die kleinen Primfaktoren von $p-1$ und $q-1$:

$$\begin{aligned} p-1 &= 2^5 \cdot 3^2 \cdot 13^2, \\ q-1 &= 2 \cdot 3 \cdot 5^4 \cdot 13. \end{aligned}$$

Als weitere Anwendung des Eulerschen Satzes erläutern wir das bekannte **RSA-Kryptosystem** (siehe [9]).

Wir beginnen mit einigen Vorbetrachtungen. Um eine Nachricht, die als Textstring gegeben ist, zu verschlüsseln, ersetzt man zunächst alle Buchstaben, Satzzeichen, Zwischenräume (blanks) durch dreistellige Dezimalzahlen. Ein Standardweg ist der **ASCII-Code**.

$$\begin{aligned} \sqcup = \text{ blank } &= 032, \\ A &= 065, \\ a &= 097, \text{ usw.} \end{aligned}$$

Den ASCII-Code von "Leonard Euler" bekommt man in ***Mathematica*** durch

M = "Leonard Euler"; a = ToCharacterCode[M] = {76, 101, 111, 110, 97, 114, 100, 32, 69, 117, 108, 101, 114}.

Jede Nachricht M kann man also zunächst in eine $3k$-stellige Dezimalzahl m verwandeln, wobei k die Anzahl der Zeichen in M ist. Aus m kann man natürlich sofort M zurückgewinnen.

Zum Beispiel ist

$$\begin{aligned} m &= 1000\hat{\ }\text{Length}[a] * \text{ Sum}[a[[i]] * 1000\hat{\ }(-1), \{i, 1, \text{Length}[a]\}] \\ &= 76101111110097114100032069117108101114 \end{aligned}$$

die 39-stellige Dezimalzahl von "Leonard Euler". Man sieht nur 38 Stellen, weil $L = 076$ mit einer Null beginnt, die hier nicht hingeschrieben wird.

Sinnvoller ist es, die Nachricht M zunächst in Blöcke konstanter Länge k zu zerlegen und dann die $3k$-stelligen Zahlen des zugehörigen Zahlentupels zu verschlüsseln.

Eine $3k$-stellige Zahl m kann man eindeutig als eine modulare Zahl in $\mathbb{Z}/n\mathbb{Z}$ auffassen, wenn $n \geq 10^{3k}$ gegeben ist.

Wir wollen das Beispiel $n = 10^{15}$ betrachten. Dann können wir eine 15-stellige Zahl m zu einer neuen 15-stelligen Zahl $V(m)$ verschlüsseln, indem wir einen Exponenten e auswählen und $V(m)$ mit

$$V(m) \equiv m^e \operatorname{mod} 10^{15}, \; 0 \leq V(m) < 10^{15},$$

als Verschlüsselung von m wählen.

Nach dem Eulerschen Satz gilt nun

$$m^{\varphi(10^{15})} \equiv 1 \bmod 10^{15}, \text{ wenn } (m, 10^{15}) = 1$$

gilt, wenn also die letzte Ziffer von m eine der Zahlen 1, 3, 7 oder 9 ist. Es sei dies der Fall. Wie kann man dann $V(m)$ entschlüsseln? Hat man e so gewählt, daß

$$(e, \varphi(10^{15})) = 1,$$

so gibt es ein $i \in \mathbb{N}$, so daß

$$ei \equiv 1 \bmod \varphi(10^{15}).$$

Es folgt $ei = 1 + y\varphi(10^{15})$ mit $y > 0$, also

$$V(m)^i \equiv m^{ei} = m \cdot m^{y\varphi(10^{15})} \equiv m \bmod 10^{15}.$$

Die i-te Potenz modulo 10^{15} gibt also die Zahl m zurück. $E(k)$ mit

$$E(k) \equiv k^i \bmod 10^{15}, \ 0 \leq E(k) < 10^{15},$$

ist also die Entschlüsselungsfunktion. Wichtig ist, daß e zu $\varphi(10^{15})$ teilerfremd ist, und daß die Zahl m, die verschlüsselt werden soll, zu 10^{15} teilerfremd ist.

In unserem Fall können wir leicht ein Beispiel für e finden. Es gilt

$$\begin{aligned}\varphi(10^{15}) &= \varphi(2^{15})\varphi(5^{15}) = 10^{15}\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) \\ &= 4 \cdot 10^{14}.\end{aligned}$$

Wir können zum Beispiel

$$e = 3$$

wählen. $V(m)$ besteht dann aus den letzten 15 Ziffern von m^3. i mit $3i \equiv 1 \bmod \varphi(10^{15})$ bekommen wir einfach durch

$$\begin{aligned}i &= \text{PowerMod}[3, -1, \varphi(10^{15})] \\ &= 266666666666667,\end{aligned}$$

eine ziemlich große Zahl.

Ein Beispiel:

$$\text{Bach} = 66097099104$$

ist nicht teilerfremd zu 10^{15}. Wir hängen eine 1 ans Ende und erhalten

$$\text{Bach'} = 660970991041 = 10 * \text{Bach } + 1,$$

teilerfremd zu 10^{15}.

Es ergibt sich die mit $e = 3$ verschlüsselte Zahl

$$\begin{aligned}V(\text{Bach'}) &= \text{PowerMod}[\text{Bach'}, 3, 10^{15}] \\ &= 338763670681921.\end{aligned}$$

Entschlüsseln geht mit

$$\text{PowerMod}[V(\text{Bach'}), i, 10^{15}] = 660970991041.$$

Obwohl i sehr groß ist, hat das Entschlüsseln geklappt.

Die Idee zur Verschlüsselung ist also:

Man fixiere eine Zahl $n \in \mathbb{N}_+$. Jede Zahl m aus der Menge

$$\mathcal{A} = \{m \mid 0 \leq m < n \text{ und } (m, n) = 1\}$$

kann verschlüsselt werden. Zum Verschlüsseln braucht man einen Exponenten $e \in \mathbb{N}_+$ mit

$$(e, \varphi(n)) = 1.$$

Die Verschlüsselungsfunktion ist dann einfach die e-te Potenz modulo n, also

$$V : \mathcal{A} \longrightarrow \mathcal{A} \text{ mit } V(m) \equiv m^e \bmod n.$$

Zum Verschlüsseln braucht man also den Schlüssel $S = (n, e)$.

Zum Entschlüsseln muß man ein Inverses i von e modulo $\varphi(n)$ bestimmen und erhält die Entschlüsselungsfunktion

$$E : \mathcal{A} \longrightarrow \mathcal{A} \text{ mit } E(m) \equiv m^i \bmod n.$$

Nach dem Satz von Euler gilt in der Tat

$$E(V(m)) = m \quad \text{für alle } m \in \mathcal{A}.$$

Kann man, wenn man nur den Schlüssel

$$S = (n, e)$$

kennt, die Entschlüsselungsfunktion finden?

Wenn man $\varphi(n)$ bestimmen kann, ist es kein Problem. Jedoch ist es aussichtslos $\varphi(n)$ etwa für eine Zahl

$$n = pq,$$

die ein Produkt von sehr großen Primzahlen p und q, $p \neq q$, ist, zu bestimmen, wenn man nur n nicht aber p und q kennt. Es gilt $\varphi(n) = (p-1)(q-1)$. Um eine sichere Verschlüsselungsmethode mit einem allgemein bekannten Schlüssel zu erhalten, kann man also so vorgehen:

Man sucht zwei 'sehr große' (≥ 60 Dezimalstellen) Primzahlen p und q, die man geheim hält. Dann bildet man $n = pq$ und legt eine zu $(p-1)(q-1)$ teilerfremde Zahl e fest.

$$S = (n, e)$$

ist der Schlüssel. Mit Hilfe der geheimen Zahlen p und q findet man ein Inverses i von e modulo $(p-1)(q-1)$. Auch i hält man geheim. Das Paar

$$\widetilde{S} = (n, i)$$

dient zum Entschlüsseln: $x \longmapsto E(x) = x^i \bmod n$. Da man die Primfaktorzerlegung von n nach dem heutigen Stand der Theorie in vertretbarer Zeit nicht bestimmen kann, ist es praktisch unmöglich, aus der Kenntis von (n, e) allein den Entschlüsselungsexponenten i zu bestimmen. Der Schlüssel $S = (n, e)$ kann also ohne die Sicherheit verschlüsselter Daten zu gefährden, veröffentlicht werden. Niemandem wird es gelingen, ohne die Kenntnis der geheimen Zahlen p und q oder der unverschlüsselten Zahl $m < n$, die mit (n, e) verschlüsselte Zahl

$$V(m) = m^e \bmod n$$

zu entschlüsseln.

Diese Verschlüsselungsmethode heißt das **RSA public key crypto-system** nach den Entwicklern Rivest, Shamir, Adleman.

Übungen 2.1.23

(1) Löse die linearen Kongruenzen

(a) $91x \equiv 84 \bmod 143$

(b) $91x \equiv 84 \bmod 147$

(c) $12x + 16y \equiv 6 \bmod 30$.

(2) Bestimme die Erzeuger der additiven Gruppe $(\mathbb{Z}/72\mathbb{Z}, +)$. Ist die Gruppe $(\mathbb{Z}/72\mathbb{Z})^\times$ zyklisch?

(3) Zeige, daß $2222^{5555} + 5555^{2222}$ durch 7 teilbar ist.

(4) Beweise:

(a) $\forall\, a \in \mathbb{Z} : a^{37} \equiv a \bmod 1729$

(b) $\forall\, a \in \mathbb{Z} : a^{13} \equiv a \bmod 2370$

(c) $\forall\, a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod 2 : a^{33} \equiv a \bmod 4080$

(5) Beweise:

(a) $(a, m) = (a - 1, m) = 1 \Longrightarrow 1 + a + a^2 + \cdots + a^{\varphi(m)-1} \equiv 0 \bmod m$.

(b) Jede Primzahl $p \neq 2, 5$ teilt unendlich viele der Zahlen 1, 11, 111, 1111, 11111,....

(6) (a) Es seien $a_1, \ldots, a_k \in \mathbb{Z}$ und $m_1, \ldots, m_k \geq 2$.
Beweise: Das System von Kongruenzen

$$x \equiv a_i \bmod m_i,\ \ i = 1, \ldots, k$$

ist genau dann lösbar, wenn

$$(m_i, m_j) \mid a_i - a_j \text{ für alle } i, j.$$

Zwei Lösungen sind kongruent modulo $\mathrm{kgV}(m_1, \ldots, m_k)$.

(b) Finde die kleinste positive ganze Zahl, die beim Teilen durch 3 bzw. 4,5,6,7 den Rest 1 bzw. 2,3,4,5 läßt.

(7) Löse die simultanen Kongruenzen

a) $x \equiv 3 \bmod 6$	b) $x \equiv 5 \bmod 6$
$x \equiv 5 \bmod 35$	$x \equiv 5 \bmod 12$
$x \equiv 7 \bmod 143$	$x \equiv 19 \bmod 30$
$x \equiv 11 \bmod 323$	

(8) (a) Finde die letzte Ziffer von 7^{139} und 17^{1717}.

(b) Finde die letzten 3 Ziffern von 19^{1603}, 17005^{2020}.

(9) Finde die Primfaktorzerlegung von

(a) 93891391424101

(b) 418907

(c) 2955756227

(10) Für welche $a \in \{1, \ldots, 14\}$ ist $\{a, a^2, \ldots, a^{14}\}$ ein primes Restsystem modulo 15?

(11) Für ***Mathematica*** -Fans:

(a) Schreibe ein Programm zum RSA-Kryptosystem.

(b) Verschlüssle den Namen "Heitor Villa Lobos" mit dem Schlüssel (n, e), wobei

$$n = 1518950245613,$$
$$e = 1234567.$$

Die Zahl $V(m) = 974990529047$ sei die Verschlüsselung von m mit (n, e). Bestimme m.

(c) Wie findet man große Primzahlen?

(12) Für ***Mathematica*** -Fans

Schreibe ein Programm zum Lösen simultaner Kongruenzen.

2.2 Nicht-lineare Kongruenzen, p-adische Zahlen

Ist R ein kommutativer Ring mit Eins, so bezeichnen wir mit $R[x]$ den Polynomenring der Polynome in der Unbestimmten x und mit Koeffizienten in R.

Ein Polynom $f \in R[x]$ vom Grad $\leq n$ ist durch die Koeffizientenfolge $(a_n, a_{n-1}, \dots, a_0)$ mit

$$f = a_n x^n + \cdots + a_1 x + a_0$$

festgelegt. a_i ist der Koeffizient vor x^i. Die Gleichheit von Polynomen prüft man durch Koeffizientenvergleich.

Sind $x_1, \dots, x_n$ Unbestimmte, $n \geq 2$, so wird der Polynomenring $R[x_1, \dots, x_n]$ der Polynome in den Unbestimmten $x_1, \dots, x_n$ induktiv definiert durch

$$R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n].$$

Man sieht leicht, daß jedes Polynom $f \in R[x_1, \dots, x_n]$ in folgender Form geschrieben werden kann:

$$f = \sum_{\substack{\nu_1, \dots, \nu_n \geq 0 \\ \nu_1 + \cdots + \nu_n \leq d}} a_{\nu_1 \dots \nu_n} x_n \, x_1^{\nu_1} \dots x_n^{\nu_n},$$

wobei $a_{\nu_1, \dots, \nu_n} \in R$ und $d \in \mathbb{N}$ geeignet. Die Folge $(a_{\nu_1, \dots, \nu_n})_{\nu_i \geq 0}$ heißt die Koeffizientenfolge von f. $a_{\nu_1, \dots, \nu_n}$ ist der Koeffizient vor dem Monom $x_1^{\nu_1} \dots x_n^{\nu_n}$. f heißt Polynom vom Grad $\leq d$, wenn $a_{\nu_1, \dots, \nu_n} = 0$ für alle $(\nu_1, \dots, \nu_n) \in \mathbb{N}^n$ mit $\nu_1 + \cdots + \nu_n > d$.

Die Theorie der diophantischen Gleichungen beschäftigt sich mit der Frage nach den ganzzahligen Lösungen $(x_1, \dots, x_n) \in \mathbb{Z}^n$ eines Systems von Polynomgleichungen

$$(1) \qquad \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_k(x_1, \dots, x_n) = 0, \end{cases}$$

wobei $f_1, \dots, f_k \in \mathbb{Z}[x_1, \dots, x_n]$.

Dieses Problem stellt sich als sehr schwierig heraus. Deshalb betrachtet man an Stelle des Gleichungssystems (1) zunächst das System von Kongruenzen

$$(2) \qquad \begin{cases} f_1(x_1, \dots, x_n) \equiv 0 \bmod m \\ \vdots \\ f_k(x_1, \dots, x_n) \equiv 0 \bmod m, \end{cases}$$

wobei $m \in \mathbb{N}$, $m \geq 2$, eine vorgegebene Zahl ist.

Ist $(x_1, \dots, x_n) \in \mathbb{Z}^n$ eine Lösung des Systems (2) und ist $(y_1, \dots, y_n) \in \mathbb{Z}^n$ mit

$$x_i \equiv y_i \bmod m \text{ für } i = 1, \dots, n,$$

so ist auch $(y_1, \dots, y_n)$ eine Lösung von (2).

Man braucht also nur Lösungen in der endlichen Menge M^n zu suchen, wobei $M \subset \mathbb{Z}$ ein vollständiges Restsystem modulo m ist. Sind m und n klein, so kann man einfach alle Elemente $x \in M$ in die Polynome $f_1, \dots, f_k$ einsetzen und prüfen, ob

$$f_1(x) \equiv \ldots \equiv f_k(x) \equiv 0 \bmod m.$$

gilt.

Beispiel 2.2.1

(1) Es sei

$$f = x^{12} + x^{10} - x^4 + x^2 - 1.$$

Um $f(x) \equiv 0 \bmod 7$ zu lösen, vereinfacht man die Kongruenz mit dem kleinen Fermat ($x^7 \equiv x \bmod 7$ für alle $x \in \mathbb{Z}$) zu

$$x^6 + x^4 - x^4 + x^2 - 1 \equiv 0 \bmod 7,$$

also

$$x^6 + x^2 - 1 \equiv 0 \bmod 7.$$

Da $x \equiv 0$ keine Lösung ist und für $x \not\equiv 0 \bmod 7$ nach dem kleinen Fermat $x^6 - 1 \equiv 0 \bmod 7$ gilt, hat das Polynom f keine Nullstellen modulo 7.

(2) Betrachten wir das Polynom

$$f = x^5 - x^4 + 3x^3 + 2x^2 - x^1 + 6,$$

so kann man den kleinen Fermat nicht anwenden, um $f(x) \equiv 0 \bmod 7$ zu vereinfachen. Jetzt macht man einfach eine Wertetabelle

x	$f(x)$ mod 7
-3	0 mod 7
-2	0 mod 7
-1	-3 mod 7
0	-1 mod 7
1	3 mod 7
2	-3 mod 7
3	-2 mod 7

Die Werte $f(x)$ bestimmt man dabei am bequemsten mit dem Hornerschema (siehe [7]).

$$\begin{aligned} y_0 &\equiv 1 \bmod 7, \\ y_1 &\equiv x\,y_0 - 1 \bmod 7, \\ y_2 &\equiv x\,y_1 + 3 \bmod 7, \\ y_3 &\equiv x\,y_2 + 2 \bmod 7, \\ y_4 &\equiv x\,y_3 - 1 \bmod 7, \\ f(x) \equiv y_5 &\equiv x\,y_4 + 6 \bmod 7. \end{aligned}$$

Für $x = -3$ ergibt sich

$$\begin{aligned} y_0 &\equiv 1, \\ y_1 &\equiv -4 \equiv 3, \\ y_2 &\equiv -9 + 3 \equiv 1, \\ y_3 &\equiv -3 + 2 \equiv -1, \\ y_4 &\equiv 3 - 1 \equiv 2, \\ f(-3) \equiv y_5 &\equiv -6 + 6 \equiv 0. \end{aligned}$$

Natürlich geht es am schnellsten mit dem Computer. In unserem Beispiel geht es so:

$$f[x\_] := x\hat{}5 - x\hat{}4 + 3x\hat{}3 + 2x\hat{}2 - x + 6x\hat{}0;$$
$$\mathrm{Table}[\{x,\ f[q[x,7]]\},\ \{x,-3,3\}]$$

Dabei haben wir die modulare Zahl $q[x,7]$ benutzt. Da wir Potenzieren und Multiplikation mit ganzen Zahlen in Beispiel 2.1.6 definiert haben, kann man $q[x,7]$ in das Polynom f einsetzen. $f(x) \equiv 0 \bmod 7$ hat also zwei inkongruente Lösungen modulo 7.

Definition 2.2.2 Es sei

$$\sum_{\substack{\nu_1,\dots,\nu_n \geq 0\\ \nu_1+\cdots+\nu_n \leq d}} a_{\nu_1,\dots,\nu_n} x_1^{\nu_1} \dots x_n^{\nu_n} \in \mathbb{Z}[x_1,\dots,x_n]$$

ein Polynom vom Grad $\leq d$. Weiter sei $m \in \mathbb{N}$, $m \geq 2$. Die **Reduktion von** f **modulo** m, wird dann definiert durch

$$\mathrm{red}_{\,m}(f) := \sum_{\substack{\nu_1,\dots,\nu_n \geq 0\\ \nu_1+\cdots+\nu_n \leq d}} [a_{\nu_1} \dots \nu_n]_m \, x_1^{\nu_1} \dots x_n^{\nu_n}.$$

Es gilt $\mathrm{red}_m(f) \in \mathbb{Z}/m\mathbb{Z}[x_1,\dots,x_n]$.

Beispiel 2.2.3 Sei $f = 5x^4 + 4x^3 + 7x^2 + 20$.

$$\mathrm{red}_{\,2}(f) = x^4 + x^2 \in \mathbb{F}_2[x],$$
$$\mathrm{red}_{\,3}(f) = [5]_3\, x^4 + [4]_3\, x^3 + [7]_3\, x^2 + [20]_3$$

Beschreibt man die Elemente von $\mathbb{Z}/3\mathbb{Z}$ durch die absolut kleinsten Reste $-1, 0, 1$, so erhält man

$$\mathrm{red}_{\,3}(f) = -x^4 + x^3 + x^2 - 1 \in \mathbb{F}_3[x].$$

Schließlich ist

$$\mathrm{red}_{\,5}(f) = -x^3 + 2x^2 \in \mathbb{F}_5[x],\ \mathrm{red}_{\,140}(f) = 0.$$

Definition 2.2.4 Seien $f_1,\dots,f_k \in \mathbb{Z}[x_1,\dots,x_n]$. Mit $V_m(f_1,\dots,f_k)$ bezeichnen wir die Menge aller n-Tupel $(x_1,\dots,x_n) \in (\mathbb{Z}/m\mathbb{Z})^n$ mit $f_1(x_1,\dots,x_n) = \dots = f_k(x_1,\dots,x_n) = 0$ in $\mathbb{Z}/m\mathbb{Z}$.
Sind $a_1,\dots,a_n \in \mathbb{Z}$ Repräsentanten von $x_1,\dots,x_n$, so bedeutet das

$$f_1(a_1,\dots,a_n) \equiv \dots \equiv f_k(a_1,\dots,a_n) \equiv 0 \bmod m.$$

Ist allgemeiner R irgendein kommutativer Ring mit Eins, so wird mit

$$V_R(f_1,\dots,f_k)$$

das Nullstellengebilde von $f_1,\dots,f_k$ über R bezeichnet.

$$x \in V_R(f_1,\dots,f_k) \Longleftrightarrow x \in R^n \text{ und } f_1(x) = \dots = f_k(x) = 0.$$

In diesem Sinne ist

$$V_m(f_1,\dots,f_k) = V_{\mathbb{Z}/m\mathbb{Z}}(f_1,\dots,f_k).$$

Trivialerweise gilt

Lemma 2.2.5 Sei $f = (f_1, \dots, f_k)$, $f_i \in \mathbb{Z}[x_1, \dots, x_n]$ und $\varphi : R \to S$ ein Ringhomomorphismus. Dann induziert φ eine Abbildung

$$\varphi_* : V_R(f) \longrightarrow V_S(f)$$

mit

$$\varphi_*(x_1, \dots, x_n) = (\varphi(x_1), \dots, \varphi(x_n)).$$

Ist $\psi : S \to T$ ein weiterer Ringhomomorphismus, so gilt

$$(\psi \circ \varphi)_* = \psi_* \circ \varphi_*.$$

Außerdem ist $(id_R)_* = id_{V_R(f)}$. Man sagt daher: $R \longmapsto V_R(f)$ ist ein Funktor $V(f)$ von der Kategorie der kommutativen Ringe mit Eins in die Kategorie der Mengen. Die Elemente von $V_R(f)$ heißen auch R-wertige Punkte von $V(f)$. Für die Zahlentheorie ist nun die Frage interessant, ob

$$V_{\mathbb{Z}}(f) \neq \emptyset$$

und wenn ja, welche Struktur die Menge $V_{\mathbb{Z}}(f)$ besitzt.
In unmittelbarem Zusammenhang damit steht die Frage nach der Existenz von rationalen Punkten:

$$\text{Ist } V_{\mathbb{Q}}(f) \neq \emptyset?$$

Zunächst befassen wir uns mit $V_{\mathbb{Z}/m\mathbb{Z}}(f)$. Aus dem chinesischen Restsatz folgt

Lemma 2.2.6 Es sei $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ die kanonische Primfaktorzerlegung von m. Dann gilt: Der Ringisomorphismus

$$\Phi : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{\alpha_r}\mathbb{Z}$$

induziert eine Bijektion

$$\Phi_* : V_m(f) \longrightarrow V_{p_1^{\alpha_1}}(f) \times \dots \times V_{p_r^{\alpha_r}}(f).$$

Beweis: Ist $R = R_1 \times \dots \times R_r$, so gilt

$$V_R(f) = V_{R_1}(f) \times \dots \times V_{R_r}(f)$$

$\square$

Durch dieses Lemma ist das Lösen von Kongruenzen modulo m auf den Fall der Primzahlpotenzen $m = p^\alpha$ reduziert.
Insbesondere ist

$$a_f : \mathbb{N}_+ \longrightarrow \mathbb{N}$$

mit $a_f := \#V_m(f)$ eine multiplikative Funktion:

$$a_f(m) = \prod_{i=1}^r a_f(p_i^{\alpha_i}), \text{ für } m = \prod_{i=1}^r p_i^{\alpha_i}.$$

Wir beginnen mit den Primzahlen selbst.
Da $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper ist, sind wir auf dem vertrauten Gebiet der Polynome mit Koeffizienten in einem Körper K. Die Polynome $f_1, \dots, f_k \in \mathbb{Z}[x_1 \dots x_n]$ kann man mit Hilfe der Reduktionsabbildung $\mathbb{Z} \longrightarrow K$, $n \longmapsto n \cdot 1_k$, welche im Fall $K = \mathbb{F}_p$ nichts anderes als die Restklassenabbildung $n \longmapsto n \bmod p$ ist, als Polynome

$$\mathrm{red}(f_1), \dots \mathrm{red}(f_k) \in K[x_1, \dots, x_n]$$

auffassen.

$$V_K(f) \subset K^n$$

ist das Nullstellengebilde dieser Polynome im n-dimensionalen Zahlenraum K^n. Ist $K = \mathbb{F}_p$, so ist K^n endlich und besitzt p^n Elemente.
Bekanntlich gilt

Lemma 2.2.7 Es sei K ein Körper und

$$f = a_n x^n + \cdots + a_1 x + a_0 \in K[x]$$

ein Polynom vom Grad n (also $a_n \neq 0$). Dann gilt

a) Für $c \in K$ gilt:

$$f(c) = 0 \Longleftrightarrow \exists\, q \in K[x] : f = (x - c) \cdot q.$$

b) f besitzt höchstens n Nullstellen.

Beweis:
zu a) Wir wählen einen "brutalen" Beweis. Sei $x = y + c$. Dann ist

$$\begin{aligned}
f(x) = f(y+c) = \sum_{k=0}^{n} a_k (y+c)^k &= \sum_{n \geq k \geq m \geq 0} a_k \binom{k}{m} c^{k-m} y^m \\
&= \sum_{m=0}^{n} \left(\sum_{k=m}^{n} a_k \binom{k}{m} c^{k-m} \right) y^m \\
&= f(c) + \left(\sum_{m=1}^{n} \sum_{k=m}^{n} a_k \binom{k}{m} c^{k-m} y^{m-1} \right) \cdot y \\
&= f(c) + q(x) \cdot (x - c),
\end{aligned}$$

also $f(c) = 0 \Longleftrightarrow f = (x - c) \cdot q$.
Eleganter ist natürlich der Beweis mit Hilfe des Divisionsalgorithmus in $K[x]$.
Analog zu 1.1 beweist man (Übung) den folgenden Divisionsalgorithmus:

$$\forall\, a, b \in K[x],\ b \neq 0\ \exists!\, q, r \in K[x],$$

so daß

$$a = qb + r \text{ und } r = 0 \text{ oder } \operatorname{grad} r < \operatorname{grad} b$$

(siehe [6]).
Jetzt ergibt also Teilen von f durch $(x-c)$ die Darstellung

$$f = q \cdot (x-c) + r \text{ mit } r = 0 \text{ oder grad } r = 0.$$

Es gilt offensichtlich, wie man durch Einsetzen von $x = c$ erkennt,

$$f(c) = r.$$

□

zu b) Sind $c_1, \ldots, c_m \in K$ Nullstellen von f, so gilt $f = (x-c_1) \cdot \ldots \cdot (x-c_m) \cdot q$, also $n = m +$ grad $q \geq m$. □

Beispiel 2.2.8

(1) Sei p eine Primzahl. Nach dem kleinen Fermat hat $f = x^p - x \in \mathbb{Z}[x]$ alle Elemente von $\mathbb{F}_p$ als Nullstellen:

$$V_p(f) = \mathbb{F}_p.$$

Es gilt also die Gleichung

$$x^p - x = \prod_{c=0}^{p-1}(x-c) \text{ in } \mathbb{F}_p[x].$$

Man beachte: $x^p - x$ ist ein von Null verschiedenes Polynom in $\mathbb{F}_p[x]$, grad $(x^p - x) = p$. Aber die durch $x^p - x$ definierte Funktion

$$\mathbb{F}_p \longrightarrow \mathbb{F}_p,\ c \longmapsto c^p - c,$$

ist die Nullfunktion.

(2) Wir wollen sehen, daß ein Polynom $f \in R[x]$ vom Grad d mit Koeffizienten in einem Ring mehr als d Nullstellen haben kann. Das wohl einfachste Beispiel ist

$$f = x^2 - 1 \text{ als Polynom in } \mathbb{Z}/8\mathbb{Z}[x].$$

f hat die vier verschiedenen Nullstellen

$$\pm 1,\ \pm 1 + 4 \text{ modulo } 8.$$

Diese vier Lösungen modulo 8 sind modulo 2 untereinander gleich. Als Polynom in $\mathbb{Z}/2\mathbb{Z}[x]$ gilt ja auch

$$x^2 - 1 = (x-1)^2.$$

1 mod 2 ist also eine doppelte Nullstelle.

(3) Nicht jedes Polynom $f \in \mathbb{F}_p[x]$ vom Grad größer als Null hat Nullstellen in $\mathbb{F}_p$. Zum Beispiel gilt $0^2 \equiv 0,\ 1^2 \equiv 1,\ 2^2 \equiv 1 \bmod 3$, also hat x^2+1 keine Nullstelle in $\mathbb{F}_3$.

Wir beschreiben jetzt ein Lösungsverfahren für nichtlineare Kongruenzen

$$f(x) \equiv 0 \bmod p^\alpha.$$

Zunächst bestimmt man die Lösungen von

$$f(x) \equiv 0 \bmod p$$

und steigt dann sukzessive zu den Potenzen $p^2, p^3, \ldots, p^{\alpha-1}, p^\alpha$ auf.
Ist schon ein $c \in \mathbb{Z}$ mit

$$f(c) \equiv 0 \bmod p^{\alpha-1},\ 0 \leq c < p^{\alpha-1},$$

gefunden, so sucht man $d \in \mathbb{Z}$ mit

$$f(d) \equiv 0 \bmod p^\alpha,\ 0 \leq d < p^\alpha \text{ und } d \equiv c \bmod p^{\alpha-1}.$$

Letztere Bedingung bedeutet:

$$d = c + tp^{\alpha-1} \text{ für ein } t \in \mathbb{Z}, 0 \leq t < p.$$

Es ist also t zu bestimmen, so daß

$$f(c + tp^{\alpha-1}) \equiv 0 \bmod p^\alpha.$$

Dazu berechnen wir $f(c+tp^{\alpha-1})$ mit Hilfe der Taylorentwicklung um den Punkt c:

$$\begin{aligned} f(c + tp^{\alpha-1}) &= f(c) + f'(c)tp^{\alpha-1} + \frac{f''(c)}{2}t^2p^{2\alpha-2} + \cdots \\ &\equiv f(c) + f'(c)tp^{\alpha-1} \bmod p^\alpha. \end{aligned}$$

Also gilt

$$\begin{aligned} & f(c + tp^{\alpha-1}) \equiv 0 \bmod p^\alpha \Longleftrightarrow \\ (*) \qquad & f(c) + f'(c)tp^{\alpha-1} \equiv 0 \bmod p^\alpha. \end{aligned}$$

Da schon $f(c) \equiv 0 \bmod p^{\alpha-1}$ gilt, folgt

$$\frac{f(c)}{p^{\alpha-1}} \in \mathbb{Z},$$

und die Kongruenz $(*)$ ist äquivalent zu der linearen Kongruenz

$$(**) \qquad \frac{f(c)}{p^{\alpha-1}} + f'(c)t \equiv 0 \bmod p.$$

Damit folgt

Lemma 2.2.9 Es sei p Primzahl und $\alpha \geq 2$, $f \in \mathbb{Z}[x]$ und $c \in \mathbb{Z}$ sei Lösung der Kongruenz

$$f(x) \equiv 0 \bmod p^{\alpha-1}.$$

Ist $f'(c) \not\equiv 0 \bmod p$, so gibt es modulo p^α genau ein $d \in \mathbb{Z}$ mit $f(d) \equiv \bmod p^\alpha$ und $d \equiv c \bmod p^{\alpha-1}$. Ist $f'(c) \equiv 0 \bmod p$, so sind entweder alle Zahlen $d \in \mathbb{Z}$ mit $d \equiv c \bmod p^{\alpha-1}$ Lösungen von $f(x) \equiv 0 \bmod p^\alpha$ oder es gibt kein $d \equiv c \bmod p^{\alpha-1}$ mit $f(d) \equiv 0 \bmod p^\alpha$.

Beweis: Die Kongruenz $(**)$ ist genau dann eindeutig modulo p nach t auflösbar, wenn $f'(c) \not\equiv 0 \bmod p$. Ist $f'(c) \equiv 0 \bmod p$, so sind entweder alle t oder kein t Lösung von $(**)$ je nachdem ob $f(c) \equiv 0 \bmod p^\alpha$ oder $f(c) \not\equiv 0 \bmod p^\alpha$. □

Definition 2.2.10 $f \in \mathbb{Z}[x]$ heißt **unverzweigt** in $c \bmod p$, wenn $f'(c) \not\equiv 0 \bmod p$ gilt.

Korollar 2.2.11 (Henselsches Lemma)
Sei $f \in \mathbb{Z}[x]$, p Primzahl, und $c \in \mathbb{Z}$ sei eine Nullstelle von f modulo p, d.h.

$$f(c) \equiv 0 \bmod p.$$

f sei unverzweigt in c modulo p. Dann gibt es zu jedem $\alpha \geq 1$ eine ganze Zahl $c_\alpha \in \mathbb{Z}$, so daß

$$f(c_\alpha) \equiv 0 \bmod p^\alpha$$

und

$$c_\alpha \equiv c \bmod p.$$

c_α ist modulo p^α eindeutig bestimmt, und es gilt $c_\alpha \equiv c_{\alpha-1} \bmod p^{\alpha-1}$ für alle $\alpha \geq 2$.

Beweis: Zur Eindeutigkeit: Seien $c_\alpha,\ c'_\alpha \in \mathbb{Z}$ mit $f(c_\alpha) \equiv f(c'_\alpha) \equiv 0 \bmod p^\alpha$ und $c_\alpha \equiv c'_\alpha \bmod p$.
Behauptung: $c_\alpha \equiv c'_\alpha \bmod p^\alpha$.
Dies zeigen wir durch Induktion nach α.
Für $\alpha = 1$ ist nichts zu zeigen.
$\alpha - 1 \to \alpha$: Aus $f(c_\alpha) \equiv f(c'_\alpha) \equiv 0 \bmod p^\alpha$ folgt auch $f(c_\alpha) \equiv f(c'_\alpha) \bmod p^{\alpha-1}$. Nach Induktionsvoraussetzung folgt $c_\alpha \equiv c'_\alpha \bmod p^{\alpha-1}$, und nach Lemma 2.2.9 folgt somit $c_\alpha \equiv c'_\alpha \bmod p^\alpha$. □

Beispiel 2.2.12 Es sei $f = x^3 - 2x^2 + 3x + 9 \in \mathbb{Z}[x]$ und $p = 3$. Dann ist

$$\mathrm{red}_3 f = x^3 - 2x = x^2(x+1) \in \mathbb{F}_3[x].$$

Also ist 2 eine einfache Nullstelle von f modulo 3. Nach dem Henselschen Lemma gibt es eine Folge $(c_\alpha)_{\alpha \in \mathbb{N}_+}$ von ganzen Zahlen $c_\alpha \in \mathbb{Z}$ mit

$$\begin{aligned} c_1 &= 2 \\ c_\alpha &\equiv c_{\alpha-1} \bmod 3^{\alpha-1} \text{ für } \alpha \geq 2 \\ \text{und } f(c_\alpha) &\equiv 0 \bmod 3^\alpha \text{ für alle } \alpha \geq 1. \end{aligned}$$

c_α wird sukzessive berechnet:
(1) $\qquad c_\alpha = c_{\alpha-1} + t_{\alpha-1} 3^{\alpha-1},\ t_\alpha \in \{0,1,2\},$
wobei $t_{\alpha-1}$ die Lösung der linearen Kongruenz

$$\frac{f(c_{\alpha-1})}{3^{\alpha-1}} + f'(2) t_{\alpha-1} \equiv 0 \bmod 3$$

ist. Da $f'(2) = \mathrm{red}_3\, f'(2) = 4 \equiv 1 \bmod 3$, folgt

(2) $$t_{\alpha-1} \equiv -\frac{f(c_{\alpha-1})}{3^{\alpha-1}} \bmod 3.$$

Wegen (1) gilt

(3) $$c_\alpha \equiv c_{\alpha-1} - f(c_{\alpha-1}) \bmod 3^\alpha.$$

Mit $c_1 = 2$ beginnend erhält man aus (3)

$$c_2 = c_1 - f(c_1) = 2 - f(2) = 2 - 15 = -13 \equiv 5 \bmod 9, \text{ also } c_2 = 5$$

usw. c_α hat wegen (1) die 3-adische Darstellung

$$c_\alpha = t_0 + t_1 3 + \cdots + t_{\alpha-1} 3^{\alpha-1} = (t_{\alpha-1} t_{\alpha-2} \ldots t_1 t_0)_3$$

wobei $t_0 = c_1$ gesetzt wird.

$$c_\alpha \equiv c_{\alpha-1} \bmod p^{\alpha-1}$$

bedeutet nun gerade, daß c_α und $c_{\alpha-1}$ in den letzten α Ziffern der 3-adischen Darstellung übereinstimmen.

Beim "Aufstieg" von $c_{\alpha-1}$ nach c_α erhält man also eine neue erste Ziffer in der 3-adischen Darstellung

$$c_{\alpha-1} = (t_{\alpha-2} \ldots t_0)_3 \rightsquigarrow c_\alpha = (\underset{\substack{\uparrow \\ \text{neue Ziffer}}}{t_{\alpha-1}} \quad t_{\alpha-2} \ldots t_0)_3$$

Die Folge $a = (c_\alpha \bmod 3^\alpha)_{\alpha \geq 1}$ ist ein Beispiel einer 3-adischen ganzen Zahl. a kann man als Nullstelle von f ansehen.

$$f(a) = 0$$

soll dabei heißen, daß $f(c_\alpha) \equiv 0 \bmod 3^\alpha \quad \forall\ \alpha \geq 1$.

Definition 2.2.13 Es sei p eine Primzahl. Für $\alpha \geq 2$ sei $\rho_\alpha : \mathbb{Z}/p^\alpha\mathbb{Z} \longrightarrow \mathbb{Z}/p^{\alpha-1}\mathbb{Z}$ die kanonische surjektive Abbildung mit

$$\rho_\alpha(c \bmod p^\alpha) = c \bmod p^{\alpha-1}.$$

Eine **ganze p-adische Zahl** a ist eine Folge $a = (a_\alpha)_{\alpha\geq 1}$ von Restklassen $a_\alpha \in \mathbb{Z}/p^\alpha\mathbb{Z}$ mit der Eigenschaft

$$\rho_\alpha(a_\alpha) = a_{\alpha-1} \quad \forall\ \alpha \geq 2.$$

Mit $\mathbb{Z}_p$ bezeichnen wir die Menge aller ganzen p-adischen Zahlen.
Sind $a = (a_\alpha),\ b = (b_\alpha) \in \mathbb{Z}_p$, so definieren wir

$$a + b := (a_\alpha + b_\alpha),$$
$$ab := (a_\alpha b_\alpha).$$

Da ρ_α ein Ringhomomorphismus ist, gilt

$$a + b,\ ab \in \mathbb{Z}_p.$$

Man sieht leicht:

$(\mathbb{Z}_p, +, \cdot)$ ist ein kommutativer Ring mit Eins.

$1 = (1, 1, \dots)$ ist das Einselement, und
$0 = (0, 0, \dots)$ ist das Nullelement in $\mathbb{Z}_p$.
$\mathbb{Z}_p$ heißt der **Ring der ganzen p-adischen Zahlen**.

Lemma 2.2.14 (p-adische Entwicklung)
Zu jeder ganzen p-adischen Zahl $a = (a_\alpha) \in \mathbb{Z}_p$ gibt es eine eindeutig bestimmte Ziffernfolge

$$(t_\alpha)_{\alpha\in\mathbb{N}} \text{ von 'Ziffern' } t_\alpha \in \{0, 1, \dots, p-1\},$$

so daß

$$a_\alpha = \left(\sum_{\nu=0}^{\alpha-1} t_\nu p^\nu\right) \bmod p^\alpha \text{ für alle } \alpha \geq 1.$$

Die natürliche Zahl $c_\alpha = \sum\limits_{\nu=0}^{\alpha-1} t_\nu p^\nu = (t_{\alpha-1}t_{\alpha-2}\dots t_0)_p$ ist der Repräsentant von a_α im kleinsten positiven Restsystem modulo p^α.
Die Ziffernfolge (t_α), die man traditionell auch in der Form

$$(\dots t_\alpha t_{\alpha-1}\dots t_1 t_0)_p$$

schreibt, heißt die **p-adische Entwicklung** von a. Suggestiver ist die Schreibweise $a = \sum\limits_{\nu=0}^{\infty} t_\nu p^\nu$. a_α (oder auch c_α) heißt die **Approximation der Ordnung** α von a.
Die Abbildung

$$\mathbb{Z}_p \longrightarrow \{(t_\alpha)_{\alpha\in\mathbb{N}} \mid t_\alpha \in \{0, 1, \dots, p-1\}\}$$

ist bijektiv. □

Lemma 2.2.15 Sei p eine Primzahl.

(1) Die Abbildung

$$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_p$$

mit

$$\varphi(n) = (n \bmod p^\alpha)_{\alpha\geq 1}$$

ist ein injektiver Ringhomomorphismus.

(2) $\mathbb{Z}_p$ ist nullteilerfrei.

Beweis:

(1) Da die Restklassenabbildungen $\mathbb{Z} \longrightarrow \mathbb{Z}/p^\alpha\mathbb{Z}$ Ringhomomorphismen sind, ist φ ein Ringhomomorphismus. Ist nun $\varphi(n) = 0$, so ist n durch alle Potenzen von p teilbar, und somit gilt $n = 0$. Folglich ist φ injektiv.

(2) Seien $a, b \in \mathbb{Z}_p$, und es gelte

$$ab = 0,\ b \neq 0.$$

Es sei

$$a_\alpha = \left(\sum_{\nu=0}^{\alpha-1} t_\nu p^\nu\right) \bmod p^\alpha,\ 0 \le t_\nu < p,$$
$$b_\alpha = \left(\sum_{\nu=0}^{\alpha-1} s_\nu p^\nu\right) \bmod p^\alpha,\ 0 \le s_\nu < p.$$

Da $b \neq 0$, gibt es ein $k \ge 0$, so daß

$$s_0 = \ldots = s_{k-1} = 0,\ s_k \neq 0.$$

$ab = 0$ bedeutet nach Definition der Multiplikation

$$\left(\sum_{\nu=0}^{\alpha-1} t_\nu p^\nu\right)\left(\sum_{\nu=0}^{\alpha-1} s_\nu p^\nu\right) \equiv 0 \bmod p^\alpha \quad \forall\ \alpha \ge 1.$$

Insbesondere ist für $\alpha = k+1$

$$0 \equiv \left(\sum_{\nu=0}^{k} t_\nu p^\nu\right) s_k p^k \equiv t_0 s_k p^k \bmod p^{k+1},$$

also $0 \equiv t_0 s_k \bmod p$. Da $t_0, s_k \in \{0, \ldots, p-1\}$ und $s_k \neq 0$, folgt $t_0 = 0$.
Sei nun schon $t_0 = \ldots = t_{m-1} = 0$ gezeigt. Dann folgt aus $a_{k+m+1} b_{k+m+1} = 0$ die Kongruenz

$$0 \equiv \left(\sum_{\nu=m}^{k+m} t_\nu p^\nu\right)\left(\sum_{\nu=k}^{k+m} s_\nu p^\nu\right) \equiv t_m p^m s_k p^k \bmod p^{k+m+1},$$

also $t_m s_k \equiv 0 \bmod p$ und somit $t_m = 0$.
Induktiv hat sich also $t_\alpha = 0 \quad \forall\ \alpha \ge 0$ ergeben, d.h. $a = 0$. □
Im Ring $\mathbb{Z}_p$ (anders als in $\mathbb{Z}/p^\alpha\mathbb{Z}$) gilt also die Kürzungsregel:

$$ab = a'b,\ b \neq 0 \Longrightarrow a = a'.$$

Definition 2.2.16 Die Einheiten in $\mathbb{Z}_p$ heißen p-adische Einheiten.

Lemma 2.2.17 Sei $a = (a_\alpha)_{\alpha \ge 1} \in \mathbb{Z}_p$.
Folgende Aussagen sind äquivalent:

(1) a ist p-adische Einheit

(2) $a_1 \neq 0$ in $\mathbb{F}_p$

(3) $p \nmid a$, d.h. $\nexists\ b \in \mathbb{Z}_p : a = pb$.

Beweis: (1) $\Longrightarrow$ (2): $a \in \mathbb{Z}_p^\times \Longrightarrow \exists\, b \in \mathbb{Z}_p$, so daß $ab = 1 \Longrightarrow a_1 b_1 = 1 \Longrightarrow a_1 \neq 0$.
(2) $\Longrightarrow$ (1): Sei $a_1 \neq 0 \Longrightarrow \exists\, \beta \in \mathbb{F}_p$ mit $a_1\beta = 1$. Nach dem Henselschen Lemma für $\mathbb{Z}_p$ (siehe 2.2.18) angewandt auf das Polynom $f = ax - 1 \in \mathbb{Z}_p[x]$ gibt es ein $b \in \mathbb{Z}_p$ mit $ab = 1$ und $b_1 = \beta$.
(2) $\Longleftrightarrow$ (3) gilt weil $a_1 = 0 \Longleftrightarrow p|a$. $\square$
Sei $q : \mathbb{Z}_p \Longrightarrow \mathbb{F}_p$ die Projektion

$$q((a_\alpha)_{\alpha \geq 1}) := a_1.$$

Dann ist q surjektiver Ringhomomorphismus mit $\ker q = p\mathbb{Z}_p = \{pb \mid b \in \mathbb{Z}_p\}$ und $\mathbb{Z}_p^\times = q^{-1}(\mathbb{F}_p^\times)$, $\mathbb{F}_p^\times = \{1, 2, \ldots, p-1\}$.
Eine p-adische Entwicklung

$$\sum_{\nu=0}^{\infty} t_\nu p^\nu, \quad t_\nu \in \{0, \ldots, p-1\},$$

beschreibt genau dann eine p-adische Einheit, wenn $t_0 \neq 0$ gilt.
Die Abbildung $q : \mathbb{Z}_p \longrightarrow \mathbb{F}_p$ induziert einen Homomorphismus von Polynomenringen

$$\mathrm{red}_p : \mathbb{Z}_p[x] \Longrightarrow \mathbb{F}_p[x]$$

mit

$$\mathrm{red}_p\left(\sum_{\nu=0}^{m} a_\nu x^\nu\right) = \sum_{\nu=0}^{m} a_{\nu,1} x^\nu,$$

wobei $a_\nu = (a_{\nu,\alpha})_{\alpha \geq 1} \in \mathbb{Z}_p$ für $\nu = 0, \ldots, m$. Genauso induziert $q : \mathbb{Z}_p \longrightarrow \mathbb{Z}/p^\alpha\mathbb{Z}$, $a \longmapsto a_\alpha$ den Homomorphismus

$$\mathrm{red}_{p^\alpha} : \mathbb{Z}_p[x] \Longrightarrow \mathbb{Z}/p^\alpha\mathbb{Z}[x].$$

Satz 2.2.18 (Henselsches Lemma für $\mathbb{Z}_p$)
Es sei $F = \sum_{\nu=0}^{m} a_\nu x^\nu \in \mathbb{Z}_p[x]$ und $f = \mathrm{red}_p F \in \mathbb{F}_p[x]$ die Reduktion modulo p. Es sei $\alpha \in \mathbb{F}_p$ eine einfache Nullstelle von f, d.h. $f(\alpha) = 0$, $f'(\alpha) \neq 0$. Dann gibt es genau eine ganze p-adische Zahl $a \in \mathbb{Z}_p$ mit $F(a) = 0$ und $a_1 = \alpha$.

Beweis: Wir machen den Ansatz $a = (a_\alpha)$ mit

$$a_\alpha = c_\alpha \bmod p^\alpha \text{ mit } c_\alpha = \sum_{\nu=0}^{\alpha-1} t_\nu p^\nu, \ 0 \leq t_\nu < p.$$

und konstruieren induktiv die Ziffern $t_0, t_1, t_2, \ldots$ mit $F(c_\alpha) \equiv 0 \bmod p^\alpha$, d.h. $\mathrm{red}_{p^\alpha} F(a_\alpha) = 0$ in $\mathbb{Z}/p^\alpha\mathbb{Z}$.
Wir starten mit $0 \leq t_0 < p$, wobei

$$\alpha = t_0 \bmod p = a_1.$$

Sei $a_\alpha = c_\alpha \bmod p^\alpha$ schon konstruiert, so daß $F(c_\alpha) \equiv 0 \bmod p^\alpha$, d.h. $F(c_\alpha) \in \mathbb{Z}_p$ hat eine p-adische Entwicklung der Form

$$(\ldots s_{\alpha+1} s_\alpha \underbrace{0\ldots 0}_{\alpha \text{ Ziffern}})_p.$$

$\dfrac{F(c_\alpha)}{p^\alpha}$ hat dann die p-adische Entwicklung $(\ldots s_{\alpha+1}s_\alpha)_p$, wobei

$$0 \leq s_\alpha < p, \ \left(\frac{F(c_\alpha)}{p^\alpha}\right)_1 = s_\alpha \bmod p.$$

Man erhält dann für $c_{\alpha+1} = c_\alpha + t_\alpha p^\alpha$:

$$F(c_{\alpha+1}) \equiv 0 \bmod p^{\alpha+1} \Longleftrightarrow F(c_\alpha) + F'(c_\alpha)t_\alpha p^\alpha \equiv 0 \bmod p^{\alpha+1} \Longleftrightarrow$$

$$(*) \qquad \frac{F(c_\alpha)}{p^\alpha} + F'(c_\alpha)t_\alpha \equiv 0 \bmod p.$$

Sei nun $\beta = b \bmod p,\ 0 < b < p$, ein Inverses von $f'(\alpha)$ in $\mathbb{F}_p$. Da $F'(c_\alpha) \bmod p = F'(c_1) \bmod p = f'(\alpha)$, ist somit $(*)$ äquivalent zu

$$bs_\alpha + t_\alpha \equiv 0 \bmod p, \quad \text{d.h. } t_\alpha \equiv -bs_\alpha \bmod p.$$

Damit haben wir die Lösung

$$a = (a_\alpha)_{\alpha \geq 1}$$

rekursiv gefunden. □

Wir erinnern an den Begriff des Quotientenkörpers. So wie man aus $\mathbb{Z}$ den Körper $\mathbb{Q}$ der rationalen Zahlen konstruiert, kann man aus jedem Integritätsbereich R den **Quotientenkörper** K von R konstruieren (siehe etwa [1]).

K besteht aus den Brüchen $\frac{a}{b}$, wobei $a, b \in R$ und $b \neq 0$. Dabei gilt

$$\frac{a}{b} = \frac{c}{d} \Longleftrightarrow ad = bc,$$

und die Rechneroperationen werden durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd} \quad \text{und } \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

eingeführt. Sind $a, b \in R\backslash\{0\}$, so ist

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}.$$

Definition 2.2.19 Der Quotientenkörper von $\mathbb{Z}_p$ wird mit $\mathbb{Q}_p$ bezeichnet und heißt der **Körper der p-adischen Zahlen**.

Lemma 2.2.20 Zu jeder p-adischen Zahl $z \in \mathbb{Q}_p\backslash\{0\}$ gibt es genau ein $k \in \mathbb{Z}$ und eine p-adische Einheit $e \in \mathbb{Z}_p^\times$, so daß $z = p^k \cdot e$.

Beweis:

(1) Sei $a \in \mathbb{Z}_p$, $a \neq 0$. Wir setzen

$$k = \max\{\alpha \in \mathbb{N}_+ \mid a_\alpha = 0\}.$$

Es gilt dann also

$$a = (0, \dots, 0, a_{k+1}, a_{k+2}, \dots)$$

mit $a_{k+1} \neq 0$ in $\mathbb{Z}/p^{k+1}\mathbb{Z}$.

Die p-adische Entwicklung von a hat die Form $(\dots t_{k+1} t_k 0 \dots 0)_p$ mit $t_k \neq 0$, also

$$a_\alpha = \sum_{\nu=k}^{\alpha-1} t_\nu p^\nu \bmod p^\alpha \text{ für } \alpha \geq k.$$

Setzt man $e = (e_\alpha)_{\alpha \geq 1}$ mit

$$e_\alpha = \sum_{\nu=0}^{\alpha-1} t_{k+\nu} p^\nu \bmod p^\alpha \text{ für } \alpha \geq 1,$$

so gilt:

$$a = p^k e \text{ und da } e_1 = t_k \bmod p \neq 0,$$

ist e nach Lemma 2.2.17 eine p-adische Einheit.

(2) Sei $z \in \mathbb{Q}_p$, $z \neq 0$, etwa $z = \frac{a}{b}$ mit $a, b \in \mathbb{Z}_p \backslash \{0\}$. Nach dem ersten Schritt gibt es Zahlen $k_1, k_2 \geq 0$ und p-adische Einheiten $e_1, e_2 \in \mathbb{Z}_p^\times$, so daß $a = p^{k_1} e_1$, $b = p^{k_2} e_2$, also $z = ab^{-1} = p^{k_1 - k_2} e_1 e_2^{-1} = p^k e$ mit $k = k_1 - k_2$ und $e = e_1 e_2^{-1}$.

Damit ist die Existenz einer Darstellung

$$z = p^k e \quad (k \in \mathbb{Z},\ e \in \mathbb{Z}_p^\times)$$

bewiesen.

(3) Zum Beweis der Eindeutigkeit geht man von zwei Darstellungen

$$z = p^k e,\ z = p^m f,\ k, m \in \mathbb{Z},\ e, f \in \mathbb{Z}_p^\times$$

aus. Dann folgt $1 = p^{k-m} e f^{-1}$, also $k - m = 0$ und $1 = e f^{-1}$, d.h. $k = m$ und $e = f$. □

Definition 2.2.21 Die **p-adische Bewertung**

$$v_p : \mathbb{Q}_p \Longrightarrow \mathbb{Z} \cup \{\infty\}$$

wird folgendermaßen definiert:

$$v_p(0) := \infty.$$

Für $z \in \mathbb{Q}_p \backslash \{0\}$ setzt man

$$v_p(z) = k,$$

wenn $z p^{-k}$ eine p-adische Einheit ist.

Lemma 2.2.22 $v_p : \mathbb{Q}_p \longrightarrow \mathbb{Z} \cup \{\infty\}$ ist eine diskrete Bewertung auf dem Körper $\mathbb{Q}_p$, d.h. es gelten die Axiome einer diskreten Bewertung:

(1) $v_p(z) = \infty \Longleftrightarrow z = 0$

(2) $v_p(zw) = v_p(z) + v_p(w) \quad \forall\, z, w \in \mathbb{Q}_p$

(3) $v_p(z + w) \geq \min(v_p(z), v_p(w))$ für alle $z, w \in \mathbb{Q}_p$.

(Dabei wird wie üblich gesetzt:

$$\infty \geq k,\ \infty + k = k + \infty = \infty \quad \forall\, k \in \mathbb{Z} \cup \{\infty\}.)$$

Weiter gilt für $z \in \mathbb{Q}_p$:

z ist ganze p-adische Zahl $\Longleftrightarrow v_p(z) \geq 0$,
z ist p-adische Einheit $\Longleftrightarrow v_p(z) = 0$. □

Man kann also $\mathbb{Z}_p$ mit Hilfe von v_p als den Unterring von $\mathbb{Q}_p$, der aus allen Elementen z mit $v_p(z) \geq 0$ besteht, charakterisieren.

Definition 2.2.23 Für $z \in \mathbb{Q}_p$ sei

$$|z|_p := \begin{cases} p^{-v_p(z)} & , \quad \text{falls } z \neq 0 \\ 0 & , \quad \text{falls } z = 0. \end{cases}$$

Lemma 2.2.24 $|\ |_p$ ist eine **nichtarchimedische Norm** auf $\mathbb{Q}_p$, d.h. es gilt

(1) $|z|_p \geq 0,\ |z|_p = 0 \Longleftrightarrow z = 0$

(2) $|zw|_p = |z|_p\ |w|_p$

(3) $|z + w|_p \leq \max(|z|_p, |w|_p)$. □

Definition 2.2.25 Eine Folge $(z_n)_{n\in\mathbb{N}}$ von p-adischen Zahlen $z_n \in \mathbb{Q}_p$ heißt

a) **p-adisch konvergent** gegen $z \in \mathbb{Q}_p$ $:\Longleftrightarrow$

$$\lim_{n\to\infty} |z - z_n|_p = 0$$

b) **p-adische Cauchyfolge**: $\Longleftrightarrow$

$$\forall\, \varepsilon > 0\ \exists\, N \in \mathbb{N} \quad \forall\, n, m \geq N : |z_n - z_m|_p < \varepsilon$$

Satz 2.2.26 $\mathbb{Q}_p$ ist vollständig, d.h. jede p-adische Cauchyfolge ist p-adisch konvergent.

Beweis: Sei (z_n) eine p-adische Cauchyfolge. Sei $N \in \mathbb{N}$ so gewählt, daß

$$|z_n - z_N|_p < 1 \text{ für alle } n \geq N.$$

Dann gilt

$$\begin{aligned} &|z_n|_p \leq \max(|z_N|_p, 1) \text{ für } n \geq N, \text{ also} \\ &|z_n|_p \leq K := \max(1, |z_1|_p, \ldots, |z_N|_p) \quad \forall\, n \in \mathbb{N} \end{aligned}$$

$\Longrightarrow v_p(z_n) \geq -\log_p K \geq l$ für ein $l \in \mathbb{Z}$
$\Longrightarrow x_n = p^{-l} z_n \in \mathbb{Z}_p$ ist ganz und (x_n) ist ebenfalls p-adische Cauchyfolge.
Es genügt zu zeigen, daß (x_n) gegen eine p-adische Zahl x konvergiert. Dann konvergiert (z_n) gegen $p^l x$.
Es gilt: $\forall\, k > 0 \quad \exists\, N_k \in \mathbb{N} \quad \forall\, n, m \geq N_k$

$$|x_n - x_m|_p \leq \frac{1}{p^k},$$

d.h.

$$v_p(x_n - x_m) \geq k.$$

Die Folge (N_k) sei monoton wachsend gewählt. Es sei

$$a_k := (x_{N_k})_k \in \mathbb{Z}/p^k\mathbb{Z}$$

(die k-te Partialsumme der p-adischen Entwicklung von x_{N_k}).
Da $v_p(x_{N_{k+1}} - x_{N_k}) \geq k$, gilt

$$\rho_{k+1}(a_{k+1}) = a_k,$$

also ist $a = (a_k)_{k \geq 1} \in \mathbb{Z}_p$.
Nach Konstruktion ist

$$v_p(a - x_{N_k}) \geq k,$$

weil $a_k = (x_{N_k})_k$. Für $n \geq N_k$ gilt

$$v_p(a - x_n) \geq \min(v_p(a - x_{N_k}),\ v_p(x_{N_k} - x_n)) \geq k,$$

also

$$a = \lim_{n \to \infty} x_n.$$

□

Lemma 2.2.27 Ist $z \in \mathbb{Q}_p$, $z \neq 0$ und $v_p(z) = k$, so gibt es eindeutig bestimmte Ziffern $t_\nu \in \{0, 1, \ldots, p-1\}$ für $\nu \geq k$, so daß

$$z = \sum_{\nu=k}^{\infty} t_\nu p^\nu \qquad (p - \text{adische Konvergenz}).$$

z ist also der p-adische Limes der Folge $\left(\sum_{\nu=k}^{n} t_\nu p^\nu\right)_{n \geq k}$ rationaler Zahlen (ganzer Zahlen, wenn z ganze p-adische Zahl ist).

Beweis: Es gilt $z = p^k e$ mit $e \in \mathbb{Z}_p^\times$. Sei $\sum\limits_{\nu=0}^{\infty} t_{\nu+k} p^\nu$ die p-adische Entwicklung von e.

$$z_n := \sum_{\nu=k}^{n} t_\nu p^\nu \in \mathbb{Q} \text{ für } n \geq k.$$

Es folgt

$$\begin{aligned} v_p(z - z_n) &= v_p\left(p^k\left(e - \sum_{\nu=k}^{n} t_\nu p^{\nu-k}\right)\right) \\ &= k + v_p\left(e - \sum_{\nu=k}^{n} t_\nu p^{\nu-k}\right) \geq k + (n-k) = n, \end{aligned}$$

also $|z - z_n|_p \leq p^{-n} \longrightarrow 0$, falls $n \to \infty$. □

Korollar 2.2.28 $\mathbb{Q}$ ist dicht in $\mathbb{Q}_p$ bzgl. der Norm $|\ |_p$. □

Man nennt daher $\mathbb{Q}_p$ die **p-adische Komplettierung** von $\mathbb{Q}$.
Die unendlich vielen verschiedenen Körper $\mathbb{Q}_p$, p Primzahl, und $\mathbb{R}$, die alle nach dem gleichen Konstruktionsprinzip gewonnen worden sind (nämlich als Vervollständigung von $\mathbb{Q}$ bzgl. einer Norm auf $\mathbb{Q}$), heißen die **lokalen Körper** von $\mathbb{Q}$.
Wir bemerken noch: Die verschärfte Dreiecksungleichung

$$|x + y|_p \leq \max(|x|_p,\ |y|_p)$$

hat ungewohnte Konsequenzen für die Topologie auf $\mathbb{Q}_p$, z.B. ist eine unendliche Reihe $\sum\limits_{n=1}^{\infty} z_n$ von p-adischen Zahlen $z_n \in \mathbb{Q}_p$ genau dann konvergent, wenn die Folge (z_n) der Glieder eine Nullfolge ist. Es gilt ja

$$\left|\sum_{n=k}^{m} z_n\right| \leq \max_{k \leq n \leq m} |z_n| \leq \varepsilon,$$

wenn $|z_n| \leq \varepsilon$ für $n \geq k$.
Zur p-adischen Analysis siehe [10] und [19].
Wir kommen zu Polynomen in mehreren Veränderlichen zurück.

Definition 2.2.29 Ein Polynom $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ heißt **reduziert**, wenn

$$f = \sum_{\nu_1, \ldots, \nu_n = 0}^{p-1} a_{\nu_1, \ldots \nu_n} x_1^{\nu_1} \ldots x_n^{\nu_n},$$

d.h. wenn f in jeder Unbestimmten vom Grad $\leq p - 1$ ist.

Lemma 2.2.30 Ist $f \in \mathbb{F}_p[x_1, \ldots, x_n]$, so gibt es ein eindeutig bestimmtes reduziertes Polynom $g \in \mathbb{F}_p[x_1, \ldots, x_n]$ mit der Eigenschaft $\forall\, a \in \mathbb{F}_p^n : f(a) = g(a)$. Weiter gilt grad $g \leq$ grad f und $V(f) = V(g)$ in $\mathbb{F}_p^n$.

Beweis:

(1) Existenz: Sei $\nu = (\nu_1, \dots, \nu_n) \in \mathbb{N}^n$.
Da $a^p = a \quad \forall\, a \in \mathbb{F}_p$, betrachtet man

$$\nu_i = q_i p + r_i,\ \ q_i \geq 0,\ \ 0 \leq r_i < p.$$

Es folgt

$$a^{\nu_i} = a^{q_i p} a^{r_i} = a^{q_i} a^{r_i} = a_i^{\tilde{\nu}_i} \quad \forall\, a \in \mathbb{F}_p$$

mit $q_i + r = \tilde{\nu}_i < \nu_i$, falls $\nu_i \geq p$.

Man iteriere solange bis die Exponenten kleiner als p sind.

Es gibt also ein $\mu = (\mu_1, \dots, \nu_n)$ mit $0 \leq \mu_i < p$ für $i = 1, \dots, n$, so daß

$$a^\nu = a^\mu \quad \forall\, a \in \mathbb{F}_p^n.$$

Im Polynom f ersetzt man dann das Monom x^ν durch x^μ und erhält ein reduziertes Polynom g mit $f(a) = g(a)$ für alle $a \in \mathbb{F}_p^n$.

(2) Eindeutigkeit: Sei $f \in \mathbb{F}_p[x_1, \dots, x_n]$ reduziert und

$$f(a) = 0 \quad \forall\, a \in \mathbb{F}_p^n.$$

Behauptung: $f = 0$ (Nullpolynom)

Beweis: Sei $f = \sum\limits_{\nu=0}^{p-1} f_\nu x_n^\nu$ mit $f_\nu \in \mathbb{F}_p[x_1, \dots, x_{n-1}]$ reduziert. Sei $a' = (a_1, \dots, a_{n-1}) \in \mathbb{F}_p^{n-1}$. Dann ist $f_{a'} := \sum\limits_{\nu=0}^{p-1} f_\nu(a') x_n^\nu \in \mathbb{F}_p[x_n]$ Polynom vom Grad $< p$ mit p Nullstellen, also $f_{a'} = 0$, d.h. $f_\nu(a') = 0 \quad \forall\, a' \in \mathbb{F}_p^{n-1}$.

Nach Induktionsvoraussetzung ist $f_\nu = 0$ für alle ν, also $f = 0$. $\square$

Satz 2.2.31 (Chevalley)
Hat ein Polynom $f \in \mathbb{F}_p[x_1, \dots, x_n]$ vom Grad $d < n$ eine Nullstelle in $\mathbb{F}_p^n$, so hat f mindestens zwei verschiedene Nullstellen in $\mathbb{F}_p^n$.

Beweis: Der Beweis ist trickreich.
Annahme: $a \in \mathbb{F}_p^n$ ist die einzige Nullstelle von f. Wir wollen den kleinen Fermat ausnutzen und betrachten deshalb

$$h := 1 - f^{p-1} \in \mathbb{F}_p[x_1, \dots, x_n].$$

Es gilt: $h(a) = 1$, und für $b \neq a$ ist $f(b) \neq 0$, also $f(b)^{p-1} = 1$ und somit

$$h(b) = 0 \text{ für alle } b \in \mathbb{F}_p^n \backslash \{a\}.$$

Sei $a = (a_1, \dots, a_n)$. Auch das Polynom

$$h^* = \prod_{i=1}^n (1 - (x_i - a_i)^{p-1})$$

hat die Eigenschaft

$$h^*(a) = 1,\ h^*(b) = 0 \text{ für } b \neq a.$$

Da h^* reduziert ist, ist (nach Lemma 2.2.30) h^* die Reduktion von h. Es folgt grad $h^* \leq$ grad h im Widerspruch zu grad $h^* = n(p-1) > d(p-1) =$ grad h. $\square$

Definition 2.2.32 Ein Polynom $f \in R[x_1, \ldots, x_n]$ heißt **homogen** vom Grad $d \Longleftrightarrow$

$$f = \sum_{\nu_1 + \cdots + \nu_n = d} a_{\nu_1} \ldots \nu_n x_1^{\nu_1} \ldots x_n^{\nu_n}.$$

Korollar 2.2.33 Ein homogenes Polynom $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ vom Grad d, $1 \leq d < n$ hat mindestens eine nichttriviale Nullstelle in $\mathbb{F}_p^n$.

Beweis: f hat die triviale Nullstelle $(0, \ldots, 0)$. Nach dem Satz von Chevalley gibt es eine weitere Nullstelle. $\square$

Das Henselsche Lemma für $\mathbb{Z}_p$ läßt sich auch für Polynome in n Veränderlichen aussprechen.

Satz 2.2.34 Sei $F \in \mathbb{Z}_p[x_1, \ldots, x_n]$ und $f \subset \mathbb{F}_p[x_1, \ldots, x_n]$ die Reduktion von F modulo p. Es sei $\alpha \in \mathbb{F}_p^n$ eine Nullstelle von f, und es gelte

$$\nabla f(\alpha) = \left(\frac{\partial f}{\partial x_1}(\alpha), \ldots, \frac{\partial f}{\partial x_n}(\alpha) \right) \neq 0.$$

Dann gibt es eine Nullstelle $a \in \mathbb{Z}_p^n$ von F mit $a \bmod p = \alpha$.

Beweis: Es sei $\frac{\partial f}{\partial x_j}(\alpha) \neq 0$ und $\widetilde{a} = (\widetilde{a}_1, \ldots, \widetilde{a}_n) \in \mathbb{Z}_p^n$ sei Repräsentant von $\alpha = (\alpha_1, \ldots, \alpha_n)$. Man setze dann

$$\begin{aligned} \widetilde{F}(x) &:= F(\widetilde{a}_1, \ldots, \widetilde{a}_{j-1}, x, \widetilde{a}_{j+1}, \ldots, \widetilde{a}_n) \text{ und} \\ \widetilde{f}(x) &:= f(\alpha_1, \ldots, \alpha_{j-1}, x, \alpha_{j+1}, \ldots, \alpha_n). \end{aligned}$$

Dann gilt $\widetilde{f}(\alpha_j) = 0$ und $\widetilde{f}'(\alpha_j) \neq 0$.

Nach dem Henselschen Lemma gibt es also ein $a_j \in \mathbb{Z}_p$ mit $\widetilde{F}(a_j) = 0$ und $a_j \bmod p = \alpha_j$. $a = (\widetilde{a}_1, \ldots, \widetilde{a}_{j-1}, a_j, \widetilde{a}_{j+1}, \ldots, a_n)$ ist dann eine Nullstelle von F mit $a \bmod p = \alpha$. $\square$

Korollar 2.2.35 Es sei

$$F = ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2fyz$$

mit $a, b, c, d, e, f \in \mathbb{Z}$, und es gelte

$$D = \det \begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} = \pm 1.$$

Dann gibt es für jede Primzahl $p > 2$ eine primitive Nullstelle $(x, y, z) \in \mathbb{Z}_p^3$ von F. Dabei heißt $(x_1, \ldots, x_n) \in \mathbb{Z}_p^n$ **primitiv**, wenn wenigstens ein x_j eine p-adische Einheit ist.

Beweis: Sei $\widetilde{F}$ die Reduktion von F modulo p. Dann ist $\widetilde{F} \in \mathbb{F}_p[x,y,z]$ homogen vom Grad 2, und nach 2.2.33 gibt es eine nichttriviale Nullstelle $(\xi,\eta,\zeta) \in \mathbb{F}_p^3$ von $\widetilde{F}$. Diese Nullstelle ist einfach, denn die Ableitung von $\widetilde{F}$ ist

$$\nabla\widetilde{F}(\xi,\eta,\zeta) = 2\begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix}\begin{pmatrix} \xi \\ \eta \\ \zeta \end{pmatrix}.$$

Da $p \neq 2$, ist also $\nabla\widetilde{F}(\xi,\eta,\zeta) \neq 0$, weil $(\xi,\eta,\zeta) \neq 0$ und $\det\begin{pmatrix} a & d & e \\ d & b & f \\ e & f & c \end{pmatrix} \not\equiv 0 \bmod p$.

Nach Satz 2.2.34 gibt es eine Nullstelle $(x,y,z) \in \mathbb{Z}_p^3$ von F mit $x \bmod p = \xi$, $y \bmod p = \eta$, $z \bmod p = \zeta$. Da $(\xi,\eta,\zeta) \neq 0$, ist (x,y,z) primitiv. $\square$

Die Frage nach der Existenz nichttrivialer ganzzahliger (oder rationaler) Nullstellen wollen wir später behandeln. Hier nur einige Beispiele:

Beispiel 2.2.36

(1) $F = x^2 + y^2 - z^2$ hat bekanntlich viele Nullstellen $(x,y,z) \in \mathbb{Z}^3$, zum Beispiel

$$(1,0,1),\ (0,1,1),\ (3,4,5).$$

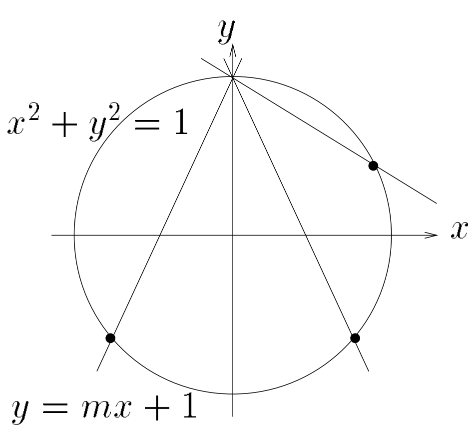
Ist $(x,y,z) \in \mathbb{Z}^3\backslash 0$ eine nichttriviale Nullstelle von F, so muß $z \neq 0$ gelten, und

$$\left(\frac{x}{z}, \frac{y}{z}\right) \in \mathbb{Q}^2$$

ist dann eine rationale Nullstelle von

$$f = x^2 + y^2 - 1.$$

Ist nun umgekehrt $(a,b) \in \mathbb{Q}^2$ eine Nullstelle von f, so ist für jeden gemeinsamen Nenner c von a und b das Tripel $(ac, bc, c) \in \mathbb{Z}^3$ Nullstelle von F. Durch eine simple geometrische Überlegung bekommt man alle rationalen Nullstellen $(a,b) \in \mathbb{Q}^2$ von f: Man schneidet die Gerade $y = mx + 1$ der rationalen Steigung $m \in \mathbb{Q}\backslash\{0\}$ mit der Kreislinie $x^2 + y^2 = 1$. Der von $(0,1)$ verschiedene Schnittpunkt (a,b) ist rational. Alle rationalen Punkte von $x^2 + y^2 = 1$ mit Ausnahme von $(0,\pm 1)$ werden so erhalten



(siehe [14].)

(2) $f = 2x^2 + y^2 - 5z^2$ besitzt keine nichttrivialen ganzzahligen Nullstellen. Dazu braucht man nur zu zeigen, daß

$$\mathrm{red}_5 f = 2x^2 + y^2 \in \mathbb{F}_5[x, y]$$

keine nichttriviale Nullstelle in $\mathbb{F}_5^2$ hat. Das erledigt man durch Einsetzen von

$$x = 0, \pm 1, \pm 2, \quad y = 0, \pm 1, \pm 2.$$

Für jede Lösung $(x, y, z) \in \mathbb{Z}^3$ von $f = 0$ gilt dann $x = 5x', y = 5y'$ und somit auch $10x'^2 + 5y'^2 - z^2 = 0$, folglich $z = 5z'$, also $2x'^2 + x'^2 - 5z'^2 = 0$.

Durch Iteration sieht man: x, y, z sind durch alle Potenzen von 5 teilbar, und somit gilt $(x, y, z) = (0, 0, 0)$.

Beispiel 2.2.37 Wir betrachten die Frage, ob eine ganze Zahl $n \in \mathbb{Z}$ in $\mathbb{Q}_p$ eine Quadratwurzel besitzt. Wir untersuchen also das Polynom

$$f = x^2 - n \in \mathbb{Z}[x]$$

auf Nullstellen in $\mathbb{Q}_p$.
(Für den Körper $\mathbb{R}$ ist die Antwort bekanntlich: Genau dann, wenn $n \geq 0$ ist, gibt es eine reelle Quadratwurzel von n.)
Ist nun $n \not\equiv 0 \bmod p$ und hat

$$\mathrm{red}_p f = x^2 - n \bmod p \in \mathbb{F}_p[x]$$

eine Nullstelle α in $\mathbb{F}_p$, so ist

$$\mathrm{red}_p f = (x - \alpha)(x + \alpha)$$

und $\alpha \neq -\alpha$ falls $p > 2$.
$\alpha, -\alpha$ sind also einfache Nullstellen und nach dem Henselschen Lemma gibt es genau zwei Nullstellen a und $-a$ in $\mathbb{Z}_p$. Sei etwa $n = -1$ und $p = 5$. Dann ist

$$2^2 = 4 \equiv -1 \bmod 5,$$

also besitzt -1 zwei Quadratwurzeln in $\mathbb{F}_5$, nämlich $\alpha = 2 \bmod 5$ und $-\alpha = -2 \bmod 5$.
$f = x^2 + 1$ hat die Ableitung $f' = 2x$ und für $c_1 := 2$ gilt $f'(2) = 4$.
Wegen $4 \cdot 4 \equiv 1 \bmod 5$ ist $\beta = 4 \bmod 5$ das Inverse von $f'(\alpha)$ in $\mathbb{F}_5$ und somit erhält man aus dem Beweis des Henselschen Lemmas die Rekursionsformel

$$(*) \left\{ \begin{array}{rcl} c_1 & = & 2 \\ c_{k+1} & \equiv & c_k - 4(c_k^2 + 1) \bmod 5^{k+1} \text{ für } k \geq 2 \end{array} \right.$$

wobei $0 \leq c_k < 5^k$

$$a = (a_k)_{k \geq 1} \text{ mit } a_k = c_k \bmod 5^k \in \mathbb{Z}/5^k\mathbb{Z}$$

ist dann eine Quadratwurzel von -1 in $\mathbb{Q}_5$.

Es ist leicht die 5-adische Entwicklung von a aus $(*)$ zu bestimmen.

$$\begin{aligned}
&c_1 = (2)_5\\
&c_2 \equiv 2 - 20 \equiv 7 \bmod 25 \Longrightarrow\\
&c_2 = 7 = (12)_5\\
&c_3 \equiv 7 - 4 \cdot 50 \equiv 7 + 50 \equiv 57 \bmod 125, \text{ also}\\
&c_3 = 57 = (212)_5\\
&c_4 \equiv 57 - 4 \cdot 2250 \equiv 57 + 1000 \equiv 432 \bmod 625, \text{ also}\\
&c_4 = 432 = (3212)_5 \quad \text{usw.}
\end{aligned}$$

Das in $\mathbb{Q}[x]$ irreduzible Polynom $x^2 + 1$ ist also in dem Oberring $\mathbb{Q}_5[x]$ reduzibel.

Beispiel 2.2.38 Wir wollen ein ***Mathematica*** -Programm zum Henselschen Lemma entwickeln. Ist $f \in \mathbb{Z}[x]$ ein Polynom, p eine Primzahl, $c \in \{0, 1, \ldots, p-1\}$ eine einfache Nullstelle von f modulo p und $k \geq 1$, so soll

$$c_k = \text{hensel}[f, c, k, p], \;\; 0 \leq c_k < p^k$$

die k-te Approximation der Lösung $a \in \mathbb{Z}_p$ von $f = 0$ mit $a \equiv c \bmod p$ sein.

Zunächst bemerken wir: In ***Mathematica*** wird ein Ausdruck wie

$$f = 2x^3 + 3x + 1$$

als Polynom in $\mathbb{Z}[x]$ betrachtet. f ist keine Funktion. Man kann den Wert von f an der Stelle a nicht durch $f[a]$ berechnen. Vielmehr bedient man sich eines anderen Konstrukts (siehe [11] Abschnitt 10):

$$x -> a$$

bedeutet, daß x durch a zu ersetzen ist. Der Befehl

$$f/.\ x -> a$$

bewirkt, daß jeder im Ausdruck f vorkommende Term x durch a ersetzt wird.

Also erhält man durch

$$fkt[f\_][a\_] := f/.\ x -> a$$

die zum Polynom $f \in \mathbb{Z}[x]$ gehörende Funktion

$$fkt[f].$$

Jetzt kann man etwa den Wert von f an Stelle $x = 2$ durch $fkt[f][2]$ berechnen. In unserem konkreten Beispiel ergibt sich

$$fkt[f][2] = f/.\ x -> 2 = 23.$$

Mit dem Befehl 'Solve' kann man Gleichungen lösen (siehe [23] 3.4.11). Sei $f \in \mathbb{Z}[x]$ ein beliebiges Polynom in x.

$$R = \text{Solve}[f == 0 \;\&\&\; \text{Modulus} \; == p, x]$$

ergibt die Liste der Lösungen der Kongruenz

$$f(x) \equiv 0 \bmod p.$$

Das erste Element der Liste R hat die Form von Einsetzungsregeln

$$R[\![1]\!] = \{\text{ Modulus} -> p, x -> c_1\}.$$

Den kleinsten positiven Rest von c_1 modulo p erhält man durch

$$c = \text{Mod}[x/.\ R[\![1]\!], p].$$

$x/.\ R[\![1]\!]$ bedeutet ja, daß auf x die 'Regel' $R[\![1]\!]$ angewendet wird, also x durch die Zahl c_1 ersetzt wird. Durch

$$L = \text{Map}[\text{Mod}[\#, p]\&, x/.\ R]$$

erhält man die Liste aller Lösungen von $f(x) \equiv 0 \bmod p$, normiert als positive kleinste Reste modulo p. Dabei ist $x/.\ R$ zunächst die Liste aller Lösungen. Auf diese Liste wird dann elementweise die Funktion $c \longmapsto \text{Mod}[c, p]$ angewandt. In ***Mathematica*** kann man diese Funktion einfach als

$$g = \text{Mod}[\#, p]\&$$

bezeichnen (siehe [23] 2.2.5). Der Befehl Map bewirkt:

$$\text{Map}[g, \{c_1, \ldots, c_n\}] = \{g[c_1], \ldots, g[c_n]\}.$$

Natürlich kann es passieren, daß die Kongruenz $f(x) \equiv 0 \bmod p$ keine Lösung besitzt. Dann wird

$$L = \{\ \}$$

ausgegeben. Weiter kann es passieren, daß einige Lösungen in der Liste $x/.\ R$ keine ganzen Zahlen sind. Mit folgendem Befehl werden aus einer Liste A die ganzen Zahlen herausgepickt.

$$\text{ganz}[A\_] := \text{Select}[A, \text{IntegerQ}]$$

Wir modifizieren unsere Definition von L durch

$$L = \text{Map}[\text{Mod}[\#, p]\&, \text{ganz}[[x/.\ R]].$$

Damit ist

$$L = \{c_1, \ldots, c_n\} \quad (n = \text{Length}[L])$$

die Liste der Lösungen von $f(x) \equiv 0 \bmod p$.

Um zu sehen, welche Nullstellen c_i einfach modulo p sind, betrachten wir die Matrix (= Wertetabelle)

$$A = \begin{pmatrix} c_1 & f'(c_1) \bmod p \\ \vdots & \vdots \\ c_n & f'(c_n) \bmod p \end{pmatrix}$$

und vergleichen sie mit

$$B = \begin{pmatrix} c_1 & 0 \\ \vdots & \\ c_n & 0 \end{pmatrix}.$$

$C = \text{Complement}[A, B]$ besteht dann nur noch aus den Zeilen $(c_i, f'(c_i) \bmod p)$ mit $c_i \bmod p \neq 0$.

In ***Mathematica*** kann man dies folgendermaßen realisieren ($D[f, x]$ ist die Ableitung von f nach x)

$A = \text{Transpose}[\{L,\ \text{Map}[\text{Mod}[D[f, x]/.\ x -> \#, p]\&, L\}];$

$B = \text{Transpose}[\{L,\ \text{Table}[0, \{\text{Length}[L]\}]\}];$

$C = \text{Complement}[A, B]$

Schließlich ist dann

$$C1 = \text{Transpose}[C][\![1]\!]$$

die Liste der einfachen Nullstellen von $f(x) \equiv 0 \bmod p$.

Jetzt erhalten wir ein Programm, welches diejenigen Lösungen von $f(x) \equiv 0 \bmod p^k$, die zu einfachen Nullstellen modulo p gehören, berechnet und ihre Dezimaldarstellung und p-adische Entwicklung ausgibt.

```
hensel [f_, k_, p_] :=
   Module [{R, L, A, B, C, C1},
      If [PrimeQ[p],
         R =Solve[f == 0 &&Modulus== p, x];
         L =Map[Mod[#, p]&, ganz[x./R]];
         If [L! = { },
            A = Transpose[{L, Map[Mod[D[f, x]/.x − > #, p]&, L}];
            B = Transpose[{L, Table[0, {Length[L]}]}];
            C = Complement[A, B];
            If [C! = { }, C1 =First[Transpose[C]];
               Map[hensel[f, #, k, p]&, C1]//TableForm,
               Print["Es gibt keine einfachen Nullstellen von", f, "modulo", p]],
         Print["Es gibt keine Nullstellen von", f, "modulo", p]],
      Print[p, "ist eine Primzahl"]]]
```

Das hierbei benutzte Programm

$$\text{hensel}[f, c, k, p]$$

ist das Approximationsverfahren aus dem Henselschen Lemma und folgendermaßen definiert:

```
hensel [f_, c_, k_, p_] :=
      Module [{b, approx= c, i = 2},
         b = PowerMod[D[f, x]/.x − > c, −1, p];
```

```
While [i <= k,
        approx=Mod[approx−b * f/.x −> approx,p^i];
        i++];
        Flatten [{approx, IntegerDigits[approx,p, k]}]]
```

Ein Beispiel: $f = (x-4)(x-2)(x-1)^2 + 7(x^2+x+3)$ hat $c = 4$ als einfache Nullstelle modulo 7.

$$c[k\_] := \text{hensel}[f, c, k, 7]$$

ist die k-te Approximation der Nullstelle $a \in \mathbb{Z}_7$ mit $a \bmod 7 = 4$.
Man erhält zum Beispiel die ersten 6 Approximationen in der Tabelle

$$\text{Table}[c[k],\ \{k, 1, 6\}]//\text{TableForm}$$

Dezimal	7-adisch
4	4
25	34
74	134
417	1134
417	01134
84452	501134

Die 7-adische Entwicklung von $c[15]$ ist zum Beispiel die folgende 15-stellige Zahl im Siebenersystem

$$(020226100501134)_7.$$

Diese Zahl ist eine Nullstelle von f modulo

$$7^{15} = (1000000000000000)_7.$$

Das Programm hensel$[f, 5, 7]$ ermittelt die Liftungen aller einfachen Nullstellen modulo 7 zu Nullstellen modulo 7^5:

$$\begin{array}{rl} 5399 & (21512)_7 \\ 417 & (01134)_7 \end{array}$$

f hat also modulo 7 die einfachen Nullstellen 2 und 4, die Modulo 7^5 zu $(21512)_7$ und $(01134)_7$ geliftet werden.

Übungen 2.2.39

(1) Konstruiere ein homogenes Polynom $f \in \mathbb{Z}[x, y]$ vom Grad 2 und ein homogenes Polynom $g \in \mathbb{Z}[x, y, z]$ vom Grad 3, so daß gilt

(a) $f(x, y) \equiv 0 \bmod 5 \iff x \equiv y \equiv 0 \bmod 5$

(b) $g(x, y, z) \equiv 0 \bmod 2 \iff x \equiv y \equiv z \equiv 0 \bmod 2$

(2) Es sei $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ vom Grad $d < n$.

Beweise: Die Anzahl s aller Nullstellen $(a_1, \ldots, a_n) \in \mathbb{F}_p^n$ von f ist durch p teilbar.

Hinweis: Betrachte das Polynom

$$\sum_{j=1}^{s}\left(\prod_{i=1}^{n}(1-(x_i-a_{ji})^{p-1})\right),$$

wobei $(a_{j1},\ldots,a_{jn})$, $j=1,\ldots,s$ die Nullstellen von f sind.

(3) Beweise zunächst $x^3 \equiv 0, 1$ oder $-1 \bmod 7$ und folgere hieraus: Für $a,b,c,d \in \mathbb{Z}$ hat das Polynom

$$f(x,y,z) = (7a+1)x^3 + (7b+2)y^3 + (7c+4)z^3 + (7d+1)xyz$$

außer (0,0,0) keine Lösungen in $\mathbb{Z}^3$.

(4) Löse die Kongruenzen

(a) $x^3 - 2x + 3 \equiv 0 \bmod 27$

(b) $x^3 - 5x^2 + 3 \equiv 0 \bmod 27$

(c) $x^3 - 2x + 4 \equiv 0 \bmod 125$

(5) Löse die Kongruenzen

(a) $x^2 + 1 \equiv 0 \bmod 65$

(b) $5x^2 + 7x - 3 \equiv 0 \bmod 35$

(c) $x^3 - 2x + 4 \equiv 0 \bmod 1000$

Hinweis: chinesischer Restsatz

(6) Löse die Kongruenz

$$4x^4 + 9x^3 - 5x^2 - 21x + 61 \equiv 0 \bmod 1125$$

(7) Finde eine nichttriviale Nullstelle von

$$f = x^2 + y^2 + z^2$$

in $\mathbb{F}_p^3$ für $p = 3, 5, 7$.

(8) Berechne die Reduktion von $f \in \mathbb{F}_3[x,y,z]$.

(a) $f = (x^2 + y^2 + z^2)^2$,

(b) $f = (xyz + x^2 + y^2 + z^2)^2$.

Berechne die Reduktion von $f = (x^2 + y^2 + z^2)^{p-1}$ in $\mathbb{F}_p[x,y,z]$, für den Fall, daß $x^2 + y^2 + z^2 \equiv 0 \bmod p$ nur die triviale Lösung besitzt. Hinweis: Fermat

(9) Sei $\sum_{k=n}^{\infty} t_k p^k$ die p-adische Entwicklung von $a \in \mathbb{Q}_p$. Bestimme die p-adische Entwicklung von $-a$.

(10) Bestimme die p-adische Entwicklung von

(a) $(6+4p+2p^2+1p^3+\cdots)(3+0p+0p^2+6p^3+\cdots)$ für $p=7$ auf 4 Stellen genau.

(b) $1/(3+2p+3p^2+1p^3+\cdots)$ für $p=5$ auf 4 Stellen genau.

(c) $2/3$ in $\mathbb{Q}_2$

(d) $-1/6$ in $\mathbb{Q}_7$

(11) Es sei $a=\sum\limits_{k=n}^{\infty} t_k p^k,\ 0\le t_k<p$.

a heißt periodisch $\iff\ \exists\ N\ge n,\ r>0$, so daß $t_{k+r}=t_k$ für alle $k\ge N$.

Beweise: $a\in\mathbb{Q}_p$ ist genau dann periodisch, wenn $a\in\mathbb{Q}$.

(12) Beweise: Die Reihe $\sum\limits_{\nu=0}^{\infty} p^\nu$ konvergiert p-adisch gegen $\frac{1}{1-p}$.

Welche rationale Zahl stellt die p-adische Entwicklung

$$1+(p-1)p+p^2+(p-1)p^3+p^4+(p-1)p^5+\cdots$$

dar?

(13) Berechne die vierten Wurzeln von 1 in $\mathbb{Q}_5$ bis auf 4 Stellen genau.

(14) Sei $f=\sum\limits_{i=0}^{n} a_i x^i\in\mathbb{Z}_p[x]$, und es gelte $v_p(a_i)\ge 1$ für $i=1,\dots,n-1$, $v_p(a_0)=1\quad v_p(a_n)=0$.

Beweise: f ist irreduzibel in $\mathbb{Q}_p[x]$.

(15) Sei $a\in\mathbb{Z}_p$. Beweise: Die Folge $(a^{p^n})_{n\in\mathbb{N}}$ konvergiert p-adisch gegen eine Nullstelle von x^p-x in $\mathbb{Z}_p$.

(16) Für $\varepsilon>0$ und $a\in\mathbb{Q}_p$ sei $U_\varepsilon(a)=\{x\in\mathbb{Q}_p|\,|x-a|_p<\varepsilon\}$. Eine Teilmenge $U\subset\mathbb{Q}_p$ heißt offen, wenn gilt $\forall\ a\in U\ \exists\,\varepsilon>0$ s.d. $U_\varepsilon(a)\subset U$.

Beweise:

(a) $\{a\in\mathbb{Q}_p\mid v_p(a)=n\}$ ist offen $\forall\, n\in\mathbb{Z}$

(b) $\mathbb{Z}_p$ und $\mathbb{Q}_p\backslash\mathbb{Z}_p$ sind offen in $\mathbb{Q}_p$.

(c) $\mathbb{Z}_p$ ist folgenkompakt, d.h. jede Folge p-adischer ganzer Zahlen besitzt eine konvergente Teilfolge.

(17) (für ***Mathematica*** -Fans)

Schreibe ein Programm, daß die periodische p-adische Entwicklung einer rationalen Zahl ermittelt.

(18) Schreibe ein Programm a) zum Divisionsalgorithmus im Polynomenring $\mathbb{F}_p[x]$. b) zum ggT von Polynomen in $\mathbb{F}_p[x]$ und c) zum erweiterten ggT von Polynomen in $\mathbb{F}_p[x]$.

Kapitel 3

Quadratische Reste

3.1 Legendre Symbol, Euler Kriterium

Es sei p eine Primzahl, $p \neq 2$.

Weiter seien $a, b, c, \in \mathbb{Z}$ und $a \not\equiv 0 \bmod p$. Wir wollen die allgemeine quadratische Kongruenz

(1) $\qquad ax^2 + bx + c \equiv 0 \bmod p$

untersuchen.

Da $a \not\equiv 0 \bmod p$ und $p > 2$, gibt es ein $a' \in \mathbb{Z}$ mit $2a'a \equiv 1 \bmod p$. Multipliziert man (1) mit a', so erhält man die normierte Kongruenz

$$x^2 + 2a'b\,x + 2a'c \equiv 0 \bmod p,$$

und diese Kongruenz ist äquivalent zu

$$(x + a'b)^2 \equiv (a'b)^2 - 2a'c \bmod p.$$

Diese Kongruenz ist genau dann lösbar, wenn $(a'b)^2 - 2a'c$ eine Quadratzahl modulo p ist. Mit den Quadratzahlen modulo p wollen wir uns in diesem Kapitel beschäftigen, also mit der Kongruenz

(2) $\qquad x^2 \equiv a \bmod p.$

Da diese Kongruenz für $a \equiv 0 \bmod p$ trivial ist, setzen wir $a \not\equiv 0 \bmod p$ voraus. Die klassische Bezeichnung für Quadratzahlen modulo p wird in der folgenden Definition eingeführt.

Definition 3.1.1 Sei $a \in \mathbb{Z}$, $a \not\equiv 0 \bmod p$.
a heißt **quadratischer Rest modulo** $p \iff$

$$x^2 \equiv a \bmod p$$

ist lösbar,

d.h. die Restklasse $\alpha = a \bmod p \in \mathbb{F}_p$ ist ein Quadrat.

Bemerkung 3.1.2 In Beispiel 2.2.38 haben wir schon gezeigt, daß jeder quadratische Rest modulo p eine Quadratwurzel im lokalen Körper $\mathbb{Q}_p$ besitzt.

Lemma 3.1.3 Es gibt genau $\frac{p-1}{2}$ modulo p inkongruente quadratische Reste modulo p.

Beweis: Wir geben zwei Beweise

(1) Sind $c, b \in \mathbb{Z}$ mit $1 \leq c \leq \frac{p-1}{2}$, $1 \leq b \leq \frac{p-1}{2}$ und gilt $c^2 \equiv b^2 \bmod p$, so gilt

$$(c-b)(c+b) \equiv 0 \bmod p, \text{ also } c \equiv \pm b \bmod p.$$

Nach der Voraussetzung über c und b folgt $c = b$. Damit ist gezeigt, daß die $\frac{p-1}{2}$ quadratischen Rest

$$b^2,\ 1 \leq b \leq \frac{p-1}{2}$$

inkongruent modulo p sind.

Da $b^2 = (-b)^2$ und

$$\left\{ b^2 \mid -\frac{p-1}{2} \leq b \leq \frac{p-1}{2} \right\}$$

die Menge aller quadratischen Reste modulo p ist, folgt die Behauptung.

(2) In diesem Beweis benutzen wir etwas triviale Gruppentheorie.

$$\varphi : \mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times \text{ mit } \varphi(x) = x^2$$

ist ein Gruppenhomomorphismus, denn $\varphi(1) = 1$, $\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$. Es gilt $\ker \varphi = \{\pm 1\}$, und somit gilt nach dem Homomorphiesatz

$$\mathbb{F}_p^\times / \{\pm 1\} \cong \mathrm{Im}\ \varphi = \{\text{Quadrate in } \mathbb{F}_p^\times\}.$$

Es folgt: Die Anzahl der Quadrate in $\mathbb{F}_p^\times$ ist

$$\#(\mathbb{F}_p^\times / \{\pm 1\}) = \frac{1}{2} \# \mathbb{F}_p^\times = \frac{p-1}{2}.$$

□

Definition 3.1.4 Sei p eine Primzahl, $p \neq 2$. Für $a \in \mathbb{Z}$ setzt man

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & , \text{ falls } a \not\equiv 0 \bmod p \text{ und } a \text{ quadratischer Rest} \bmod p \\ 0 & , \text{ falls } a \equiv 0 \bmod p \\ -1 & , \text{ falls } a \not\equiv 0 \bmod p \text{ und } a \text{ `quadratischer Nichtrest'} \bmod p \end{cases}$$

$(\frac{a}{p})$ heißt das **Legendre-Symbol**.

Offensichtlich ist $(\frac{a}{p}) + 1$ die Anzahl der inkongruenten Lösungen von $x^2 \equiv a \bmod p$.

Satz 3.1.5 (Eulersches Kriterium)
Es sei p eine Primzahl, $p \neq 2$ und $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$. Dann gilt

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Beweis: Es gibt $\frac{p-1}{2}$ quadratische Reste $a_1, \dots, a_{\frac{p-1}{2}}$ und ebensoviele Nichtreste $a'_1, \dots, a'_{\frac{p-1}{2}}$.
Es sei $b_i \in \mathbb{Z}$ mit $a_i \equiv b_i^2 \bmod p$.
Nach dem kleinen Fermat gilt dann

$$a_i^{\frac{p-1}{2}} \equiv b_i^{p-1} \equiv 1 \bmod p$$

und somit hat das Polynom

$$f = x^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[x]$$

die $\frac{p-1}{2}$ Restklassen $[a_i]_p$, $i = 1, \dots, \frac{p-1}{2}$ als Nullstellen. Da $x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1)$ und $x^{p-1} - 1$ alle Elemente von $\mathbb{F}_p^\times$ als Nullstellen hat, besitzt das Polynom

$$g = x^{\frac{p-1}{2}} + 1 \in \mathbb{F}_p[x]$$

die $\frac{p-1}{2}$ Restklassen der Nichtreste als Nullstellen. Daraus folgt die Behauptung. □

Lemma 3.1.6 Für alle $a, b \in \mathbb{Z}$ gilt

(1) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

(2) $a \equiv b \bmod p \Longrightarrow (\frac{a}{p}) = (\frac{b}{p})$

(3) $(\frac{a^2}{p}) = 1$, $(\frac{1}{p}) = 1$

(4) $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$

Beweis:

(1) ist trivial, falls a oder b durch p teilbar ist. Sei also $a \not\equiv 0 \bmod p$ und $b \not\equiv 0 \bmod p$. Dann ergibt das Eulersche Kriterium

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

(2) und (3) sind trivial.

(4) folgt aus dem Eulerschen Kriterium. □

Korollar 3.1.7 -1 besitzt eine Quadratwurzel in $\mathbb{F}_p$ genau dann, wenn $p \equiv 1 \bmod 4$. □

Beispiel 3.1.8 Ist $x^2 \equiv 63 \bmod 11$ lösbar?

Es gilt $(\frac{63}{11}) = (\frac{8}{11}) = (\frac{2\cdot 2^2}{11}) = (\frac{2}{11})(\frac{2^2}{11}) = (\frac{2}{11}) = (\frac{-9}{11}) = (\frac{-1}{11})\cdot(\frac{3^2}{11}) = (\frac{-1}{11}) = -1$. Also ist die Kongruenz nicht lösbar. Man kann natürlich auch einfach die Liste aller quadratischen Reste und Nichtreste modulo 11 anschauen.

$x \bmod 11$	$x^2 \bmod 11$
± 1	1
± 2	4
± 3	-2
± 4	5
± 5	3

quadratische Reste $\bmod 11 : 1, -2, 3, 4, 5$

quadratische Nichtreste $\bmod 11 : -1, 2, -3, -4, -5$

Satz 3.1.9 (Gaußsches Lemma)
Es sei p eine Primzahl, $p \neq 2$. $k = \frac{p-1}{2}$. Es sei $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$. t sei die Anzahl der Zahlen mit negativem absolut kleinstem Rest modulo p in der Menge

$$M_a = \{a, 2a, \ldots, ka\}.$$

Dann gilt

$$\left(\frac{a}{p}\right) = (-1)^t.$$

Beweis: Es sei b_ν der absolut kleinste Rest von νa. Dann gilt

$$(*) \qquad b_1 \cdot \ldots \cdot b_k \equiv a(2a)\ldots(ka) = k!a^k \underset{\text{[Euler]}}{\equiv} k!(\tfrac{a}{p}) \bmod p.$$

Da $a \not\equiv 0 \bmod p$, sind die Zahlen $\pm\nu a,\ \nu = 1, \ldots, k$ paarweise inkongruent modulo p und folglich sind ihre absolut kleinsten Reste

$$\pm b_\nu,\ \nu = 1, \ldots, k$$

paarweise verschieden, d.h. diese Zahlen sind alle von Null verschiedenen absolut kleinsten Reste.
Es folgt daher

$$\prod_{\substack{1\le\nu\le k\\ b_\nu<0}} (-b_\nu) \cdot \prod_{\substack{1\le\nu\le k\\ b_\nu>0}} b_\nu = 1 \cdot 2 \cdot \ldots \cdot k = k!$$

und nach Definition von t ergibt sich somit

$$(**) \qquad b_1 \cdot \ldots \cdot b_k = (-1)^t \prod_{b_\nu<0} (-b_\nu) \prod_{b_\nu>0} b_\nu = (-1)^t k!$$

Da $k! \not\equiv 0 \bmod p$, folgt dann aus $(*)$ und $(**)$

$$\left(\frac{a}{p}\right) = (-1)^t.$$

□

Beispiel 3.1.10 Man kann das Gaußsche Lemma an der Multiplikationstafel von $\mathbb{F}_p^\times$, in der die Elemente von $\mathbb{F}_p^\times$ durch die absolut kleinsten Reste repräsentiert werden, überprüfen.

Zunächst definiert man

$$\begin{aligned}\text{akrest}[n\_, p\_] := &\text{Module}[\{r = \text{Mod}[n, p]\},\\ &\text{If}[r <= (p-1)/2,\\ &\quad r,\\ &\quad p - r]]\end{aligned}$$

Der relevante Teil der Multiplikationstafel ist dann

$$\begin{aligned}m[p-] := &\text{Table}[\text{akrest}[x * y, p],\\ &\{x, 1, (p-1)/2\}, \{y, 1, (p-1)/2\}]\end{aligned}$$

Durch

$$t[p\_] := N[\text{Map}[(2\# + p - 1)/(2p-2)\&, m[p], \{2\}]]$$

und

$$s[p\_] := N[\text{Map}[(\text{Sign}[\#] + 1)/2\&, m[p], \{2\}]]$$

erhält man eine Grauwerttafel von $m[p]$, bzw. eine Schwarz-Weiß-Tafel der Vorzeichen von $m[p]$ mit schwarz $= 0$ und weiß $= 1$.

Als Beispiel betrachten wir $p = 19$

$m[19]$//TableForm
$t[19]$//TableForm
$s[19]$//TableForm

Die graphische Darstellung erhält man durch

Show[Graphics[Raster[$t[19]$]]] und
Show[Graphics[Raster[$s[19]$]]].

Durch Zählen der Nullen in der a-ten Zeile von $s[p]$ kann man feststellen, ob a quadratischer Rest modulo p ist:

$(\frac{a}{p}) = 1 \iff$ die Anzahl der Nullen in der a-ten Zeile von $s[p]$ ist gerade.

Das Gaußsche Lemma ergibt auch sofort

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

und weiter

Lemma 3.1.11 Sei p eine Primzahl, $p \neq 2$. Dann gilt:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

d.h.

$$\begin{aligned}\left(\frac{2}{p}\right) &= 1 \iff p \equiv \pm 1 \bmod 8\\ \left(\frac{2}{p}\right) &= -1 \iff p \equiv \pm 3 \bmod 8\end{aligned}$$

Beweis: Es sei $k = \frac{p-1}{2}$, also $2k = p-1$. Die Anzahl t der negativen absolut kleinsten Reste modulo p von $M_2 = \{2, 4, \ldots, 2k\}$ ist gleich $\#\{x \in M_2 \mid x > k\} = \#\{\nu \in \mathbb{Z} \mid \frac{k}{2} < \nu \leq k\}$.

Wir gehen die möglichen Fälle durch:

1. Fall: $p = 8l + 1 \Longrightarrow k = 4l \Longrightarrow$

$$t = \#\{\nu \in \mathbb{Z} \mid 2l < \nu \leq 4l\} = 4l - 2l = \text{gerade} \;\Longrightarrow \left(\frac{2}{p}\right) = 1.$$

2. Fall: $p = 8l - 1 \Longrightarrow k = 4l - 1 \Longrightarrow$

$$t = \#\{\nu \in \mathbb{Z} \mid 2l - \frac{1}{2} < \nu \leq 4l - 1\} = (4l - 1) - (2l - 1) = \text{gerade} \;\Longrightarrow \left(\frac{2}{p}\right) = 1.$$

3. Fall: $p = 8l + 3 \Longrightarrow k = 4l + 1 \Longrightarrow$

$$t = \#\{\nu \in \mathbb{Z} \mid 2l + \frac{1}{2} < \nu \leq 4l + 1\} = 4l + 1 - 2l = \text{ungerade} \;\Longrightarrow \left(\frac{2}{p}\right) = -1.$$

4. Fall: $p = 8l - 3 \Longrightarrow k = 4l - 2 \Longrightarrow$

$$t = \#\{\nu \in \mathbb{Z} \mid 2l - 1 < \nu \leq 4l - 2\} = 4l - 2 - (2l - 1) = \text{ungerade} \Longrightarrow \left(\frac{2}{p}\right) = -1.$$

Wir schreiben allgemein nun

$$p = q \cdot 8 + r \text{ mit } r \in \{-3, -1, 1, 3\}.$$

Dann gilt

$$\begin{aligned} p^2 - 1 &= 8(q^2 8 + 2qr) + r^2 - 1 \equiv r^2 - 1 \bmod 8 \equiv 0 \bmod 8, \\ \frac{p^2 - 1}{8} &= q^2 8 + 2qr + \frac{r^2 - 1}{8} \equiv \frac{r^2 - 1}{8} \bmod 2 \end{aligned}$$

$$\text{und } \frac{r^2 - 1}{8} = \begin{cases} 0 & , \quad \text{falls } r = \pm 1, \\ 1 & , \quad \text{falls } r = \pm 3. \end{cases}$$

Also gilt die Behauptung. □

Übungen 3.1.12

(1) Berechne die quadratischen Reste modulo p für $p = 3, 5, 7, 11, 13, 17, 19, 23$.

(2) Berechne $(\frac{2}{3})$, $(\frac{9}{17})$, $(\frac{19}{23})$, $(\frac{-1}{37})$, $(\frac{21}{37})$.

(3) Beweise mit Hilfe des Gaußschen Lemmas

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & , \quad \text{falls } p \equiv \pm 5 \bmod 12 \\ -1 & , \quad \text{falls } p \equiv \pm 1 \bmod 12. \end{cases}$$

(4) Beweise: $(\frac{-3}{p}) = 1 \Longrightarrow p \equiv 1 \bmod 3$

(5) Für welche $m \in \mathbb{N}_+$ hat die Kongruenz

$$x^2 \equiv 2 \bmod m$$

eine Lösung? (Hinweis: Chinesischer Restsatz)

(6) Beweise mit Hilfe von Aufgabe 3

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$$

für alle Primzahlen $p \geq 5$.

(7) (Für ***Mathematica*** -Fans)

Schreibe ein Programm, welches $(\frac{a}{p})$ mit Hilfe des Gaußschen Lemmas berechnet. Berechne dann

$$\left(\frac{641}{48751}\right), \ \left(\frac{1001}{48673}\right).$$

3.2 Das quadratische Reziprozitätsgesetz

Satz 3.2.1 (Gaußsches quadratisches Reziprozitätsgesetz)
Seien p, q ungerade Primzahlen $p \neq q$. Dann gilt

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

d.h.

$$\begin{aligned}
\left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right), \text{ falls } p \equiv 1 \bmod 4 \text{ oder } q \equiv 1 \bmod 4 \\
\left(\frac{p}{q}\right) &= -\left(\frac{q}{p}\right), \text{ falls } p \equiv q \equiv 3 \bmod 4.
\end{aligned}$$

Beweis: Wir geben zwei der vielen Beweise für diesen Satz.
1. Beweis: Es sei s die Anzahl der Elemente von $\{q,\, 2q,\, 3q, \ldots, \frac{p-1}{2}\cdot q\}$ mit negativem absolut kleinstem Rest. Es gilt

$$\nu q = \left[\frac{\nu q}{p}\right] p + r_\nu \text{ mit } 0 \leq r_\nu < p$$

und

$$\begin{aligned}
q\frac{p^2-1}{8} &= \sum_{\nu=1}^{\frac{p-1}{2}} \nu q = \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{\nu q}{p}\right] p + \sum_{\nu=1}^{\frac{p-1}{2}} r_\nu \\
&= \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{\nu q}{p}\right] p + \sum_{r_\nu > \frac{p-1}{2}} (r_\nu - p) + sp + \sum_{r_\nu \leq \frac{p-1}{2}} r_\nu \\
&\equiv \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{\nu q}{p}\right] + s + \sum_{r_\nu > \frac{p-1}{2}} (p - r_\nu) + \sum_{r_\nu \leq \frac{p-1}{2}} r_\nu \bmod 2,
\end{aligned}$$

Die beiden letzten Summanden stellen die Summe aller Zahlen j mit $1 \leq j \leq \frac{p-1}{2}$ dar, weil die $p-1$ Zahlen $\pm r_\nu \equiv \pm \nu q,\ \nu = 1, \ldots, \frac{p-1}{2}$, paarweise inkongruent modulo p sind, also

$$\{1, \ldots, \frac{p-1}{2}\} = \{p - r_\nu \mid r_\nu > \frac{p-1}{2}\} \cup \{r_\nu \mid r_\nu \leq \frac{p-1}{2}\}.$$

Da $\sum\limits_{j=1}^{\frac{p-1}{2}} j = \frac{p^2-1}{8}$, folgt

$$\begin{aligned} q\frac{p^2-1}{8} &\equiv \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{\nu q}{p}\right] + s + \frac{p^2-1}{8} \operatorname{mod}, \text{ also} \\ 0 \equiv (q-1)\frac{p^2-1}{8} &\equiv \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{\nu q}{p}\right] + s \bmod 2, \text{ d.h.} \\ s &\equiv \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{\nu q}{p}\right] \bmod 2. \end{aligned}$$

Nach dem Gaußschen Lemma folgt

$$\left(\frac{q}{p}\right) = (-1)^{\sum\limits_{\nu=1}^{\frac{p-1}{2}}\left[\frac{q\nu}{p}\right]}$$

und analog

$$\left(\frac{p}{q}\right) = (-1)^{\sum\limits_{\mu=1}^{\frac{q-1}{2}}\left[\frac{p\mu}{q}\right]}.$$

Es bleibt jetzt nur noch zu zeigen, daß

$$(*) \qquad \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{q\nu}{p}\right] + \sum_{\mu=1}^{\frac{q-1}{2}} \left[\frac{p\mu}{q}\right] = \frac{p-1}{2}\ \frac{q-1}{2}$$

Dies ist ein einfaches Abzählargument.
$\frac{p-1}{2} - \frac{q-1}{2} = \#M$, wobei M das Rechteckgitter

$$M = \{(\nu,\mu) \in \mathbb{Z}^2 \mid 1 \le \nu \le \frac{p-1}{2},\ 1 \le \mu \le \frac{q-1}{2}\{\subset \mathbb{R}^2.$$

Die Gerade $y = \frac{q}{p}x$ trifft die Menge M nicht und teilte M in zwei disjunkte Teilmengen

$$\begin{aligned} M_1 &= \{(\nu\mu) \in M \mid \mu < \frac{q}{p}\nu\} \text{ und} \\ M_2 &= \{(\nu\mu) \in M \mid \mu > \frac{q}{p}\nu\} = \{(\nu\mu) \in M \mid \nu\frac{p}{q}\mu\}. \end{aligned}$$

Es gilt

$$\#M_1 = \sum_{\nu=1}^{\frac{p-1}{2}} \left[\frac{q\nu}{p}\right] \text{ und } \#M_2 = \sum_{\mu=1}^{\frac{q-1}{2}} \left[\frac{p\mu}{q}\right].$$

2. Beweis: (nach Eisenstein)
Zunächst beweisen wir

Lemma 3.2.2 Sei $m \in \mathbb{N}$ ungerade. Dann gilt

$$\frac{\sin mx}{\sin x} = (-1)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin^2 x - \sin^2 \frac{2\pi j}{m}\right).$$

Beweis:

(1) Durch Induktion nach k $(m = 2k+1)$ zeigen wir:

Es gibt Polynome F_m und G_m in $\mathbb{R}[y]$ vom Grad $k = \frac{m-1}{2}$ und mit Leitkoeffizient $(-4)^k$, so daß

$$\begin{aligned} F_m(sin^2 x) &= \frac{\sin mx}{\sin x} \quad \text{und} \\ G_m(\sin^2 x) &= \frac{\cos mx}{\cos x}. \end{aligned}$$

Für $k = 0$, d.h. $m = 1$, können wir $F_1 = G_1 = 1$ wählen.

Seien F_m, G_m schon konstruiert, $m = 2k+1$. Wir konstruieren F_{m+2} und G_{m+2}: $(m+2 = 2(k+1)+1)$

$$\begin{aligned} \frac{\sin(m+2)x}{\sin x} &= \frac{\sin mx \cos 2x + \cos mx \sin 2x}{\sin x} \\ &= \frac{\sin mx}{\sin x}(1 - 2\sin^2 x) + \frac{\cos mx}{\cos x}\,\frac{\cos x}{\sin x} 2 \sin x \cos x \\ &= F_m(\sin^2 x)(1 - 2\sin^2 x) + G_m(\sin^2 x)(2 - 2\sin^2 x) \end{aligned}$$

Also kann man

$$F_{m+2} = F_m \cdot (1 - 2y) + G_m \cdot (2 - 2y)$$

wählen. Es gilt

$$\text{grad } F_{m+2} = \text{grad } F_m + 1 = k + 1$$

und

$$\begin{aligned} \text{Leitkoeffizient } F_{m+2} &= (-4) \cdot \text{Leitkoeffizient } F_m \\ &= (-4)^{k+1}. \end{aligned}$$

Analog findet man G_{m+2}.

(2) Es gilt nun für $m = 2k+1$ und $j = 1, \ldots, k$

$$F_m\left(\sin^2 \frac{2\pi j}{m}\right) = \frac{\sin 2\pi j}{\sin \frac{2\pi j}{m}} = 0.$$

Also sind

$$\sin^2 \frac{2\pi j}{m}, \sin^2 \frac{4\pi}{m}, \ldots, \sin^2 \frac{2k\pi}{m}$$

Nullstellen von F_m. Zeigen wir noch, daß diese paarweise verschieden sind, so folgt

$$F_m = (-4)^k \prod_{j=1}^{k} \left(y - \sin^2 \frac{2\pi j}{m}\right)$$

und durch Einsetzen von $y = \sin^2 x$ die gesuchte Formel.

Seien $j_1, j_2 \in \{1, \dots, k\}$ und

$$\sin^2 \frac{2\pi j_1}{m} = \sin^2 \frac{2\pi j_2}{m}.$$

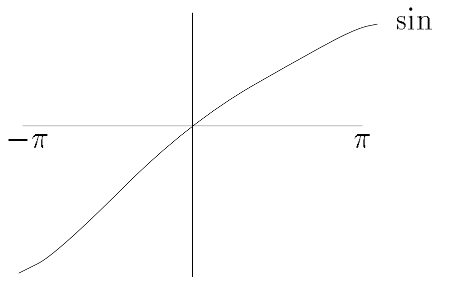
Dann gilt

$$\sin \frac{2\pi j_1}{m} = \pm \sin \frac{2\pi j_2}{m}$$

also

$$\sin \frac{2\pi j_1}{m} = \sin \pm \frac{2\pi j_2}{m}.$$

Da $0 < \frac{2\pi j_1}{m}, \frac{2\pi j_2}{m} \leq \frac{\pi 2k}{2k+1} < \pi$ und



sin auf $[-\pi, \pi]$ injektiv ist, folgt $j_1 = j_2$. Damit ist gezeigt, daß die Werte

$$\sin^2 \frac{2\pi j}{m}, \; j = 1, \dots, k$$

paarweise verschieden sind. □

Jetzt kommen wir zum Eisensteinschen Beweis.
Ist $a \in \mathbb{Z}$ und $a \not\equiv 0 \bmod q$, so bezeichnen wir mit

$$e(a, \mu)$$

das Signum (Vorzeichen) des absolut kleinsten Restes von $a\mu$ modulo q. Nach dem Gaußschen Lemma gilt also

$$\left(\frac{a}{q}\right) = \prod_{\mu=1}^{\frac{q-2}{2}} e(a, \mu).$$

Sei nun für $1 \leq \mu \leq \frac{q-1}{2}$ mit μ_a der Absolutbetrag des absolut kleinsten Restes von $a\mu$ modulo q bezeichnet.
$\mu_a = \mathrm{Abs}[\mathrm{akrest}[a\mu, q]]$
Dann gilt

$$a\mu \equiv e(a, \mu)\mu_a \bmod q$$

und somit für $a = p :$

$$\sin \frac{2\pi p\mu}{q} = e(p, \mu) \sin \frac{2\pi \mu_p}{q}$$

Da die Abbildung $\mu \longmapsto \mu_p$ eine Permutation von $\{1, \ldots, \frac{q-1}{2}\}$ ist, folgt weiter

$$\begin{aligned}
\left(\frac{p}{q}\right) &= \prod_{\mu=1}^{\frac{q-1}{2}} e(p,\mu) = \prod_{\mu=1}^{\frac{q-1}{2}} \sin\frac{2\pi p\mu}{q} \Big/ \sin\frac{2\pi\mu_p}{q} \\
&= \prod_{\mu=1}^{\frac{q-1}{2}} \sin\frac{2\pi\mu}{q}p \Big/ \sin\frac{2\pi\mu}{q} \\
&= \prod_{\mu=1}^{\frac{q-1}{2}} (-4)^{\frac{p-1}{2}} \prod_{\nu=1}^{\frac{q-1}{2}} \left(\sin^2\frac{2\pi\mu}{q} - \sin^2\frac{2\pi\nu}{p}\right) \\
&= (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{\mu=1}^{\frac{q-1}{2}} \prod_{\nu=1}^{\frac{q-1}{2}} \left(\sin^2\frac{2\pi\mu}{q} - \sin^2\frac{2\pi\nu}{p}\right) \\
&= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} (-4)^{\frac{p-1}{2}\frac{q-1}{2}} \prod_{\nu=1}^{\frac{p-1}{2}} \prod_{\mu=1}^{\frac{q-1}{2}} \left(\sin^2\frac{2\pi\nu}{p} - \sin^2\frac{2\pi\mu}{q}\right) \\
&= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).
\end{aligned}$$

□

Beispiel 3.2.3 $p = 641,\ q = 37$ sind Primzahlen, $\frac{p-1}{2} = 320,\ \frac{q-1}{2} = 18.$
Es folgt also

$$\begin{aligned}
\left(\frac{37}{641}\right) &= \left(\frac{641}{37}\right) = \left(\frac{641-740}{37}\right) = \left(\frac{-99}{37}\right) = \left(\frac{-11}{37}\right) \\
&= \left(\frac{-1}{37}\right)\left(\frac{11}{37}\right) = \left(\frac{37}{11}\right) = \left(\frac{4}{11}\right) = 1
\end{aligned}$$

Damit ist die Kongruenz

$$x^2 \equiv 37 \bmod 641$$

lösbar. Die Lösungen erhalten wir durch

$$x/.\mathrm{Solve}[x^2 == 37\&\&\mathrm{Modulus} == 641,\ x] = \{-590, -51\}.$$

Das Legendresymbol $(\frac{q}{p})$ ist für alle $a \in \mathbb{Z}$ aber nur für Primzahlen $p > 2$ definiert. Einer Zahl p sieht man aber nicht so ohne weiteres an, ob sie eine Primzahl ist. Da jede ungerade Zahl $b \in \mathbb{N}$ ein Produkt

$$b = \prod_{i=1}^{r} p_i$$

von Primzahlen $p_1, \ldots, p_r$ ist ($r = 0$ bedeutet: $b = 1 =$ leeres Produkt) kann man die Funktion

$$p \longmapsto \left(\frac{a}{p}\right)$$

von der Menge der ungeraden Primzahlen auf das Monoid $\mathbb{U} = 2\mathbb{N}+1$ der positiven ungeraden Zahlen fortsetzen.

Definition 3.2.4 Ist $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ ungerade, $b = \prod_{i=1}^{r} p_i$ die Primfaktorzerlegung von b, so sei

$$\left(\frac{a}{b}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right).$$

$(\frac{a}{b})$ heißt das **Jacobisymbol**.
Für festes $a \in \mathbb{Z}$ ist also die Funktion $b \longmapsto (\frac{a}{b})$ ein Homomorphismus $(\mathbb{U}, \cdot) \longrightarrow (\{-1, 0, 1\}, \cdot)$ von Monoiden, wobei $\mathbb{U}$ die Menge der positiven ungeraden Zahlen bezeichne. $\mathbb{U}$ wird als multiplikatives Monoid von den ungeraden Primzahlen erzeugt. Es gilt $(\frac{a}{1}) = 1$ für alle $a \in \mathbb{Z}$.

Bemerkung 3.2.5 Es sei $a \in \mathbb{Z}$ und $b \in \mathbb{N}$, $b \not\equiv 0 \bmod 2$. Gilt $(\frac{a}{b}) = 1$, so ist die Kongruenz

$$x^2 \equiv a \bmod b$$

nicht lösbar, denn: wenn $(\frac{a}{b}) = -1$, gibt es einen Primteiler p von b mit $(\frac{a}{p}) = -1$. Also ist sogar $x^2 \equiv a \bmod p$ nicht lösbar.
Ist dagegen $(\frac{a}{b}) = 1$, b keine Primzahl, so kann $x^2 \equiv a \bmod b$ ebenfalls nicht lösbar sein. Man wähle zum Beispiel $b = p^2$, p Primzahl, $p \neq 2$.

Lemma 3.2.6 Seien $a, b \in \mathbb{Z}$, $m, n \in \mathbb{N}$ ungerade.
Dann gilt

(1) $(\frac{ab}{m}) = (\frac{a}{m})(\frac{b}{m})$

(2) $a \equiv b \bmod m \Longrightarrow (\frac{a}{m}) = (\frac{b}{m})$

(3) $(\frac{a}{m}) \neq 0 \Longleftrightarrow (a, m) = 1$

(4) $(\frac{a}{mn}) = (\frac{a}{m})(\frac{a}{n})$

(5) $(\frac{-1}{m}) = (-1)^{\frac{m-1}{2}}$, $(\frac{2}{m}) = (-1)^{\frac{m^2-1}{8}}$

Beweis: (1) – (4) ergeben sich aus der Definition des Jacobisymbols und den entsprechenden Eigenschaften des Legendresymbols.
(1), (2) und (3) bedeuten, daß für festes m durch $a \longmapsto (\frac{a}{m})$ ein Gruppenhomomorphismus

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^{\times} &\longrightarrow \{-1, 1\} \\ a \bmod m &\longmapsto \left(\frac{a}{m}\right) \end{aligned}$$

induziert wird.
Zu (5): Sei $m = kl$. Dann sind k, l ungerade, also $0 \equiv (k-1)(l-1) = m-k-l+1 \bmod 4$ und somit $m - 1 \equiv k - 1 + l - 1 \bmod 4$ und $\frac{m-1}{2} \equiv \frac{k-1}{2} + \frac{l-1}{2} \bmod 2$. Es folgt

$$(-1)^{\frac{m-1}{2}} = (-1)^{\frac{k-1}{2}}(-1)^{\frac{l-1}{2}}.$$

Da weiter

$$\left(\frac{a}{m}\right) = \left(\frac{a}{k}\right) \cdot \left(\frac{a}{l}\right),$$

folgt jetzt durch Induktion nach m sofort

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}.$$

Analog gilt

$$m^2 - 1 = (k^2-1)(l^2-1) + k^2 - 1 + l^2 - 1 \equiv k^2 - 1 + l^2 - 1 \bmod 8,$$

woraus man wieder durch Induktion nach m

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

folgert. □

Das quadratische Reziprozitätsgesetz impliziert

Lemma 3.2.7 Seien $m, n \in \mathbb{N}$ ungerade. Dann gilt

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}, \text{ falls } (m,n) = 1.$$

Beweis: Es seien $m = \prod_{i-1}^{r} p_i,\ n = \prod_{j=1}^{s} q_j$ die Primfaktorzerlegungen von m und n. Dann gilt $p_i \neq q_j$, also

$$\begin{aligned}
\left(\frac{m}{n}\right) &= \prod_{i,j}\left(\frac{p_i}{q_j}\right) = \prod_{i,j}(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}\left(\frac{q_j}{p_i}\right) \\
&= (-1)^{\sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2}}\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right), \\
\text{weil} \quad & \sum_{i,j}\frac{p_i-1}{2}\frac{q_j-1}{2} = \sum_i \frac{p_i-1}{2}\sum_j\frac{q_j-1}{2} \\
&\equiv \frac{m-1}{2}\ \frac{n-1}{2} \bmod 2.
\end{aligned}$$

□

Beispiel 3.2.8 405 und 1001 sind keine Primzahlen. Nach Lemma 3.2.7 kann man das Jacobisymbol $(\frac{405}{1001})$ nach dem Reziprozitätsgesetz berechnen, da

$$(405, 1001) = (405, 191) = (23, 191) = (23, 7) = (2, 7) = (2, 1) = 1.$$

Es gilt

$$\begin{aligned}
\left(\frac{405}{1001}\right) &= \left(\frac{1001}{405}\right) = \left(\frac{191}{405}\right) = \left(\frac{404}{191}\right) = \left(\frac{23}{191}\right) = -\left(\frac{191}{23}\right) \\
&= -\left(\frac{7}{23}\right) = \left(\frac{23}{7}\right) = \left(\frac{2}{7}\right) = (-1)^6 = 1
\end{aligned}$$

Als kleine Anwendung des Jacobisymbols zeigen wir

Satz 3.2.9 Ist $a \in \mathbb{Z}$ keine Quadratzahl, so gibt es eine Primzahl p, so daß $(\frac{a}{p}) = -1$, also a kein quadratischer Rest modulo p ist.

Beweis: Sei $a \in \mathbb{Z}$, $a \neq b^2$ für alle $b \in \mathbb{Z}$.
1. Fall.
$$a = -b^2 \text{ für ein } b \in \mathbb{Z}$$
Für eine ungerade positive Zahl $k \geq 3$ mit $(b, k) = 1$ gilt dann
$$\left(\frac{a}{k}\right) = \left(\frac{-b^2}{k}\right) = \left(\frac{-1}{k}\right) = (-1)^{\frac{k-1}{2}}.$$
Wir wählen $k \equiv 3 \bmod 4$ und teilerfremd zu b. Dann gilt
$$\left(\frac{a}{k}\right) = -1.$$
Für wenigstens einen Primfaktor p von k gilt dann
$$\left(\frac{a}{p}\right) = -1.$$
2. Fall.
$a = \pm 2^t b$ mit $t, b \in \mathbb{N}_+$ ungerade. Ist $b = 1$, so sei $k = 5$. Ist $b > 1$, so sei $k \in \mathbb{N}_+$ mit
$$\begin{aligned} k &\equiv 5 \bmod 8 \\ k &\equiv 1 \bmod b. \end{aligned}$$
Dann gilt
$$\left(\frac{\pm 2^t}{k}\right) = \left(\frac{\pm 2}{k}\right) = \left(\frac{\pm 1}{k}\right)\left(\frac{2}{k}\right) = \left(\frac{2}{k}\right) = (-1)^{\frac{k^2-1}{8}} = -1,$$
weil $k = 8l + 5$, also $k^2 = 64l^2 + 80l + 25 = 8(8l^2 + 10l + 3) + 1$ und somit $\frac{k^2-1}{8} = 8l^2 + 10l + 3$ ungerade.
Weiter ist
$$\left(\frac{b}{k}\right) = \left(\frac{k}{b}\right) = \left(\frac{1}{b}\right) = 1.$$
Es folgt
$$\left(\frac{a}{k}\right) = \left(\frac{\pm 2^t}{k}\right)\left(\frac{b}{k}\right) = -1.$$
3. Fall.
$a = \pm 2^{2s} q^t b$, wobei t, b positive ungerade Zahlen sind, q Primzahl, $q \neq 2$ und $(q, b) = 1$. Dann sei $k \in \mathbb{N}_+$ mit
$$\begin{aligned} k &\equiv 1 \bmod 4b \\ k &\equiv c \bmod q \end{aligned}$$

wobei c ein quadratischer Nichtrest modulo q sei. Dann gilt

$$\left(\frac{\pm 2^{2s}}{k}\right) = \left(\frac{\pm 1}{k}\right) = 1,$$

weil $\frac{k-1}{2}$ gerade ist.

$$\left(\frac{b}{k}\right) = \left(\frac{k}{b}\right) = \left(\frac{1}{b}\right) = 1$$

und weil t ungerade ist, folgt

$$\left(\frac{q^t}{k}\right) = \left(\frac{q}{k}\right) = \left(\frac{k}{q}\right) = \left(\frac{c}{q}\right) = -1.$$

Also ist auch

$$\left(\frac{a}{k}\right) = \left(\frac{\pm 2^{2s}}{k}\right)\left(\frac{b}{k}\right)\left(\frac{q^t}{k}\right) = -1.$$

□

Übungen 3.2.10

(1) 311, 467, 587, 661, 761, 887, 997 sind Primzahlen. Berechne die Legendresymbole

$$\left(\frac{311}{467}\right), \left(\frac{661}{761}\right), \left(\frac{587}{887}\right), \left(\frac{997}{311}\right), \left(\frac{467}{997}\right), \left(\frac{887}{997}\right)$$

(2) Welche der folgenden Kongruenzen sind lösbar.

(a) $x^2 \equiv 4977 \bmod 1997$

(b) $x^2 + 4x - 262 \equiv 0 \bmod 173$

(c) $3x^2 + 5x + 1 \equiv 0 \bmod 37$

(d) $15x^2 - 6x + 7 \equiv 0 \bmod 59$

(3) Welche der folgenden diophantischen Gleichungen ist in $\mathbb{Z}^2$ lösbar?

(a) $2x^2 + 3y + 5 = 0$

(b) $6x^2 - 17y + 100 = 0$

(c) $x^2 + 43y + 40 = 0$

(d) $x^2 + 4999y + 100000 = 0$

(4) Beweise

$$y^2 = x^3 + 45$$

besitzt keine Lösung in $\mathbb{Z}^2$.

Hinweis: Schließe zunächst die Fälle $x \equiv 0 \bmod 2$, $x \equiv 1 \bmod 4$ aus. Für den Fall $x \equiv -1 \bmod 8$ betrachte die Umformung

$$y^2 - 2 \cdot 9 = (x+3)(x^2 - 3x + 9)$$

und beweise die Existenz eines Primfaktors p von x^2-3x+9 mit $p \equiv \pm 3 \bmod 8$, und untersuche

$$y^2 - 2 \cdot 9 \equiv 0 \bmod p.$$

Im letzten Fall $x \equiv 3 \bmod 8$ betrachte man die Umformung

$$y^2 - 2 \cdot 36 = (x-3)(x^2+3x+9)$$

und verfahre analog.

(5) Sei p eine ungerade Primzahl. Zeige:

(a) $\sum\limits_{a=1}^{p-1} \left(\dfrac{a}{p}\right) = 0$

(b) $\sum\limits_{i=1}^{p-2} \left(\dfrac{i(i+1)}{p}\right) = -1$

(6) (Beweis des quadratischen Reziprozitätsgesetzes mit Hilfe des chinesischen Restsatzes)

Seien p, q ungerade Primzahlen, $p \neq q$. $U = \{\pm\{1,1\}\}$ ist Untergruppe von $G = \mathbb{F}_p^\times \times \mathbb{F}_q^\times$. $Q = G/U$ sei die Faktorgruppe. Beweise:

(a) Das Produkt über alle Elemente von Q wird durch das Paar

$$X := \{(p-1)!^{\frac{q-1}{2}},\ (q-1)!^{\frac{q-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\}$$

repräsentiert. Dazu zeige, daß die Paare (i,j), $i = 1, \ldots, p-1$; $j = 1, \ldots, \frac{q-1}{2}$ ein vollständiges Repräsentantensystem für die Elemente von Q bilden.

(b) $L = \{\{\mathrm{Mod}[t,p], \mathrm{Mod}[t,q]\} \mid 1 \leq t \leq \frac{pq-1}{2}, (t,pq) = 1\}$ ist ebenfalls ein vollständiges Repräsentantensystem für die Gruppe Q (d.h. die Komposition der Abbildungen

$$L \subset \{\{x,y\} \in \mathbb{Z}^2 \mid x \not\equiv 0 \bmod p,\ y \not\equiv 0 \bmod q\} \longrightarrow F_p^\times \times \mathbb{F}_q^\times \longrightarrow Q$$

ist eine Bijektion $L \longrightarrow Q$).

Zeige, daß das Produkt aller Elemente von Q auch durch das Paar

$$Y = \{\mathrm{Mod}[A,p],\ \mathrm{Mod}[A,q]\}$$

repräsentiert wird, wobei

$$A = \prod_{\substack{t=1\\(t,pq)=1}}^{\frac{pq-1}{2}} t = \prod_{\nu=0}^{\frac{q-1}{2}} \prod_{\mu=1}^{p-1} (\nu p + \mu) \cdot \prod_{\mu=1}^{\frac{p-1}{2}} \left(\frac{q-1}{2}p + \mu\right) \Big/ \prod_{\mu=1}^{\frac{p-1}{2}} \mu q.$$

Folgere

$$A \equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \bmod p$$

und durch Symmetrieüberlegungen

$$A \equiv (q-1)!^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \bmod q.$$

(c) Beweise, daß $x^p - 1 - \prod_{\mu=1}^{p-1}(x-\mu) \in \mathbb{F}_p[x]$ das Nullpolynom ist, und schließe daraus

$$(p-1)! \equiv -1 \bmod p.$$

Analog gilt natürlich $(q-1)! \equiv -1 \bmod q$.

(d) Aus (a) -(c) folgere man das quadratische Reziprozitätsgesetz.

(7) (Eine Variante des Eisensteinschen Beweises)

Sei $f(z) = 2i \sin 2\pi z = e^{2\pi i z} - e^{-2\pi i z}$.

(a) Für $m \in \mathbb{N}$ ungerade beweise:

$$\frac{f(mz)}{f(z)} = \prod_{j=1}^{\frac{m-1}{2}} f\left(z + \frac{j}{m}\right) f\left(z - \frac{j}{m}\right)$$

(b) Ist p ungerade Primzahl und $a \not\equiv 0 \bmod p$, so folgere man aus dem Gaußschen Lemma

$$\prod_{j=1}^{\frac{p-1}{2}} f\left(\frac{ja}{p}\right) = \left(\frac{a}{p}\right) \prod_{j=1}^{\frac{p-1}{2}} f\left(\frac{j}{p}\right)$$

(c) Beweise nun das quadratische Reziprozitätsgesetz analog zum zweiten Beweis von 3.2.1.

(8) (für ***Mathematica*** -Fans)

Schreibe ein Programm zum Jacobisymbol mit Hilfe von 3.2.6 (2), (3), (5) und 3.2.7.

Kapitel 4

Algebraische Methoden

4.1 Algebraische Zahlen

$\mathbb{C}$ ist der Körper der komplexen Zahlen.

Definition 4.1.1 Sei $\alpha \in \mathbb{C}$.

(1) α heißt **algebraische Zahl**, wenn ein normiertes Polynom $f \in \mathbb{Q}[x]$ mit $f(\alpha) = 0$ existiert.

(2) α heißt **ganze algebraische Zahl**, wenn ein normiertes Polynom $f \in \mathbb{Z}[x]$ mit $f(\alpha) = 0$ existiert.

Lemma 4.1.2 Es gilt

(1) Ist $\alpha \in \mathbb{Q}$ ganz algebraisch, so ist $\alpha \in \mathbb{Z}$.

(2) Ist $\alpha \in \mathbb{C}$ algebraisch, so gibt es ein $c \in \mathbb{Z}$, so daß $c\alpha$ ganz algebraisch ist.

Beweis:

(1) Es sei $\alpha \neq 0$ und $\alpha = \frac{a}{b}$ mit $a, b \in \mathbb{Z}$, $(a, b) = 1$. Ist nun α ganz algebraisch, so gibt es ganze Zahlen $a_1, \ldots, a_k \in \mathbb{Z}$, so daß

$$\alpha^k + a_1\alpha^{k-1} + \cdots + a_k = 0.$$

Es folgt

$$a^k + a_1 a^{k-1} b + \cdots + a_k b^k = 0$$

und somit ist b ein Teiler von a^k, also $b = \pm 1$, weil $(a, b) = 1$. Somit ist $\alpha = \pm a \in \mathbb{Z}$.

(2) Seien $a_i,\ c \in \mathbb{Z}$ und

$$\alpha^k + \frac{a_1}{c}\alpha^{k-1} + \cdots + \frac{a_k}{c} = 0.$$

Durch Multiplizieren mit c^k folgt

$$(c\alpha)^k + a_1(c\alpha)^{k-1} + a_2 c(c\alpha)^{k-2} + \cdots + a_k c^{k-1} = 0,$$

d.h. $c\alpha$ ist ganz algebraisch.

$\square$

Sehr wichtig ist folgender

Satz 4.1.3 Seien $\beta_1, \ldots, \beta_m \in \mathbb{C}$.
$V = \mathbb{Q}\beta_1 + \cdots + \mathbb{Q}\beta_m$ sei der von $\beta_1, \ldots, \beta_m$ erzeugte $\mathbb{Q}$-Untervektorraum von $\mathbb{C}$. Es sei $V \neq 0$. Dann gilt:
Ist $\alpha \in \mathbb{C}$ und gilt $\alpha V \subset V$, so ist α algebraisch.

Beweis: $\alpha V \subset V \Longrightarrow \ \exists\ a_{ij} \in \mathbb{Q}$, so daß

$$\alpha\beta_i = \sum_{j=1}^{m} a_{ij}\beta_j \ \text{ für alle } i = 1, \ldots, m.$$

Da $(\beta_1, \ldots, \beta_m) \neq 0$, folgt $\det(a_{ij} - \delta_{ij}\alpha) = 0$. Entwickelt man die Determinante, so erhält man eine algebraische Relation für α. Also ist α algebraisch. □

Analog ergibt sich

Satz 4.1.4 Seien $\beta_1, \ldots, \beta_m \in \mathbb{C}$ und $M = \mathbb{Z}\beta_1 + \cdots + \mathbb{Z}\beta_m$ die von $\beta_1, \ldots, \beta_m$ erzeugte Untergruppe von $(\mathbb{C}, +)$. Es sei $M \neq 0$. Dann gilt: Ist $\alpha \in \mathbb{C}$ mit $\alpha M \subset M$, so ist α ganz algebraisch.

Beweis: Der Beweis geht genauso wie der von Satz 4.1.3. Jetzt sind aber die $a_{ij} \in \mathbb{Z}$ und somit liefert $\det(a_{ij} - \delta_{ij}\alpha) = 0$ eine 'Ganzheitsrelation' für α. □

Es folgt der wichtige Satz

Satz 4.1.5 (a) Die Menge $\mathbb{A}$ aller algebraischen Zahlen $\alpha \in \mathbb{C}$ ist ein Unterkörper von $\mathbb{C}$.
(b) Die Menge $\mathbb{I}$ aller ganzen algebraischen Zahlen $\alpha \in \mathbb{C}$ ist ein Unterring von $\mathbb{C}$.

Beweis:

(1) Seien $\alpha, \beta \in \mathbb{A}$ und $a_i, b_j \in \mathbb{Q}$, so daß

   (a) $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$
   (b) $\beta^m + b_1\beta^{m-1} + \cdots + b_m = 0.$

   Es sei V der von den Elementen

$$\gamma_{ij} := \alpha^i\beta^j,\ 0 \leq i < n,\ 0 \leq j < m$$

   erzeugte $\mathbb{Q}$-Untervektorraum von $\mathbb{C}$.

   Wegen (a) und (b) gilt dann

$$\alpha V \subset V \text{ und } \beta V \subset V$$

   und somit auch

$$(\alpha + \beta)V \subset V \text{ und } \alpha\beta V \subset V.$$

   Nach 4.1.3 sind daher $\alpha + \beta$ und $\alpha\beta$ algebraisch. Weiter folgt im Fall $\alpha \neq 0$ aus (a)

$$a_n\alpha^{-n} + a_{n-1}\alpha^{-n+1} + \cdots + a_1\alpha^{-1} + 1 = 0.$$

Dabei darf man OE $a_n \neq 0$ annehmen. Dann erhält man

$$(\alpha^{-1})^n + \frac{a_{n-1}}{a_n}(\alpha^{-1})^{n-1} + \cdots + \frac{1}{a_n} = 0,$$

d.h. α^{-1} ist algebraisch. Damit ist $\mathbb{A}$ Unterkörper von $\mathbb{C}$.

(2) Seien $\alpha, \beta \in \mathbb{I}$ und es gelte (a) und (b) mit $a_i, b_j \in \mathbb{Z}$. M sei von den Elementen $\gamma_{ij} = \alpha^i\beta^j$, $0 \leq i < n$, $0 \leq j < m$ erzeugte additive Untergruppe von $\mathbb{C}$. Wieder folgt

$$(\alpha + \beta)M \subset M, \alpha\beta M \subset M$$

und nach 4.1.4 somit $\alpha + \beta$, $\alpha\beta \in \mathbb{I}$. Damit ist $\mathbb{I}$ Unterring von $\mathbb{C}$.

Satz 4.1.6 Zu jeder algebraischen Zahl $\alpha \in \mathbb{A}$ gibt es genau ein normiertes irreduzibles Polynom $f \in \mathbb{Q}[x]$, so daß $f(\alpha) = 0$.

Beweis: Es sei $f \in \mathbb{Q}[x]$ ein normiertes Polynom minimalen Grades mit $f(\alpha) = 0$. Da α algebraisch ist, existiert f.

Behauptung: f ist irreduzibel.

Sei dazu $f = q \cdot g$ mit $q, g \in \mathbb{Q}[x]$. Es folgt $0 = f(\alpha) = q(\alpha)g(\alpha)$, also ist $g(\alpha) = 0$ oder $q(\alpha) = 0$ und somit $\operatorname{grad} g \geq \operatorname{grad} f$ oder $\operatorname{grad} q \geq \operatorname{grad} f$. Da aber $\operatorname{grad} f = \operatorname{grad} g + \operatorname{grad} q$, bedeutet das: $\operatorname{grad} q = 0$ oder $\operatorname{grad} g = 0$, also ist q oder g Einheit in $\mathbb{Q}[x]$. Ist nun $\widetilde{f}$ ein weiteres irreduzibles Polynom mit $\widetilde{f}(\alpha) = 0$, so ergibt Division mit Rest

$$\widetilde{f} = qf + r \quad \text{mit } \operatorname{grad} r < \operatorname{grad} f.$$

Da $f(\alpha) = \widetilde{f}(\alpha) = 0$, ist auch $r(\alpha) = 0$ und nach Wahl von f somit $r = 0$, d.h. $\widetilde{f} = qf$. Da $\widetilde{f}$ irreduzibel und normiert ist, muß $q = 1$ gelten, also

$$f = \widetilde{f}.$$

Damit ist der Satz bewiesen. □

Definition 4.1.7 Sei $\alpha \in \mathbb{A}$ und $f \in \mathbb{Q}[x]$ das irreduzible normierte Polynom mit $f(\alpha) = 0$.

(1) f heißt das **Minimalpolynom** von α.

(2) $\operatorname{grad} \alpha = \operatorname{grad} f$ heißt der **Grad** von α.

(3) $\beta \in \mathbb{A}$ heißt zu α **konjugiert**, wenn $f(\beta) = 0$.

Wir benutzen den Fundamentalsatz der Algebra, der besagt, daß jedes nichtkonstante Polynom $f \in \mathbb{C}[x]$ eine komplexe Nullstelle besitzt, also in Linearfaktoren zerfällt.

Lemma 4.1.8 Sei $f \in \mathbb{Q}[x]$ normiertes irreduzibles Polynom vom Grad $n \geq 1$. Dann besitzt f genau n verschiedene Nullstellen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$.

Beweis: Wir müssen (wegen des Fundamentalsatzes der Algebra) nur zeigen, daß alle Nullstellen von f einfach sind, d.h. ist

$$f(\alpha) = 0, \quad \text{so ist } f'(\alpha) \neq 0.$$

Da die Ableitung f' von f den Grad $n-1$ hat, sind f und f' teilerfremd und der erweiterte euklidische Algorithmus in $\mathbb{Q}[x]$ gibt uns eine Darstellung

$$1 = af + bf' \text{ mit } a, b \in \mathbb{Q}[x].$$

Da $f(\alpha) = 0$, muß daher $f'(\alpha) \neq 0$ gelten. □

Eine algebraische Zahl α vom Grad n hat also (einschließlich α) n verschiedene konjugierte Zahlen $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ und

$$f = (x - \alpha_1) \ldots (x - \alpha_n)$$

ist das Minimalpolynom von α in $\mathbb{Q}[x]$.

Satz 4.1.9 Es sei $\alpha \in \mathbb{A}$, $\operatorname{grad} \alpha = n$ und

$$\mathbb{Q}[\alpha] := \{p(\alpha) \mid p \in \mathbb{Q}[x]\}.$$

Dann ist $\mathbb{Q}[\alpha]$ ein Unterkörper von $\mathbb{A}$ und $(1, \alpha, \ldots, \alpha^{n-1})$ ist eine $\mathbb{Q}$-Vektorraumbasis von $\mathbb{Q}[\alpha]$.

Beweis: $\mathbb{Q}[\alpha]$ ist das Bild des Ringhomomorphismus

$$\mathbb{Q}[x] \longrightarrow \mathbb{C}, \ p \longmapsto p(\alpha).$$

Also ist $\mathbb{Q}[\alpha]$ ein Unterring von $\mathbb{C}$.

Nach Satz 4.1.3 sind alle Elemente in $\mathbb{Q}[\alpha]$ algebraisch, weil α algebraisch ist. Es sei $f = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{Q}[x]$ das Minimalpolynom von α. Dann gilt

$$\alpha^{n+k} = -a_1 \alpha^{n+k-1} - \cdots - a_n \alpha^k \text{ für } k \geq 0$$

sukzessive erhält man schließlich

$$\alpha^{n+k} \in \mathbb{Q} + \mathbb{Q}\alpha + \cdots + \mathbb{Q}\alpha^{n-1}.$$

Damit ist $(1, \alpha, \ldots, \alpha^{n-1})$ Erzeugendensystem des $\mathbb{Q}$-Vektorraums $\mathbb{Q}[\alpha]$.

$1, \alpha, \ldots, \alpha^{n-1}$ sind $\mathbb{Q}$-linear unabhängig, weil sonst ein normiertes Polynom $h \in \mathbb{Q}[x]$ vom Grad $m < n$ existieren würde mit $h(\alpha) = 0$. Wir müssen noch zeigen, daß für jedes Element $\beta \in \mathbb{Q}[\alpha]$ mit $\beta \neq 0$ auch

$$\beta^{-1} \in \mathbb{Q}[\alpha]$$

gilt.

Es sei also $\beta \in \mathbb{Q}[\alpha]$, $\beta \neq 0$. Dann existiert ein Polynom $g \in \mathbb{Q}[x]$ mit $\operatorname{grad} g < n$, so daß

$$\beta = g(\alpha).$$

Da f irreduzibel ist und $\operatorname{grad} f > \operatorname{grad} g$, sind f und g teilerfremd in $\mathbb{Q}[x]$, und somit gibt es Polynome $a, b \in \mathbb{Q}[x]$, so daß

$$1 = af + bg.$$

Durch Einsetzen von α folgt

$$1 = b(\alpha)g(\alpha),$$

also

$$g(\alpha)^{-1} = b(\alpha) \in \mathbb{Q}[\alpha].$$

$\square$

Beispiel 4.1.10 Sei $\alpha = \sqrt[3]{2} \in \mathbb{R}$. Dann ist $f = x^3 - 2$ das Minimalpolynom von α, und $\alpha, \omega\alpha, \omega^2\alpha$ sind die sämtlichen Nullstellen von f, wobei

$$\omega := \frac{-1 + \sqrt{3}\, i}{2} \in \mathbb{C}.$$

$\omega\alpha \notin \mathbb{Q}[\alpha] = \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus \mathbb{Q}\alpha^2$, weil $\omega\alpha$ nicht reell ist. $\omega\alpha$ hat natürlich ebenfalls f als Minimalpolynom, aber

$$\mathbb{Q}[\alpha] \neq \mathbb{Q}[\omega\alpha].$$

Jedoch ist $\varphi : \mathbb{Q}[\alpha] \longrightarrow \mathbb{Q}[\omega\alpha]$ mit

$$\varphi(a_0 + a_1\alpha + a_2\alpha^2) := a_0 + a_1\omega\alpha + a_2\omega^2\alpha^2$$

ein Isomorphismus von Körpern (Übung!). Der kleinste Körper, der sowohl α als auch $\omega\alpha$ enthält, ist

$$K[\omega\alpha],$$

wobei $K = \mathbb{Q}[\alpha]$. Da $\omega^2 + \omega + 1 = 0$, erhält man

$$\begin{aligned} f &= (x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha) \\ &= (x-\alpha)(x^2+\alpha x+\alpha^2), \\ g &= x^2 + \alpha x + \alpha^2 \in K[x] \end{aligned}$$

ist daher das Minimalpolynom von $\omega\alpha$ über dem Körper K. Es folgt

$$\dim_K K[\omega\alpha] = 2,$$

und $(1, \omega\alpha)$ ist eine K-Basis von $K[\omega\alpha]$. Da $(1, \alpha, \alpha^2)$ eine $\mathbb{Q}$-Basis von K ist, folgt sofort:

$$(1, \alpha, \alpha^2,\ \omega\alpha,\ \omega\alpha^2,\ \omega\alpha^3)$$

ist eine $\mathbb{Q}$-Basis von $K[\omega\alpha] = \mathbb{Q}[\alpha, \omega\alpha]$. Da $\omega^2 + \omega + 1 = 0$, ist

$$\omega^2\alpha = -\omega\alpha - \alpha \in \mathbb{Q}[\alpha, \omega\alpha]$$

und damit ist

$$\mathbb{Q}[\alpha, \omega\alpha] = \mathbb{Q} \oplus \mathbb{Q}\alpha \oplus \mathbb{Q}\alpha^2 \oplus \mathbb{Q}\omega\alpha \oplus \mathbb{Q}\omega\alpha^2 \oplus \mathbb{Q}\omega\alpha^3$$

der kleinste Körper, der alle zu α konjugierten algebraischen Zahlen enthält.
Sei nun $\vartheta := \alpha - \omega\alpha$. Dann ist $\alpha = \vartheta + \omega\alpha$ und

$$h(x) := f(\vartheta + x) \in \mathbb{Q}[\vartheta][x] \text{ mit } h(\omega\alpha) = f(\alpha) = 0.$$

Da

$$f = (x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha),$$

ist

$$\begin{aligned} h &= (\vartheta + x - \alpha)(\vartheta + x - \omega\alpha)(\vartheta + x - \omega^2\alpha) \\ &= (x-\omega\alpha)(x+\vartheta-\omega\alpha)(x-\vartheta-\omega^2\alpha) \\ &= (x-\omega\alpha)(x+\alpha-2\omega\alpha)(x+\alpha-\omega\alpha-\omega^2\alpha) \\ &= (x-\omega\alpha)(x-\alpha(2\omega-1))(x-\alpha(\omega^2+\omega-1)). \end{aligned}$$

Da nun $\omega^2+\omega+1=0$ sind

$$\alpha, \omega^2\alpha,\ \ \alpha(2\omega-1),\ \ \alpha(\omega^2+\omega-1)$$

paarweise verschieden, d.h. f und h haben nur die Nullstelle $\omega\alpha$ gemeinsam.
Folglich gibt es Polynome $a, b \in \mathbb{Q}[\vartheta][x]$ mit

$$x - \omega\alpha = af + bh,$$

und somit erhält man durch Einsetzen von $x = 0$:

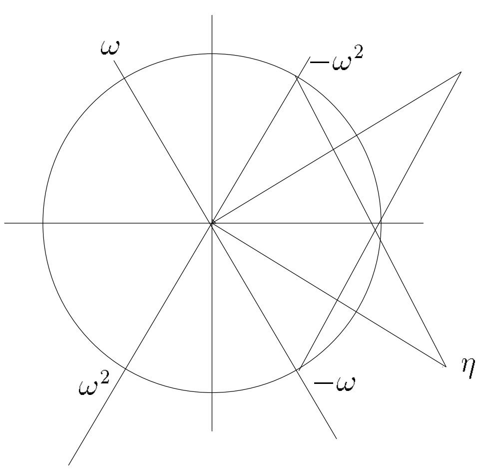
$$-\omega\alpha = a(0)f(0) + b(0)h(0) \in \mathbb{Q}[\vartheta].$$

Da $\alpha = \vartheta + \omega\alpha$, ist auch $\alpha \in \mathbb{Q}[\vartheta]$ und damit haben wir bewiesen, daß

$$\mathbb{Q}[\alpha, \omega\alpha] = \mathbb{Q}[\vartheta]$$

wobei

$$\begin{aligned} \vartheta = \alpha(1-\omega) &= \alpha\left(1 - \frac{-1+\sqrt{3}\,i}{2}\right) \\ &= \alpha\frac{3-\sqrt{3}\,i}{2} = \alpha\eta, \end{aligned}$$



Man erhält $\vartheta^6 = \alpha^6\eta^6 = 4\eta^6$. Da $|\eta| = \sqrt{3}$, ist (siehe Bild)

$$\eta^6 = -\sqrt{3}^6 = -27$$

und somit

$$\vartheta^6 = -4 \cdot 27.$$

Da $\operatorname{grad}\vartheta = \dim_{\mathbb{Q}} \mathbb{Q}[\vartheta] = 6$, muß

$$x^6 + 4 \cdot 27 \in \mathbb{Q}[x]$$

das Minimalpolynom von ϑ sein.

Es ist kein Zufall, daß der Körper $\mathbb{Q}[\alpha, \omega\alpha]$ von einem Element erzeugt wird. Um dies zu sehen, führen wir zunächst $\mathbb{Q}[\alpha_1, \ldots, \alpha_m]$ in der folgenden Verallgemeinerung von Satz 4.1.9 ein.

Satz 4.1.11 Seien $\alpha_1, \ldots, \alpha_m \in \mathbb{A}$. Dann ist

$$\mathbb{Q}[a_1, \ldots, \alpha_m] := \{p(\alpha_1, \ldots, \alpha_m) \mid p \in \mathbb{Q}[x_1, \ldots, x_m]\}$$

ein Unterkörper von $\mathbb{C}$, und es gilt

$$n = \dim_{\mathbb{Q}} Q[\alpha_1, \ldots, \alpha_m] < \infty.$$

Der Grad von α_i über $\mathbb{Q}$ ist ein Teiler von n.

Beweis: Induktion nach m.

Für $m = 1$ ist der Satz schon bewiesen. Induktionsschluß $m - 1 \to m$ $(m \geq 2)$: Es sei

$$K = \mathbb{Q}[a_1, \ldots, \alpha_{m-1}] \text{ und } L = \mathbb{Q}[a_1, \ldots, \alpha_m].$$

Dann ist

$$L = K[\alpha_m],$$

und wie im Beweis zu 4.1.9 (mit K an Stelle von $\mathbb{Q}$ folgt, daß L ein Unterkörper von $\mathbb{C}$ ist mit

$$\dim_K L < \infty.$$

Ist nun $\{\beta_1, \ldots, \beta_s\}$ eine $\mathbb{Q}$-Basis von K und $\{\gamma_1, \ldots, \gamma_t\}$ eine K-Basis von L, so ist

$$\{\beta_i\gamma_j \mid i = 1, \ldots, s;\ j = 1, \ldots, t\}$$

eine $\mathbb{Q}$-Basis von L. Es gilt also

$$\dim_{\mathbb{Q}} L = \dim_{\mathbb{Q}} K \cdot \dim_K L < \infty.$$

Die 'Kette' $\mathbb{Q} \subset \mathbb{Q}[\alpha_i] \subset \mathbb{Q}[\alpha_1, \ldots, \alpha_m]$ zeigt auch, daß $\dim_{\mathbb{Q}} \mathbb{Q}[\alpha_i]$ ein Teiler von $\dim_{\mathbb{Q}} \mathbb{Q}[a_1, \ldots, \alpha_m]$ ist. $\square$

Definition 4.1.12 Es seien $\alpha_1, \ldots, \alpha_m \in \mathbb{A}$. $\mathbb{Q}[a_1, \ldots, \alpha_m]$ heißt der von $\alpha_1, \ldots, \alpha_m$ erzeugte algebraische Zahlkörper.
Die Unterkörper K von $\mathbb{C}$, die man auf diese Weise erhält, sind durch die Eigenschaft

$$\dim_{\mathbb{Q}} K < \infty$$

charakterisiert. Diese Körper heißen **algebraische Zahlkörper**.

Wichtig ist nun der folgende Satz:

Satz 4.1.13 (Satz vom primitiven Element)
Es seien $\alpha_1, \ldots, \alpha_m \in \mathbb{A}$. Dann gibt es rationale Zahlen $c_2, \ldots, c_m \in \mathbb{Q}$, so daß

$$\mathbb{Q}[a_1, \ldots, \alpha_m] = \mathbb{Q}[\vartheta],$$

wobei

$$\vartheta := \alpha_1 + c_2\alpha_2 + \cdots + c_m\alpha_m.$$

ϑ heißt ein **primitives Element** des algebraischen Zahlkörpers $\mathbb{Q}[a_1, \ldots, \alpha_m]$.

Beweis: Induktion nach m, $m \geq 2$.
Es sei zunächst $m = 2$, $K = \mathbb{Q}[\alpha, \beta]$. $f \in \mathbb{Q}[x]$ sei das Minimalpolynom von α und $g \in \mathbb{Q}[x]$ sei das Minimalpolynom von β. Es sei zunächst $c \in \mathbb{Q}^\times$ ein beliebiges fest gewähltes Element. Wir setzen

$$\vartheta := \alpha + c\beta.$$

Da $f \in \mathbb{Q}[x]$, ist h mit

$$h(x) := f(\vartheta - cx)$$

ein Polynom in x mit Koeffizienten in dem Erweiterungskörper $\mathbb{Q}[\vartheta]$ von $\mathbb{Q}$. Da $\alpha = \vartheta - c\beta$, folgt

$$h(\beta) = f(\alpha) = 0.$$

Die Polynome h und g haben daher β als eine gemeinsame Nullstelle.
Da f und g irreduzibel in $\mathbb{Q}[x]$ sind, besitzen f und g nur einfache Nullstellen. Nach Definition von h gilt dies auch für h. f besitze die Nullstellen

$$\alpha_1, \ldots, \alpha_n \in \mathbb{C},$$

wobei $\alpha = \alpha_1$ sei.
Es sei $\gamma_i := \frac{\vartheta - \alpha_i}{c}$, also $\beta = \gamma_1$. Dann sind $\gamma_1, \ldots, \gamma_n$ die verschiedenen Nullstellen von h.
Es gilt

$$\gamma_i = \frac{\alpha - \alpha_i}{c} + \beta.$$

Seien $\beta_1, \ldots, \beta_r$ die Nullstellen von g. Es gelte $\beta = \beta_1$,. Man kann nun $c \in \mathbb{Q}^x$ so wählen, daß für alle $i = 2, \ldots, n$ und $j = 2, \ldots, r$

$$\frac{\alpha - \alpha_i}{c} + \beta \neq \beta_j$$

gilt. Alle Werte $c \in \mathbb{Q}^*$ mit

$$c \notin \left\{ \frac{\alpha - \alpha_i}{\beta_j - \beta} \;\Big|\; i = 2, \ldots, n;\; j = 2, \ldots, r \right\}$$

sind möglich. Hat man nun c so gewählt, so haben h und g nur die Nullstelle β gemeinsam.

Nach dem euklidischen Algorithmus im Ring $\mathbb{Q}[\vartheta][x]$ gibt es daher Polynome $a, b \in \mathbb{Q}[\vartheta][x]$, so daß

$$x - \beta = ag + bh.$$

Durch Einsetzen von $x = 0$ folgt hieraus

$$-\beta = a(0)g(0) + b(0)h(0) \in \mathbb{Q}[\vartheta].$$

Damit gilt

$$\beta \in \mathbb{Q}[\vartheta]$$

und wegen $\alpha = \vartheta - c\beta$ folgt auch

$$\alpha \in \mathbb{Q}[\vartheta].$$

Wir haben somit

$$\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\vartheta]$$

bewiesen.

Es sei nun $m \geq 3$, und die Behauptung sei für $m - 1$ schon bewiesen. Seien $\alpha_1, \ldots, \alpha_m \in \mathbb{C}$ algebraisch und

$$K = \mathbb{Q}[\alpha_1, \ldots, \alpha_m].$$

Nach Induktionsvoraussetzung gibt es rationale Zahlen $c_2, \ldots, c_{m-1} \in \mathbb{Q}$, so daß

$$\mathbb{Q}[\alpha_1, \ldots, \alpha_{m-1}] = \mathbb{Q}[\vartheta_1],$$

wobei $\vartheta_1 = \alpha_1 + c_2\alpha_2 + \cdots + c_{m-1}\alpha_{m-1}$.

Nach dem Fall $m = 2$ gibt es nun eine rationale Zahl $c_m \in \mathbb{Q}$, so daß

$$\mathbb{Q}[\vartheta_1, \alpha_m] = \mathbb{Q}[\vartheta_1 + c_m\alpha_m].$$

$\vartheta = \vartheta_1 + c_m\alpha_m = \alpha_1 + c_2\alpha_2 + \cdots + c_m\alpha_m$ ist das gesuchte primitive Element. □

Definition 4.1.14 Es sei K ein algebraischer Zahlkörper vom Grad n über $\mathbb{Q}$. Dann ist $K \cong \mathbb{Q}^n$ als $\mathbb{Q}$-Vektorraum. Jedes Element $\beta \in K$ definiert die $\mathbb{Q}$-lineare Abbildung

$$\varphi_\beta^K : K \longrightarrow K$$

mit $\varphi_\beta^K(\gamma) := \beta\gamma$.

(1) $N(\beta) = N_{K/\mathbb{Q}}(\beta) := \det \varphi_\beta^K \in \mathbb{Q}$ heißt die **Norm** von β über $\mathbb{Q}$.

(2) $Tr(\beta) = Tr_{K/\mathbb{Q}}(\beta) := Tr\varphi_\beta^K \in \mathbb{Q}$ heißt die **Spur** von β über $\mathbb{Q}$.

Wir bemerken:

Ist $L \subset K$ ein Unterkörper, so ist $\varphi_\beta^K : K \longrightarrow K$ auch L-linear. Fassen wir φ_β^K als L-linear auf, so schreiben wir $\varphi_\beta^{K/L}$.

(3) $N_{K/L}(\beta) := \det(\varphi_\beta^{K/L}) \in L$ heißt die **Norm** von β über L.

(4) $Tr_{K/L}(\beta) := Tr(\varphi_\beta^{K/L}) \in L$ heißt die **Spur** von β über L.

Beispiel 4.1.15 Wir betrachten den Körper

$$K = \mathbb{Q}[\vartheta] \text{ mit } \vartheta = \sqrt[3]{2}\,\frac{3-\sqrt{3}i}{2}.$$

Wie wir in Beispiel 4.1.10 gesehen haben, ist K vom Grad 6 über $\mathbb{Q}$ und

$$f = x^6 + 4 \cdot 27 \in \mathbb{Q}[x]$$

ist das Minimalpolynom von ϑ.

Bzgl. der $\mathbb{Q}$-Basis $(1, \vartheta, \dots, \vartheta^5)$ von K ist $\varphi_\vartheta^K : K \longrightarrow K$ somit durch die Matrix

$$A_\vartheta = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -4\cdot 27 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

gegeben.

Also ist

$$N(\vartheta) = \det A_\vartheta = 4 \cdot 27$$

und

$$Tr(\vartheta) = 0.$$

Betrachten wir dagegen $\alpha = \sqrt[3]{2} \in K$, so ist die Berechnung mit Hilfe der Basis $(1, \vartheta, \dots, \vartheta^5)$ nicht einfach. Wir wählen eine andere Basis von K, nämlich (siehe 4.1.10)

$$(1, \alpha, \alpha^2, \omega\alpha, \omega\alpha^2, \omega\alpha^3),$$

wobei $\omega = \frac{-1+\sqrt{3}i}{2}$.

Bezüglich dieser Basis ist φ_α^K durch die Matrix

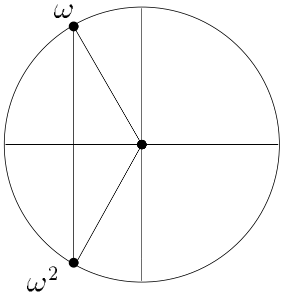
$$A_\alpha = \left(\begin{array}{ccc|ccc} 0 & 0 & 2 & & & \\ 1 & 0 & 0 & & 0 & \\ 0 & 1 & 0 & & & \\ \hline & & & 0 & 0 & 2 \\ & 0 & & 1 & 0 & 0 \\ & & & 0 & 1 & 0 \end{array}\right)$$

gegeben, denn: $\omega\alpha^4 = 2\omega\alpha$.
Also ist

$$N(\alpha) = 4,$$
$$Tr(\alpha) = 0.$$

Schließlich sei $L = \mathbb{Q}[\alpha]$. Dann ist K eine quadratische Erweiterung von L und $(1, \vartheta)$ ist eine L-Basis von K. Um eine Relation für ϑ^2 zu erhalten, betrachten wir die Darstellung $\vartheta = \alpha(1-\omega) = \alpha - \alpha\omega$. Es folgt

$$\vartheta^2 = \alpha^2(1 - 2\omega + \omega^2) = \alpha^2(1 - 3\omega + \omega + \omega^2) = -3\alpha^2\omega,$$



also $\vartheta^2 - 3\alpha\vartheta = -3\alpha^2\omega - 3\alpha^2 + 3\alpha^2\omega = -3\alpha^2$ und somit $\vartheta^2 - 3\alpha\vartheta + 3\alpha^2 = 0$.

$$g = x^2 - 3\alpha x + 3\alpha^2 \in L[x]$$

ist das Minimalpolynom von ϑ über L.
Die Matrix von

$$\varphi_\vartheta^{K/L} : K \longrightarrow K$$

bzgl. der L-Vektorraumbasis $(1, \vartheta)$ von K ist somit

$$B_\vartheta = \begin{pmatrix} 0 & -3\alpha^2 \\ 1 & 3\alpha \end{pmatrix},$$

denn $\varphi_\vartheta^{K/L}(\vartheta) = \vartheta^2 = -3\alpha^2 + 3\alpha\vartheta$. Also gilt

$$N_{K/L}(\vartheta) = 3\alpha^2,$$
$$Tr_{K/L}(\vartheta) = 3\alpha.$$

Man sieht: $N_{K/\mathbb{Q}}(\vartheta) = N_{K/L}(\vartheta)^3$. Ebenso gilt

$$N_{K/\mathbb{Q}}(\alpha) = N_{L/Q}(\alpha)^2$$

denn

$$N_{L/\mathbb{Q}}(\alpha) = \det \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = 2.$$

Weiter ist

$$N_{K/L}(\alpha) = \det \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} = \alpha^2 \quad \text{weil } \alpha \in L.$$
$$N_{K/\mathbb{Q}}(\alpha)4 = (\alpha^2)^3 = N_{K/L}(\alpha)^3$$

Lemma 4.1.16 Es seien $K, L \subset \mathbb{C}$ algebraische Zahlkörper und $L \subset K$.
Es sei $\beta \in K$ und $g = x^m + b_{m-1}x^{m-1} + \cdots + b_0 \in L[x]$ sei das Minimalpolynom von β über L. Weiter sei $n = \dim_L K$. $\beta_1, \ldots, \beta_m \in \mathbb{C}$ seien die Nullstellen von g (etwa $\beta_1 = \beta$), d.h. $\beta_1, \ldots, \beta_m$ sind die zu β konjugierten algebraischen Zahlen über L. Dann gilt $n = mk$ mit $k \in \mathbb{N}$ und

(1) $N_{k/L}(\beta) = N_{L[\beta]/L}(\beta)^k = (\beta_1 \cdot \ldots \cdot \beta_m)^k = (-1)^n b_0^k$

(2) $Tr_{K/L}(\beta) = kTr_{L[\beta]/L}(\beta) = k(\beta_1 + \cdots + \beta_m) = -kb_{m-1}$

(3) $g^k = \det_L(x\; id_K - \varphi_\beta^{K/L})$

Beweis:

(1) $N_{L[\beta]/L}(\beta) = \det \begin{pmatrix} 0 & & & -b_0 \\ 1 & & & \\ & \ddots & & \vdots \\ & & 1 & -b_{m-1} \end{pmatrix} = (-1)^m b_0.$

Da $g = \prod_{i=1}^{m}(x - \beta_i)$, ist $b_0 = (-1)^m \beta_1 \cdot \ldots \cdot \beta_m$.

Es sei nun $(\gamma_1, \ldots, \gamma_k)$ eine $L[\beta]$-Basis von K. Dann ist

$$(\gamma_1, \gamma_1\beta, \ldots, \gamma_1\beta^{m-1},\ \gamma_2, \gamma_2\beta, \ldots,\ \gamma_k\beta^{m-1})$$

eine L-Basis von K und die Matrix A von $\varphi_\beta^{K/L} : K \longrightarrow K$ bezüglich dieser Basis hat Blockdiagonalgestalt

$$A = \begin{pmatrix} A' & & \\ & \ddots & \\ & & A' \end{pmatrix},$$

wobei A' die Matrix von $\varphi_\beta^{L[\beta]/L} : L[\beta] \longrightarrow L[\beta]$ ist. Es gilt also

$$N_{K/L}(\beta) = N_{L[\beta]/L}(\beta)^k.$$

(2) Mit den Bezeichnungen von (1) erhält man

$$Tr_{K/L}(\beta) = Tr\ A = k\ Tr\ A' = -kb_{m-1} = k(\beta_1 + \cdots + \beta_m).$$

(3) Es gilt weiter

$$\det{}_L(x\; id_K - \varphi_\beta^{K/L}) = \det(x\ E_n - A) = \det(x\ E_m - A')^k$$

$$\text{und} \quad \det(x\ E_m - A') = \det \begin{pmatrix} x & & \ldots & b_0 \\ 1 & \ddots & & \vdots \\ & \ddots & x & \\ & & 1 & x + b_{m-1} \end{pmatrix}$$
$$= x^m + b_{m-1}x^{m-1} + \cdots + b_0.$$

□

Die Aussage (3) besagt, daß das charakteristische Polynom von $\varphi_\beta^{K/L}$ die k-te Potenz des Minimalpolynoms $g \in L[x]$ von β über L ist.

Lemma 4.1.17 Sei $K = \mathbb{Q}[\alpha]$, $N = N_{K/\mathbb{Q}}$, $Tr = Tr_{K/\mathbb{Q}}$. Es gilt

(1) $\forall\, \beta, \gamma \in K:\ N(\beta\gamma) = N(\beta)N(\gamma)$

(2) $\forall\, \beta \in K^\times:\ N(\beta^{-1}) = N(\beta)^{-1}$
$N : K^\times \longrightarrow \mathbb{Q}^\times$ ist also ein Gruppenhomomorphismus

(3) $\forall\, \beta, \gamma \in K:\ Tr(\beta + \gamma) = Tr(\beta) + Tr(\gamma)$

(4) $\forall\, a \in \mathbb{Q},\ \beta \in K:\ Tr(a\beta) = aTr(\beta)$
$Tr : K \longrightarrow \mathbb{Q}$ ist also $\mathbb{Q}$-linear

(5) $\forall\, a \in \mathbb{Q}:\ N(a) = a^n$, wobei $n = \dim_\mathbb{Q} K$ der Grad von K über $\mathbb{Q}$ ist.

Beweis: Sei $\varphi_\beta = \varphi_\beta^{K/\mathbb{Q}}$.

(1) Aus $\varphi_{\beta\gamma} = \varphi_\beta \circ \varphi_\gamma$ und dem Determinantenmultiplikationssatz folgt $N(\beta\gamma) = N(\beta)N(\gamma)$.

(2) $id_K = \varphi_1 = \varphi_\beta \circ \varphi_{\beta^{-1}} \Longrightarrow 1 = N(1) = N(\beta)N(\beta^{-1})$

(3) $\varphi_{\beta+\gamma} = \varphi_\beta + \varphi_\gamma \Longrightarrow Tr(\beta+\gamma) = Tr(\varphi_\beta+\varphi_\gamma) = Tr\varphi_\beta + Tr\varphi_\gamma = Tr(\beta)+Tr(\gamma)$

(4) $\varphi_{a\beta} = a\varphi_\beta \Longrightarrow Tr(a\beta) = Tr(a\varphi_\beta) = a\ Tr\varphi_\beta = a\ Tr(\beta)$

(5) $\varphi_a = a\ id_K \Longrightarrow N(a) = \det(a\ id_K) = a^n$, wobei $n = \dim_\mathbb{Q} K$. □

Ist K ein algebraischer Zahlkörper, so gibt es neben der Inklusion $K \subset \mathbb{C}$ noch weitere Ringhomomorphismen $\varphi : K \longrightarrow \mathbb{C}$, d.h. Abbildungen $\varphi : K \longrightarrow \mathbb{C}$ mit $\varphi(ab) = \varphi(a)\varphi(b)$, $\varphi(a+b) = \varphi(a)+\varphi(b)$ für alle $a, b \in K$ und mit $\varphi(1) = 1$. Solche Homomorphismen sind injektiv, denn wäre $\varphi(a) = 0$ für ein $a \neq 0$, so wäre auch $\varphi(1) = \varphi(a)\varphi(a^{-1}) = 0$. Das Bild $\varphi(K)$ ist also ein zu K isomorpher Unterkörper von $\mathbb{C}$. Wie wir schon in Beispiel 4.1.10 gesehen haben, sind K und $\varphi(K)$ als Teilmengen von $\mathbb{C}$ im allgemeinen verschieden.

Lemma 4.1.18 Es seien K, L algebraische Zahlkörper und $L \subset K$. α sei primitives Element von K und

$$h = x^k + \eta_{k-1}x^{k-1} + \cdots + \eta_0 \in L[x]$$

sei das Minimalpolynom von α über L.
Es seien $\alpha_1, \ldots, \alpha_k$ die zu α über L konjugierten Zahlen (d.h. die komplexen Nullstellen von h).
Dann ist $\varphi_j : K \longrightarrow \mathbb{C}$ mit

$$\varphi_j\left(\sum_{i=0}^{k-1} \lambda_i \alpha^i\right) := \sum_{i=0}^{k-1} \lambda_i \alpha_j^i\ (\lambda_i \in L)$$

ein Ringhomomorphismus mit

$$\varphi_j(\lambda) = \lambda \quad \text{für} \quad \lambda \in L$$

und es gilt

$$\varphi_i \neq \varphi_j \text{ falls } i \neq j$$

und $\{\varphi_1, \dots, \varphi_k\}$ ist die Menge aller Ringhomomorphismen, $\varphi : K \longrightarrow \mathbb{C}$, die die Inklusion $L \subset \mathbb{C}$ fortsetzen.

Beweis: Nach dem Homomorphiesatz induziert die Auswertungsabbildung

$$L[x] \longrightarrow K, \ f \longmapsto f(\alpha)$$

einen Isomorphismus

$$\Phi : L[x]/h \cdot L[x] \longrightarrow K.$$

Ebenso induziert

$$L[x] \longrightarrow K_j = L[\alpha_j], \ f \longmapsto f(\alpha_j)$$

einen Isomorphismus

$$\Phi_j : L[x]/h \cdot L[x] \longrightarrow K_j.$$

Dann ist auch

$$\Phi_j \circ \Phi^{-1} : K \longrightarrow K_j$$

einen Isomorphismus.

Nach Definition ist

$$\begin{aligned}\Phi_j \circ \Phi^{-1}\left(\sum_{i=0}^{k-1} \lambda_i \alpha^i\right) &= \Phi_j\left(\sum_{i=0}^{k-1} \lambda_i x^i \bmod h\right) \\ &= \sum_{i=0}^{k-1} \lambda_i \alpha_j^i = \varphi_j\left(\sum_{i=0}^{k-1} \lambda_i \alpha^i\right).\end{aligned}$$

$\varphi_j : K \longrightarrow \mathbb{C}$ ist also ein Homomorphismus. Ist $i \neq j$, so ist $\varphi_i(\alpha) = \alpha_i \neq \alpha_j = \varphi_j(\alpha)$, also $\varphi_i \neq \varphi_j$. Damit haben wir k verschiedene Homomorphismen $\varphi : K \longrightarrow \mathbb{C}$, die die Inklusion $L \subset \mathbb{C}$ fortsetzen.

Ist nun $\varphi : K \longrightarrow \mathbb{C}$ irgendein Homomorphismus mit $\varphi(\lambda) = \lambda \quad \forall\ \lambda \in L$, so folgt aus

$$h(\alpha) = 0$$

auch $\varphi(h(\alpha)) = 0$ und da andererseits

$$\varphi(h(\alpha)) = \varphi\left(\sum_{i=0}^{k} \eta_i \alpha^i\right) = \sum_{i=0}^{k} \eta_i \varphi(\alpha)^i = h(\varphi(\alpha)),$$

ist $\varphi(\alpha)$ eine Nullstelle von h und somit

$$\varphi(\alpha) = \alpha_j \text{ für ein } j = 1, \dots, k.$$

Es folgt $\varphi = \varphi_j$. □

Wir benutzen die Gelegenheit, um den Begriff der Galoisgruppe einzuführen.

Definition 4.1.19 Es seien K, L algebraische Zahlkörper und $L \subset K$. Mit $G(K/L)$ wird die Menge aller Isomorphismen $\varphi : K \longrightarrow K$ bezeichnet, die L festlassen, d.h. für die $\varphi(\lambda) = \lambda \quad \forall\, \lambda \in L$ gilt. Offensichtlich ist $G(K/L)$ mit der Komposition als Multiplikation eine Gruppe.

$G(K/L)$ heißt die **Galoisgruppe** von K über L.

Wie Lemma 4.1.18 zeigt, ist $G(K/L)$ eine endliche Gruppe der Ordnung kleiner oder gleich $k = \dim_L K$ und besitzt genau dann die Ordnung k, wenn die k verschiedenen Ringhomomorphismen

$$\varphi_j : K \longrightarrow \mathbb{C}, \quad j = 1, \dots, k$$

Automorphismen von K sind, d.h. wenn

$$\varphi_j(K) = K, \text{ also } L[\alpha_j] = L[\alpha]$$

gilt. Körpererweiterungen $L \subset K$ mit dieser Eigenschaft

$$|G(K/L)| = \dim_L K$$

heißen **Galoiserweiterungen**.

Beispiel 4.1.20 Wir schließen an das Beispiel 4.1.10 an. Die Bezeichnungen seien wie dort, also $\alpha = \sqrt[3]{2}$. $\mathbb{Q}[\alpha]$ ist nicht galoissch über $\mathbb{Q}$, weil die drei Homomorphismen

$$\varphi_j : \mathbb{Q}[\alpha] \longrightarrow \mathbb{C} \text{ mit } \alpha \longmapsto \alpha\omega^j \ (j = 0, 1, 2)$$

bis auf φ_0 keine Automorphismen von $\mathbb{Q}[\alpha]$ sind. Daher ist die Galoisgruppe $G(\mathbb{Q}[\alpha]/\mathbb{Q})$ von $\mathbb{Q}[\alpha]$ über $\mathbb{Q}$ die triviale Gruppe. Wir haben schon gesehen, daß $\vartheta = \alpha\eta$ ein primitives Element des von α und $\alpha\omega$ erzeugten Körpers K ist. Dabei ist $\eta = 1 - \omega = \frac{3-\sqrt{3}i}{2}$. Nun ist aber $\zeta := 1 + \omega$ eine primitive sechste Einheitswurzel, und somit sind $\vartheta_0 = \vartheta,\ \vartheta_1 = \vartheta\zeta, \dots, \vartheta_5 = \vartheta\zeta^5$ die sechs Nullstellen von $x^6 + 4 \cdot 27$. Diese Nullstellen liegen in $K = \mathbb{Q}[\vartheta] = \mathbb{Q}[\alpha, \alpha\omega]$, weil $\zeta = 1 + \omega = 1 + \frac{\alpha\omega}{\alpha} \in K$. Die sechs Homomorphismen

$$\varphi_j : K \longrightarrow \mathbb{C} \text{ mit } \varphi_j(\vartheta) = \vartheta_j \ (j = 0, \dots, 5)$$

sind daher Automorphismen von K, und somit ist $G(K/\mathbb{Q}) = \{\varphi_0, \dots, \varphi_5\}$.

K ist somit eine Galoissche Erweiterung von $\mathbb{Q}$.

Lemma 4.1.21 Es seien K, L algebraische Zahlkörper wie in Lemma 4.1.18.

$\varphi_1, \dots, \varphi_k : K \longrightarrow \mathbb{C}$ seien die Homomorphismen mit $\varphi_j | L = id$, dann gilt für jedes $\beta \in K$

$$N_{K/L}(\beta) = \varphi_1(\beta) \cdot \ldots \cdot \varphi_k(\beta)$$
$$Tr_{K/L}(\beta) = \varphi_1(\beta) + \dots + \varphi_k(\beta)$$

Beweis: Es sei

$$g = x^m + b_{m-1}x^{m-1} + \dots + b_0 \in L[x]$$

das Minimalpolynom von β über L. $m = \mathrm{grad}(\beta)$, $l = \frac{k}{m}$

$$L \subset L[\beta] \subset K.$$

Nach 4.1.16 gilt

$$g^l = \det_L(x\, id_K - \varphi_\beta^{K/L}).$$

Es folgt also $\det_L(\beta\, id_K - \varphi_\beta^{K/L}) = 0$ und somit auch

$$0 = \varphi_j(\det(\beta\, id_K - \varphi_\beta^{K/L})) = \det(\varphi_j(\beta) id_K - \varphi_\beta^{K/L}) \text{ für } j = 1, \ldots, k.$$

Folglich sind

$$\varphi_1(\beta), \ldots, \varphi_k(\beta)$$

Nullstellen von g.

Da $\mathrm{grad}\, g = m$, hat g nur m verschiedene Nullstellen. Um zu sehen, daß $\varphi_1(\beta), \ldots, \varphi_k(\beta)$ alle Nullstellen von g durchlaufen, müssen wir nur zeigen, daß $l + 1$ dieser Zahlen nicht untereinander gleich sein können.

Annahme: $\varphi_1(\beta) = \ldots = \varphi_{l+1}(\beta)$ (nach evtl. Umnumerieren) Dann gilt

$$\psi := \varphi_1 \mid L[\beta] = \ldots = \varphi_{l+1} \mid L[\beta].$$

Da $\dim_{L[\beta]} K = l$, gibt es nach Lemma 4.1.18 aber nur l Fortsetzungen von $\psi : L[\beta] \longrightarrow \mathbb{C}$ zu einem Homomorphismus $\varphi : K \longrightarrow \mathbb{C}$. Wir haben aber $l + 1$. Widerspruch!

Da $k = lm$, sind somit mindestens m Elemente von $\{\varphi_1(\beta), \ldots, \varphi_k(\beta)\}$ paarweise verschieden. Da $\mathrm{grad}\, g = m$, folgt

$$g^l = \prod_{j=1}^{k} (x - \varphi_j(\beta)).$$

Es folgt $\det_L(x\, id_K - \varphi_\beta^{K/L}) = \prod\limits_{j=1}^{k} (x - \varphi_j(\beta))$ und somit

$$N_{K/L}(\beta) = \det \varphi_\beta^{K/L} = \prod_{j=1}^{k} \varphi_j(\beta),$$

$$Tr_{K/L}(\beta) = Tr \varphi_\beta^{K/L} = \sum_{j=1}^{k} \varphi_j(\beta).$$

□

Definition 4.1.22 Sei $\alpha \in \mathbb{C}$ algebraisch, $K = \mathbb{Q}[\alpha]$.

$$O_K := \{\beta \in K \mid \beta \text{ ist ganz über } \mathbb{Q}\}$$

ist ein Unterrring von K.

O_K heißt der **Ring der ganzen algebraischen Zahlen** in K.

Übungen 4.1.23

(1) Beweise das Eisensteinsche Irreduzibilitätskriterium:

Es sei $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ und p eine Primzahl, so daß gilt: $\mathrm{red}_p\, f = (a_n \bmod p)x^n \neq 0$ und $a_0 \not\equiv 0 \bmod p^2$.

Dann ist f irreduzibel in $\mathbb{Q}[x]$.

(2) Ein Polynom $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ heißt **primitiv**, wenn $\mathrm{ggT}(a_0, \ldots, a_n) = 1$ gilt.

(a) Zeige: Sind $f, g \in \mathbb{Z}[x]$ primitiv, so ist auch fg primitiv.

(b) $f \in \mathbb{Z}[x]$ ist irreduzibel $\Longleftrightarrow$ f ist primitiv und f ist irreduzibel in $\mathbb{Q}[x]$.

(c) Es sei α eine algebraische Zahl mit Minimalpolynom $f \in \mathbb{Q}[x]$. Dann gilt:

$$\alpha \text{ ist ganz algebraisch } \Longleftrightarrow f \in \mathbb{Z}[x].$$

(3) Welche der folgenden Polynome sind irreduzibel in $\mathbb{Z}[x]$?

a) $x^2 + 3$ b) $x^2 - 169$ c) $x^3 + x^2 + x + 1$, d) $x^4 + x^3 + x^2 + x + 1$,
e) $x^3 + 2x^2 + 3x + 4$

(4) Bestimme die Konjugierten von $\cos \frac{2\pi}{5}$

(5) Bestimme die Minimalpolynome der algebraischen Zahlen $\sqrt{3}+\sqrt{5}$, $e^{\frac{\pi i}{17}}$, $\sqrt{1+\sqrt{2}}+\sqrt{1-\sqrt{2}}$, $\dfrac{1+i}{\sqrt{2}}$, $i+\sqrt{2}$, $e^{\frac{2\pi i}{3}}+2$.

(6) Bestimme ein primitives Element von

(a) $\mathbb{Q}[\sqrt{3},\ \sqrt[3]{5}]$

(b) $\mathbb{Q}[\sqrt[3]{5},\ \omega\sqrt[3]{5}]$, wobei $\omega = \dfrac{-1+\sqrt{-3}}{2}$

(7) Es sei $K = \mathbb{Q}[\sqrt[4]{3}],\ L = \mathbb{Q}[\sqrt{3}]$.
Berechne $Tr_{K/L}(\alpha)$, $Tr_{K/\mathbb{Q}}(\alpha)$, $N_{K/L}(\alpha)$, $N_{K/\mathbb{Q}}(\alpha)$ für $\alpha = \sqrt[4]{3},\ \sqrt{3},\ 1+\sqrt[4]{3},\ \frac{1}{2}(1+\sqrt{3}),\ \sqrt{3}+\sqrt[4]{3}$.

(8) (für ***Mathematica*** -Fans)

(a) Es sei α eine algebraische Zahl vom Grad n mit Minimalpolynom f. Führe die Elemente von $K = \mathbb{Q}[\alpha]$ als abstrakten Datentyp ein, und erkläre dann die Arithmetik im Körper K (vgl. Beispiel 2.1.6).

(b) Schreibe ein Programm zur Berechnung der Matrix A von $\varphi_\beta^{K/\mathbb{Q}} : K \to K$ bezüglich der Basis $(1, \alpha, \ldots, \alpha^{n-1})$, wobei $\beta \in K$.

(c) Schreibe ein Programm zur Berechnung von Norm und Spur eines Elementes in K. Benutze dazu b). Versuche die Aufgabe auch mit Lemma 4.1.16 oder 4.1.21 zu lösen.

4.2 Reell-quadratische Zahlkörper

Es sei $d \in \mathbb{Z}$ quadratfrei, $\alpha := \sqrt{d}$.

Definition 4.2.1 $K = \mathbb{Q}[\alpha]$ heißt **quadratischer Zahlkörper**.

$$f = x^2 - d$$

ist das Minimalpolynom von α.
Sind $a, b \in \mathbb{Q}$ und $\beta = a + b\alpha$, so ist

$$\begin{aligned}\beta^2 &= a^2 + 2ab\alpha + b^2\alpha^2 = (a^2 + db^2) + 2ab\alpha \\ &= (-a^2 + db^2) + 2a\beta,\end{aligned}$$

also

$$\beta^2 - 2a\beta + a^2 - db^2 = 0.$$

Ist $b \neq 0$, so ist $x^2 - 2ax + a^2 - db^2$ irreduzibel in $\mathbb{Q}[x]$, also das Minimalpolynom von β, und somit gilt in diesem Fall

$$\begin{aligned}N(\beta) &= a^2 - db^2 \\ Tr(\beta) &= 2a\end{aligned}$$

Dies gilt auch im Fall $b = 0$, denn dann ist $x - a$ das Minimalpolynom und man kann Lemma 4.1.16 anwenden.
Auch mit Hilfe von Lemma 4.1.21 kann man $N(\beta)$ und $Tr(\beta)$ bestimmen: $\alpha, -\alpha$ sind konjugiert. Die Homomorphismen $K \longrightarrow \mathbb{C}$ sind $\varphi_1 = id_K$, $\varphi_2 : K \longrightarrow \mathbb{C}$ mit $\varphi_2(a + b\alpha) = a - b\alpha$.
Es folgt

$$\begin{aligned}N(a + b\alpha) &= (a + b\alpha)(a - b\alpha) = a^2 - db^2, \\ Tr(a + b\alpha) &= a + b\alpha + a - b\alpha = 2a.\end{aligned}$$

Wir betrachten nur den Fall $K \subset \mathbb{R}$, d.h. $d > 0$.

Definition 4.2.2 Ist $d > 0$, so heißt K reell-quadratischer Zahlkörper.

Außerdem setzen wir voraus, daß

$$d \equiv 1 \bmod 4.$$

Es gilt nun $\beta = a + b\alpha$ $(a, b \in \mathbb{Q})$ ist genau dann ganz, wenn das Minimalpolynom von β in $\mathbb{Z}[x]$ liegt (Übung 4.1.23(2c)), also wenn

$$2a \in \mathbb{Z} \text{ und } a^2 - db^2 \in \mathbb{Z}.$$

Es gilt dann

$$\begin{aligned}&\beta = a + b\alpha \text{ ganz } (a, b \in \mathbb{Q}) \Longrightarrow a = \frac{a'}{2} \text{ mit } a' \in \mathbb{Z},\ \frac{a'^2}{4} - db^2 \in \mathbb{Z} \\ &\Longrightarrow 4db^2 \in \mathbb{Z} \Longrightarrow b = \frac{b'}{2} \text{ mit } b' \in \mathbb{Z} \\ &\Longrightarrow \frac{a'^2 - db'^2}{4} \in \mathbb{Z} \Longrightarrow\end{aligned}$$

$$a'^2 - b'^2 \underset{[d \equiv 1 \bmod 4]}{\equiv} a'^2 - db'^2 \equiv 0 \bmod 4$$

$\Longrightarrow a' \equiv b' \bmod 2$. Umgekehrt gilt: Sind $a', b' \in \mathbb{Z}$ mit $a' \equiv b' \bmod 2$, so ist $\beta = \frac{1}{2}(a' + b'\alpha)$ ganz. Wir setzen

$$\gamma := \frac{1+\alpha}{2} = \frac{1+\sqrt{d}}{2}.$$

Lemma 4.2.3 $O_K = \mathbb{Z} \oplus \mathbb{Z}\gamma$

Beweis: $\beta \in O_K \Longleftrightarrow \exists\ a'b' \in \mathbb{Z}$ mit $a' \equiv b' \bmod 2$ und

$$\beta = \frac{a'}{2} + \frac{b'}{2}\alpha = \frac{a'-b'}{2} + b'\gamma$$

□

Nicht ganz trivial ist es nun, die Einheitengruppe $O_K^\times$ von O_K zu bestimmen.
Ist $\beta \in O_K$ eine Einheit, so ist $N(\beta)$ Einheit in $\mathbb{Z}$, also $N(\beta) = \pm 1$. Ist umgekehrt $N(\beta) = \pm 1$, so heißt das

$$\beta\beta' = \pm 1, \text{ wobei } \beta' = a - b\alpha, \text{ wenn } \beta = a + b\alpha,$$

also ist β Einheit in O_K. Also gilt

Lemma 4.2.4 $O_K^\times = \{\beta \in O_K \mid N(\beta) = \pm 1\}$.
Sei nun

$$f(a,b) := \max(|\beta|,\ |\beta'|) \text{ für } a, b \in \mathbb{Q}, \quad \text{wobei } \beta = a + b\alpha,\ \beta' = a - b\alpha.$$

Lemma 4.2.5 Ist $N > 0$, so gilt

$$\{(a,b) \in \mathbb{Q}^2 \mid f(a,b) \le N\} \subset \left\{(a,b) \in \mathbb{Q}^2 \mid |a| < N,\ |b| \le \frac{N}{\alpha}\right\}.$$

Beweis:

(1) Ist $a > N$, so ist $f(a,b) > N$.

Beweis: Ist $\beta = a + b\alpha \le N$, so ist $b < 0$, also $a - b\alpha > N$ und somit $f(a,b) > N$. Ist $\beta > N$, so ist ebenfalls $f(a,b) > N$.

(2) Ist $-a > N$, so ist $f(a,b) > N$.

Beweis: Ist $-\beta' = -a + b\alpha \le N$, so ist $b < 0$, also $-a - b\alpha > N$ und somit $f(a,b) > N$. Ist $-\beta > N$, so ist natürlich auch $f(a,b) > N$.

(3) $b > \frac{N}{\alpha} \Longrightarrow f(a,b) > N$.

Beweis: Ist $\beta = a + b\alpha \le N$, so ist $a < 0$, also $-a + b\alpha > N$ und somit $f(a,b) > N$. Ist $\beta > N$, so ist sowieso $f(a,b) > N$.

(4) $-b > \frac{N}{\alpha} \Longrightarrow f(a,b) > N$.

Beweis: Ist $\beta' = a - b\alpha \le N$, so ist $a < 0$, also $-a - b\alpha > N$ und somit $f(a,b) > N$. □

Lemma 4.2.6 Für $N > 1$ gibt es nur endlich viele Einheiten $\beta \in O_K^\times$ mit $1 < \beta \leq N$.

Beweis: $\beta = a + b\alpha \in O_K^\times$ und $1 < \beta \leq N \Longrightarrow$

$$\begin{aligned} 1 = N(\beta)^2 = N(\beta)\beta'\beta &\Longrightarrow \\ \beta^{-1} = N(\beta)\beta' \Longrightarrow |\beta'| = \frac{1}{\beta} < 1 \\ \Longrightarrow f(a,b) = \max(\beta, \frac{1}{\beta}) = \beta \leq N \\ \underset{[Lemma\, 4.2.5]}{\Longrightarrow} |a| \leq N,\ |b| \leq \frac{N}{\alpha} \end{aligned}$$

Da für ganze β nach Lemma 4.2.3 $2a, 2b \in \mathbb{Z}$ gilt, gibt es nur endlich viele Möglichkeiten. □

Wir benutzen nun den folgenden Existenzsatz, den wir später beweisen werden (siehe Satz 4.2.19).

Es gibt positive Zahlen $a, b \in \mathbb{N}_+$ mit

$$a^2 - db^2 = 1.$$

Insbesondere gibt es eine Einheit $\varepsilon \in O_K^\times$ mit $\varepsilon > 1$. Nach Lemma 4.2.6 gibt es nur endlich viele Einheiten ε' mit $1 < \varepsilon' \leq \varepsilon$. Man findet daher eine wohlbestimmte kleinste Einheit $\varepsilon > 1$ in O_K^x.

Satz 4.2.7 Es sei $\varepsilon \in O_K^\times$ die kleinste Einheit mit $\varepsilon > 1$. Dann gilt

$$O_K^\times = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$$

ε heißt die **Fundamentaleinheit** in O_K.

Beweis:

(1) Es sei $\varepsilon' \in O_K^\times$ mit $\varepsilon' > 1$.

Es folgt $\varepsilon \leq \varepsilon'$, und da $\varepsilon > 1$ ist, gibt es ein eindeutig bestimmtes $n \in \mathbb{N}_+$ mit $\varepsilon^{n-1} < \varepsilon' \leq \varepsilon^n$. Es folgt $\varepsilon' = \varepsilon^n$, denn sonst wäre $\varepsilon' < \varepsilon^n$, also $\frac{\varepsilon^n}{\varepsilon'} > 1$ und somit $\frac{\varepsilon^n}{\varepsilon'} > \varepsilon$, woraus $\varepsilon^{n-1} \geq \varepsilon'$ im Widerspruch zu $\varepsilon^{n-1} < \varepsilon'$ folgen würde.

(2) Es sei $\varepsilon' \in O_K^\times$ beliebig. Dann gilt $\varepsilon' = \pm 1$ oder $\pm\varepsilon' > 1$ oder $\pm\frac{1}{\varepsilon'} > 1$ und somit $\varepsilon' = \pm\varepsilon^\circ$ oder $\varepsilon' = \pm\varepsilon^n$ mit $n > 0$ oder $\varepsilon' = \pm\varepsilon^n$ mit $n < 0$. Insgesamt ergibt sich

$$O_K^\times = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}.$$

□

Wir haben hier die Existenz einer nichttrivialen Lösung $(x, y) \in \mathbb{Z}^2$ der Gleichung $x^2 - dy^2 = 1$ benutzt. Im Fall $d = 5$ können wir dies ad hoc einsehen.

Beispiel 4.2.8 Es sei $d = 5$, $\gamma = \frac{1+\sqrt{5}}{2}$, $N(\gamma) = (\frac{1}{2})^2 - 5(\frac{1}{2})^2 = -1$, also ist γ eine Einheit in O_K.

Behauptung: γ ist die Fundamentaleinheit.

Beweis: Nach Lemma 4.2.5 gilt mit $N := \gamma$

$$\{(a,b) \in \mathbb{Q}^2 \mid f(a,b) \le \gamma\} \subset \left\{(a,b) \in \mathbb{Q}^2 \mid |a| \le \gamma,\ |b| \le \frac{\gamma}{\alpha}\right\},$$

wobei $\alpha = \sqrt{5}$, $f(a,b) = \max(|a+b\alpha|,\ |a-b\alpha|.)$

Ist $\beta = a + b\alpha$ eine Einheit, so ist $\beta' = a - b\alpha = \pm\beta^{-1}$, und aus $1 < \beta \le \gamma$ folgt somit

$$|\beta'| = |\beta^{-1}| < 1,$$

also $f(a,b) = \max(\beta, |\beta'|) = \beta \le \gamma$. Es folgt

$$\{\beta \in O_K^\times \mid 1 \le \beta \le \gamma\} \subset \left\{\beta = a + b\alpha \in O_K \mid |a| \le \gamma,\ |b| \le \frac{\gamma}{\alpha}\right\}.$$

Es gilt $\gamma = \frac{1}{2}(1+\sqrt{5}) \le \frac{1}{2}(1+2,3) = 1,65$ und $\frac{\gamma}{\alpha} = \frac{\sqrt{5}}{10} + \frac{1}{2} \le 0,23 + 0,5 = 0,73$.

Damit sind die Zahlen $\beta = a + b\alpha$ mit

$$\begin{aligned}(a,b) = &\left(-\frac{3}{2},\ \frac{1}{2}\right),\ \left(-\frac{1}{2},\ \frac{1}{2}\right), \left(\frac{1}{2},\ \frac{1}{2}\right), \left(\frac{3}{2},\ \frac{1}{2}\right),\\ &(-1,0),\ (0,0),\ (1,0),\\ &\left(-\frac{3}{2}, -\frac{1}{2}\right),\ \left(-\frac{1}{2}, -\frac{1}{2}\right),\ \left(\frac{1}{2}, -\frac{1}{2}\right),\ \left(\frac{3}{2}, -\frac{1}{2}\right)\end{aligned}$$

die einzigen Elemente in O_K mit

$$|a| < 1,65 \text{ und } |b| \le 0,73,$$

Die Paare, die Einheiten definieren, sind

$$\left(-\frac{1}{2}, \frac{1}{2}\right)\ \left(\frac{1}{2}, \frac{1}{2}\right)(-1,0),\ (1,0),\ \left(-\frac{1}{2}, -\frac{1}{2}\right),\ \left(\frac{1}{2}, -\frac{1}{2}\right)$$

und davon ergibt nur $(\frac{1}{2}, \frac{1}{2})$ eine Zahl größer als 1 und zwar $\gamma = \frac{1}{2} + \frac{1}{2}\alpha$.

Damit ist die Behauptung bewiesen.

Es folgt somit für $d = 5$:

$$O_K^\times = \{\pm\gamma^n \mid n \in \mathbb{Z}\}.$$

Es besteht ein Zusammenhang zu den Fibonacci-Zahlen: Da $\gamma^2 = 1 + \gamma$, folgt aus

$$\begin{aligned}\gamma^{n-1} &= u_{n-2} + u_{n-1}\gamma\\ \gamma^n &= (u_{n-2} + u_{n-1})\gamma + u_{n-1}\\ &= u_{n-1} + u_n\gamma,\end{aligned}$$

wobei

$$\begin{aligned}&u_0 = 0,\ u_1 = 1\\ &u_n = u_{n-2} + u_{n-1} \text{ für } n \ge 2.\end{aligned}$$

Wir wollen den Beweis der Existenz einer nichttrivialen Lösung $(x, y) \in \mathbb{Z}^2$ von $x^2 - dy^2 = 1$ nachtragen.
Dazu müssen wir zunächst etwas über Kettenbrüche lernen.

Definition 4.2.9 Ein **Kettenbruch** ist ein Ausdruck der Form

$$[q_0, q_1, q_2, \dots, q_n] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{\ddots}{\qquad \cfrac{1}{q_{n-1} + \frac{1}{q_n}}}}}},$$

wobei $q_0, \dots, q_n$ reelle Zahlen größer oder gleich 1 sind.
Es gilt

$$\begin{aligned}
[q_0, \dots, q_n] &= \left[q_0, \dots, q_{n-2},\ q_{n-1} + \frac{1}{q_n}\right] \\
&= [q_0, \dots, q_{n-2},\ [q_{n-1},\ q_n]]
\end{aligned}$$

Allgemeiner

$$[a_0, \dots, q_n] = [q_0, \dots, q_{k-1}, [q_k, \dots, q_n]].$$

Man kann $[q_0, \dots, q_n]$ rekursiv nach folgendem Schema berechnen:

0	1	$a_0 = q_0$	$a_1 = 1 + q_0 q_1$	$a_2 = a_0 + a_1 q_2$	$\dots$	$a_n = a_{n-2} + a_{n-1} q_n$
1	0	$b_0 = 1$	$b_1 = q_1$	$b_2 = b_0 + b_1 q_2$	$\dots$	$b_n = b_{n-2} + b_{n-1} q_n$

Es gilt dann

$$[q_0, \dots, q_n] = \frac{a_n}{b_n}.$$

Der Beweis geht durch Induktion nach n:
Für $n = 0$ ist $[q_0] = q_0 = \frac{a_0}{b_0}$.

$$\begin{aligned}
&n - 1 \to n : \\
&[q_0, \dots, q_n] = \left[q_0, \dots, q_{n-2},\ q_{n-1} + \frac{1}{q_n}\right] = \frac{a'_{n-1}}{b'_{n-1}} = \\
&\qquad = \frac{a_{n-3} + a_{n-2}(q_{n-1} + \frac{1}{q_n})}{b_{n-3} + b_{n-2}(q_{n-1} + \frac{1}{q_n})} = \frac{a_{n-3} q_n + a_{n-2}(q_{n-1} q_n + 1)}{b_{n-3} q_n + b_{n-2}(q_{n-1} q_n + 1)} = \\
&\qquad = \frac{a_{n-2} + (a_{n-3} + a_{n-2} q_{n-1}) q_n}{b_{n-2} + (b_{n-3} + b_{n-2} q_{n-1}) q_n} = \frac{a_{n-2} + a_{n-1} q_n}{b_{n-2} + b_{n-1} q_n} = \frac{a_n}{b_n}.
\end{aligned}$$

$\square$

In ***Mathematica*** kann man also den Wert von $[q_0, \dots, q_n]$ durch

```
Kettenbruch[q_List]:=Module[{n =Length[q],i, v, w},
   For[i = 1; {v, w} = {{0,1}, {1,0}}, i ≤ n,
      {v, w} = {w, v + q[[i]]w}; i++];
      w[[1]]/w[[2]]]
```

berechnen.

Definition 4.2.10 Ein unendlicher Kettenbruch $[q_0, q_1, q_2, \ldots]$ ist eine Folge $([q_0, \ldots, q_n])_{n\geq 0}$ von endlichen Kettenbrüchen, wobei $q_i \in \mathbb{R}$ für $i \geq 0$ und $q_i \geq 1$ falls $i \geq 1$. $[q_0, q_1, q_2, \ldots]$ konvergiert, wenn die Folge $([q_0, \ldots, q_n])_{n\geq 0}$ konvergiert, d.h. wenn die Folge $(\frac{a_n}{b_n})_{n\geq 0}$ der **Näherungsbrüche** von $[q_0, q_1, \ldots]$ konvergiert.

Es gilt also

Lemma 4.2.11 Sei $[q_0, q_1, q_2, \ldots,]$ ein endlicher oder unendlicher Kettenbruch mit $q_0 \geq 0$, $q_i \geq 1$ für $i \geq 1$. Es sei weiter

$$\begin{array}{ll} a_0 = q_0,\ a_1 = 1 + a_0 q_1, \ldots, & a_n = a_{n-2} + a_{n-1} q_n, \ldots \\ b_0 = 1,\ b_1 = q_1, \ldots, & b_n = b_{n-2} + b_{n-1} q_n, \ldots \end{array}$$

Dann gilt

$$[q_0, \ldots, q_n] = \frac{a_n}{b_n} \text{ für } n \geq 0.$$

Weiter gilt für jede reelle Zahl $\alpha \geq 1$

$$[q_0, \ldots, q_n \alpha] = \frac{a_{n-1} + a_n \alpha}{b_{n-1} + b_n \alpha}$$

□

a_n heißt n**-ter Näherungszähler** und b_n n**-ter Näherungsnenner** von $[q_0, q_1, \ldots]$. Es gilt

Lemma 4.2.12 Sei $q_0 \in \mathbb{N}$ und $q_i \in \mathbb{N}_+$ für $i > 0$.

(a)
$$a_n b_{n+1} - a_{n+1} b_n = (-1)^n,\ \frac{a_n}{b_n} - \frac{a_{n+1}}{b_{n+1}} = \frac{(-1)^{n+1}}{b_n b_{n+1}}$$

(b) $(a_n, b_n) = 1$

(c) $b_0 \leq b_1 < b_2 < \ldots < b_n < b_{n+1}$

(d) $\frac{a_0}{b_0} < \frac{a_2}{b_2} < \ldots < \frac{a_{2n}}{b_{2n}} < \frac{a_{2n+1}}{b_{2n+1}} < \frac{a_{2n-1}}{b_{2n-1}} < \ldots < \frac{a_1}{b_1}$.

(e) $[q_0, q_1, q_2, \ldots]$ ist konvergent.

Beweis:

(a) $a_0 b_1 - a_1 b_0 = q_0 q_1 - (1 + q_0 q_1) = -1$ und

$$\begin{aligned} a_n b_{n+1} - a_{n+1} b_n &= a_n(b_{n-1} + b_n q_{n+1}) - (a_{n-1} + a_n q_{n+1}) b_n \\ &= a_n b_{n-1} - a_{n-1} b_n = -(a_{n-1} b_n - a_n b_{n-1}) \end{aligned}$$

$\Longrightarrow a_n b_{n+1} - a_{n+1} b_n = (-1)^n$

und

$$(*) \qquad \frac{a_n}{b_n} - \frac{a_{n+1}}{b_{n+1}} = \frac{(-1)^{n+1}}{b_n b_{n+1}}.$$

(b) folgt sofort aus (a).

(c) $1 = b_0 \leq b_1 \underset{[q_2 \geq 1]}{<} 1 + b_1 q_2 = b_2$, und für $n > 2$ ist $b_{n-2} > 0$, $q_n \geq 1$, also

$$b_n = b_{n-2} + b_{n-1} > b_{n-1}$$

(d) Nach (*) ist

$$\frac{a_{2n}}{b_{2n}} - \frac{a_{2n+1}}{b_{2n+1}} = \frac{-1}{b_n b_{n+1}} < 0$$

Außerdem ist

$$\frac{a_{2k}}{b_{2k}} - \frac{a_{2k+2}}{b_{2k+2}} = \frac{(-1)^{2k+1}}{b_{2k} b_{2k+1}} + \frac{(-1)^{2k}}{b_{2k+1} b_{2k+2}} = \frac{-b_{2k+2} + b_{2k}}{b_{2k} b_{2k+1} b_{2k+2}} < 0$$

und analog

$$\frac{a_{2k-1}}{b_{2k-1}} = \frac{a_{2k+1}}{b_{2k+1}} = \frac{b_{2k+1} - b_{2k-1}}{b_{2k-1} b_{2k} b_{2k+1}} > 0.$$

Also gilt (d).

(e) $[q_0, \ldots, q_n] = \frac{a_n}{b_n}$. Nach (a) und (c) gilt für alle $k \geq 1$ und $m \geq 1$

$$\begin{aligned} \left| \frac{a_m}{b_m} - \frac{a_{m+k}}{b_{m+k}} \right| &\leq \sum_{j=0}^{k-1} \frac{1}{b_{m+j} b_{m+j+1}} \underset{[b_k \geq k]}{\leq} \\ & \sum_{j=0}^{k-1} \frac{1}{(m+j)(m+j+1)} = \sum_{j=1}^{m+k-1} \frac{1}{j(j+1)} - \sum_{j=1}^{m-1} \frac{1}{j(j+1)} \\ &= \frac{m+k-1}{m+k} - \frac{m-1}{m} = \frac{k}{(m+k)m} \end{aligned}$$

Also ist $(\frac{a_n}{b_n})_{n \geq 0}$ eine Cauchyfolge und somit konvergent.

Kettenbrüche $[q_0, q_1, q_2, q_3, \ldots]$ mit $q_0 \in \mathbb{N}$ und $q_i \in \mathbb{N}_+$ für $i \geq 1$, heißen **regelmäßig**. Wir betrachten nur regelmäßige Kettenbrüche.

Definition 4.2.13 Sei $\alpha \in \mathbb{R}$, $\alpha > 0$. Die **Kettenbruchentwicklung** von α wird rekursiv definiert:

$$\alpha_0 := \alpha, \; q_0 := [\alpha_0].$$

Ist $\alpha_0 - q_0 \neq 0$, so sei $\alpha_1 := \frac{1}{\alpha_0 - q_0}$. Dann ist

$$\alpha = q_0 + \frac{1}{\alpha_1} = [q_0, \alpha_1]$$

Sind $\alpha_0, \dots, \alpha_{n-1}, q_0, \dots, q_{n-1}$ schon definiert, sei $\alpha_n = \frac{1}{\alpha_{n-1} - q_{n-1}}$, falls $\alpha_{n-1} - q_{n-1} \neq 0$ und $q_n = [\alpha_n]$. Es gilt $\alpha = [q_0, \dots, q_{n-1}, \alpha_n]$. Ist $\alpha_{n-1} = q_{n-1}$, so bricht die Kettenbruchentwicklung ab und es gilt

$$\alpha = [q_0, \dots, q_{n-1}].$$

Der unendliche oder endliche Kettenbruch

$$[q_0, q_1, q_2, \dots]$$

heißt die **Kettenbruchentwicklung** von α.

In ***Mathematica*** kann man diese Entwicklung folgendermaßen definieren:

$$\begin{aligned}
&\text{Kettenbruchentwicklung}[\alpha_, n_] := \\
&\quad \text{Module}[\{Q,\ \beta = \alpha,\ q = \text{Floor}[\alpha],\ i = 0\}, \\
&Q = \{q\};\ \text{While}[\beta - q \neq 0 \land i \leq n - 2, \\
&\qquad\qquad \beta = \frac{1}{\beta - q};\ q = \text{Floor}[\beta]; i{+}{+}; \\
&\qquad\qquad Q = \text{Append}[Q, q]];\ Q]
\end{aligned}$$

Ein eleganteres Programm:

$$\text{Kettenbruchentwicklung}[\alpha\_, n\_] := \text{Floor}[\text{NestList}[\frac{1}{\# - \text{Floor}[\#]}\&, \alpha, n-1]]$$

Lemma 4.2.14 Sei $\alpha \in \mathbb{R}$, $\alpha > 0$. Die Kettenbruchentwicklung von α ist genau dann endlich, wenn α rational ist.

Beweis: Sei $\alpha = \frac{a}{b}$ rational mit $a, b > 0$ und $(a,b) = 1$. Dann ist nach dem euklidischen Algorithmus

$$\begin{aligned}
&a = q_1 b + r_1\ , && \text{also } \frac{a}{b} = q_1 + \frac{1}{\frac{b}{r_1}},\ \text{falls } r_1 > 0 \\
&b = q_2 r_1 + r_2\ , && \text{also } \frac{b}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}},\ \text{falls } r_2 > 0, \\
&\vdots \\
&r_{k-2} = q_k r_{k-1},\ r_k = 0
\end{aligned}$$

Somit gilt $\frac{a}{b} = [q_1, \dots, q_k]$. □

Offensichtlich ist

$$[q_0, \dots, q_{n-1}, 1, 1] = \left[q_0, \dots, q_{n-1}, 1 + \frac{1}{1}\right] = [q_0, \dots, q_{n-1}, 2].$$

Um die Eindeutigkeit der Kettenbruchentwicklung einer rationalen Zahl zu erhalten muß man die letzte Stelle ≥ 2 wählen.

Lemma 4.2.15 Seien $q_0, q_0' \in \mathbb{N},\; q_1, \dots, q_n, q_1', \dots, q_m' \in \mathbb{N}_+$.
Es gelte $q_n \geq 2$ und $q_m' \geq 2$. Gilt nun

$$[q_0, \dots, q_n] = [q_0', \dots, q_m'],$$

so folgt $n = m$ und $q_i = q_i'$ für $i = 0, \dots, n$

Beweis: Ohne Einschränkung sei $n \leq m$. Induktion nach n:
$n = 0:\quad q_0 = [q_0] = [q_0', \dots, q_m']$. Annahme: $m > 1$. Dann ist $0 < \frac{1}{[q_1', \dots, q_m']} < 1$, weil $q_1', \dots, q_m' > 0, q_m' \geq 2$. Andererseits gilt $[q_1', \dots, q_n'] = q_0 - q_0' \in \mathbb{Z}$, was nicht sein kann. Also ist $m = 0$ und $q_0 = q_0'$.
$n-1 \to n:$ Aus $[q_0, \dots, q_n] = [q_0', \dots, q_m']$ folgt $q_0 + \frac{1}{[q_1, \dots, q_n]} = q_0' + \frac{1}{[q_1', \dots, q_m']}$. Da $q_n = q_n' \geq 2$ folgt $0 < \frac{1}{[q_1', \dots, q_n']}, \frac{1}{[q_1', \dots, q_m']} < 1$, also $q_0 = q_0'$ und $[q_1, \dots, q_n] = [q_1', \dots, q_m']$.
Nach Induktionsvoraussetzung folgt

$$n = m \;\text{ und }\; q_1 = q_1', \dots, q_n = q_n'$$

□

Lemma 4.2.16 Ist $\alpha \in \mathbb{R} \backslash \mathbb{Q}, \alpha > 0$, so konvergiert die Kettenbruchentwicklung $[q_0, q_1, q_2, \dots]$ von α gegen α.
Wir schreiben daher auch

$$\alpha = [q_0, q_1, q_2, \dots]$$

Beweis: Es gilt mit den Bezeichnungen von Definition 4.2.13

$$\begin{aligned}\alpha - [q_0, \dots, q_n] &= [q_0, \dots, q_n, \alpha_{n+1}] - [q_0, \dots, q_n] \\ &\underset{[Lemma\, 4.2.11]}{=} \frac{a_{n-1} + a_n\alpha_{n+1}}{b_{n-1} + b_n\alpha_{n+1}} - \frac{a_n}{b_n} = \frac{(-1)^n}{b_n(b_{n-1} + b_n\alpha_{n+1})} \longrightarrow 0 \text{ für } n \to \infty.\end{aligned}$$

Dabei ist $[q_0, \dots, q_n] = \frac{a_n}{b_n}$ der n-te Näherungsbruch. □

Lemma 4.2.17 Seien

$$\alpha = [q_0, q_1, q_2, \dots],\; \alpha' = [q_0', q_1', q_2', \dots]$$

zwei unendliche Kettenbrüche, $q_0, q_0' \in \mathbb{N}$, $q_i, q_i' \in \mathbb{N}_+$ für $i > 0$. Gilt nun $\alpha = \alpha'$, so gilt

$$q_i = q_i' \text{ für alle } i \geq 0.$$

Beweis: Es gilt
$\beta := [q_1, q_2, \dots] > 1$, weil $q_1 \geq 1$ und ebenso ist $\beta' = [q_1', q_2', \dots] > 1$. Es folgt $0 < \beta^{-1} < 1,\; 0 < \beta'^{-1} < 1$. Weiter gilt

$$\alpha = \lim_{n\to\infty} [q_0, \dots, q_n] = \lim_{n\to\infty} \left(q_0 + \frac{1}{[q_1, \dots, q_n]} \right) = q_0 + \frac{1}{\lim\limits_{n\to\infty} [q_1, \dots, q_n]} = q_0 + \beta^{-1}$$

und analog $\alpha' = q_0' + \beta'^{-1}$.

Aus $\alpha = \alpha'$ folgt wegen $q_0, q_0' \in \mathbb{Z}$ und $0 < \beta^{-1} < 1$, $0 < \beta'^{-1} < 1$ sofort $q_0 = q_0'$ und $\beta = \beta'$. Jetzt kann man mit β und β' genauso verfahren und erhält schließlich

$$q_i = q_i' \text{ für alle } i \geq 0.$$

$\square$

Jetzt kommen wir zu den algebraischen Zahlen vom Grad 2 zurück.

Satz 4.2.18 Es sei $\alpha \in \mathbb{R} \backslash \mathbb{Q}$, $\alpha > 0$.
$\alpha = [q_0, q_1, \dots]$ sei die Kettenbruchentwicklung von α. Dann sind folgende Aussagen äquivalent.

(1) α ist algebraisch vom Grad 2

(2) $\exists\, k \geq -1$, $l \geq 1$, so daß

$$\begin{aligned}[q_0, q_1, \dots] &= [q_0, \dots, q_k\, q_{k+1}, \dots, q_{k+l},\ q_{k+1}, \dots, q_{k+l}, \dots \\ &= [q_0, \dots, q_k\, \overline{q_{k+1}, \dots, q_{k+l}}]\end{aligned}$$

ein periodischer Kettenbruch ist mit Vorperiode $(q_0, \dots, q_k)$ (leer, falls $k = -1$) und der Periode $(q_{k+1}, \dots, q_{k+l})$ der Länge $l \geq 1$. Es gilt also

$$q_{m+l} = q_m \text{ für alle } m > k.$$

Beweis: Wir brauchen im folgenden nur die Aussage (1) $\Longrightarrow$ (2).
Sei also $f = c_0x^2 + d_0x + e_0 \in \mathbb{Z}[x]$ mit $\mathrm{ggT}(c_0, d_0, e_0) = 1$ und

$$f(\alpha) = 0.$$

Es sei weiter $D_0 := d_0^2 - 4e_0c_0 \in \mathbb{Z}$ die Diskriminante von f. Da $\alpha \notin \mathbb{Q}$ besitzt f zwei verschiedene reelle Nullstellen, und somit ist $D_0 > 0$.
Nach Definition 4.2.13 ist

$$\begin{aligned}\alpha = \alpha_0,\ \alpha_0 &= q_0 + \frac{1}{\alpha_1},\ \alpha_1 = q_1 + \frac{1}{\alpha_2}, \dots \\ \alpha_{k+1} &= \frac{1}{\alpha_k - q_k},\end{aligned}$$

Behauptung: $\forall\ k \in \mathbb{N} \quad \exists\ c_k, d_k, e_k \in \mathbb{Z}$ mit $\mathrm{ggT}(c_k, d_k, e_k) = 1$, so daß α_k Nullstelle von

$$f_k = c_kx^2 + d_kx + e_k$$

ist und die Diskriminante $D_k = d_k^2 - 4c_ke_k$ mit D_0 übereinstimmt.
Beweis: Induktion nach k.
Für $k = 0$ ist nichts zu zeigen.
$k \longrightarrow k+1$. Es gelte schon

$$c_k\alpha_k^2 + d_k\alpha_k + e_k = 0.$$

Seien $c_{k+1}, d_{k+1}, e_{k+1} \in \mathbb{Z}$. Dann gilt wegen $\alpha_{k+1} = \frac{1}{\alpha_k - q_k}$

$$c_{k+1}\alpha_{k+1}^2 + d_{k+1}\alpha_{k+1} + e_{k+1} = 0 \Longleftrightarrow$$

[mit $(\alpha_k - q_k)^2$ multiplizieren]

$$\begin{aligned} &c_{k+1} + d_{k+1}(\alpha_k - q_k) + e_{k+1}(\alpha_k - q_k)^2 = 0 \Longleftrightarrow \\ &c_{k+1} - d_{k+1}q_k + e_{k+1}q_k^2 + (d_{k+1} - 2q_k e_{k+1})\alpha_k + e_{k+1}\alpha_k = 0. \end{aligned}$$

Setzt man für $c_{k+1}, d_{k+1}, e_{k+1}$ die Werte mit

$$(*) \qquad \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & -2q_k \\ 1 & -q_k & q_k^2 \end{pmatrix} \begin{pmatrix} c_{k+1} \\ d_{k+1} \\ e_{k+1} \end{pmatrix} = \begin{pmatrix} c_k \\ d_k \\ e_k \end{pmatrix}$$

so ist die Gleichung

$$c_{k+1}\alpha_{k+1}^2 + d_{k+1}\alpha_{k+1} + e_{k+1} = 0$$

erfüllt. Auflösen des linearen Gleichungssystems (*) liefert

$$\begin{aligned} c_{k+1} &= q_k^2 c_k + q_k d_k + e_k, \\ d_{k+1} &= 2q_k c_k + d_k, \\ e_{k+1} &= c_k, \end{aligned}$$

woraus man sofort

$$\mathrm{ggT}(c_{k+1}, d_{k+1}, e_{k+1}) = \mathrm{ggT}(c_k, d_k, e_k) = 1$$

abliest. Die Diskriminante ist ebenfalls unverändert:

$$\begin{aligned} D_{k+1} = &d_{k+1}^2 - 4c_{k+1}e_{k+1} = 4q_k^2 c_k^2 + 4q_k c_k d_k + d_k^2 \\ &- 4q_k^2 c_k^2 - 4q_k d_k c_k - 4e_k c_k = d_k^2 - 4e_k c_k = D_k. \end{aligned}$$

Wir wollen nun sehen, daß die Folge $(c_k)_{k \geq 0}$ beschränkt ist.
Dazu beachten wir, daß nach Konstruktion

$$\alpha = [q_0, \ldots, q_n, \alpha_{n+1}] = \frac{a_n\alpha_{n+1} + a_{n-1}}{b_n\alpha_{n+1} + b_{n-1}},$$

wobei $[q_0, \ldots, q_k] = \frac{a_k}{b_k}$ der k-te Näherungsbruch von α ist.
Aus $f(\alpha) = 0$ folgt dann

$$c_0(a_n\alpha_{n+1} + a_{n-1})^2 + d_0(a_n\alpha_{n+1} + a_{n-1})(b_n\alpha_{n+1} + b_{n-1}) + e_0(b_n\alpha_{n+1} + b_{n-1})^2 = 0$$

Ordnet man nach Potenzen von α_{n+1}, so folgt

$$\begin{aligned} &(c_0 a_n^2 + d_0 a_n b_n + e_0 b_n^2)\alpha_{n+1}^2 + \\ &+(2c_0 a_n a_{n-1} + d_0 a_n b_{n-1} + d_0 a_{n-1} b_n + 2e_0 b_n b_{n-1})\alpha_{n+1} + \\ &+c_0 a_{n-1}^2 + d_0 a_{n-1} b_{n-1} + e_0 b_{n-1}^2 = 0 \end{aligned}$$

Da aber auch
$$c_{n+1}\alpha_{n+1}^2 + d_{n+1}\alpha_{n+1} + e_{n+1} = 0 \quad \text{mit} \quad \mathrm{ggT}(c_{n+1}, d_{n+1}, e_{n+1}) = 1,$$
folgt, daß c_{n+1} ein Teiler von $c_0a_n^2 + d_0a_nb_n + e_0b_n^2$ ist (Übung!). Insbesondere ist
$$\begin{aligned}
|c_{n+1}| &\le |c_0a_n^2 + d_0a_nb_n + e_0b_n^2| \\
&= b_n^2\left|f\left(\frac{a_n}{b_n}\right)\right| = b_n^2\left|f\left(\alpha + \left(\frac{a_n}{b_n} - \alpha\right)\right)\right| \\
&= b_n^2\left|f'(\alpha)\left(\frac{a_n}{b_n} - \alpha\right) + \frac{f''(\alpha)}{2}\left(\frac{a_n}{b_n} - \alpha\right)^2\right| \\
&= b_n^2\left|(2c_0\alpha + d_0)\left(\frac{a_n}{b_n} - \alpha\right) + c_0\left(\frac{a_n}{b_n} - \alpha\right)^2\right| \\
&\underset{[Lemma\,4.2.16]}{=} b_n^2\left|(2c_0\alpha + d_0)\frac{(-1)^{n+1}}{b_n(b_{n-1} + b_n\alpha_{n+1})} + \frac{c_0}{b_n^2(b_{n-1} + b_n\alpha_{n+1})^2}\right| \\
&= \left|(2c_0\alpha + d_0)\frac{(-1)^{n+1}b_n}{b_{n-1} + b_n\alpha_{n+1}} + \frac{c_0}{(b_{n-1} + b_n\alpha_{n+1})^2}\right| \\
&\le |2c_0\alpha + d_0| + |c_0|.
\end{aligned}$$

Damit ist $(c_k)_{k\ge 0}$ beschränkt, also auch $e_k = c_{k-1}$ und somit schließlich auch $|d_k| = \sqrt{D_0 + 4c_ke_k}$.

Für die Tripel $(c_k, d_k, e_k) \in \mathbb{Z}^3$ gibt es also nur endlich viele Möglichkeiten, und damit treten auch nur endlich viele verschiedene Zahlen α_k in der Folge $(\alpha_k)_{k\ge 0}$ auf. Ist nun α_{k+1} die erste Zahl mit
$$\alpha_{k+1+l} = \alpha_{k+1} \text{ für ein } l \ge 1$$
und ist l minimal gewählt, so folgt
$$\begin{aligned}
\alpha &= [q_0, \ldots, q_k,\ \alpha_{k+1}] \\
&= [q_0, \ldots, q_n,\ q_{k+1}, \ldots, q_{k+l},\ \alpha_{k+1}] \\
&= [q_0, \ldots, q_k,\ q_{k+1}, \ldots, q_{k+l},\ q_{k+1}, \ldots, q_{k+l},\ \alpha_{k+1}] \\
&= [q_0, \ldots, q_k,\ \overline{q_{k+1}, \ldots, q_{k+l}}]
\end{aligned}$$

Die Behauptung ist bewiesen. □

Jetzt zeigen wir, daß die **Pellsche Gleichung** $x^2 - dy^2 = 1$ ($d \in \mathbb{N}_+$ quadratfrei) lösbar ist. Zur Gechichte der Pellschen Gleichung siehe [21].

Satz 4.2.19 Sei $d \in \mathbb{N}_+$ eine quadratfreie natürliche Zahl. Dann gibt es positive natürliche Zahlen $x, y \in \mathbb{N}_+$, so daß
$$x^2 - dy^2 = 1.$$

Beweis: Es sei $\alpha := \sqrt{d}$ und $[q_0, q_1, \ldots]$ sei die Kettenbruchentwicklung von α. Weiter sei $(\alpha_k)_{k\ge 0}$ durch
$$\alpha_0 = \alpha \qquad \text{und}$$
$$\alpha_{k+1} = \frac{1}{\alpha_k - q_k}, \quad k \ge 0$$

definiert. Es gilt also $\alpha_k \in \mathbb{Q}[\alpha]$ für alle k.
Somit gibt es eindeutig bestimmte rationale Zahlen $x_k, y_k \in \mathbb{Q}$, $y_k \neq 0$, so daß

$$\alpha_k = \frac{x_k + \sqrt{d}}{y_k}.$$

Es sei

$$\frac{a_n}{b_n} = [q_0, \ldots, q_n]$$

der n-te Näherungsbruch von α. Dann gilt

$$\begin{aligned}\sqrt{d} = [q_0, \ldots, q_{n-1}, \alpha_n] &= \frac{a_{n-2} + a_{n-1}\alpha_n}{b_{n-2} + b_{n-1}\alpha_n} = \\ &= \frac{a_{n-2}y_n + a_{n-1}(x_n + \sqrt{d})}{b_{n-2}y_n + b_{n-1}(x_n + \sqrt{d})}.\end{aligned}$$

Multipliziert man mit dem Nenner, so erhält man

$$db_{n-1} + (b_{n-2}y_n + b_{n-1}x_n)\sqrt{d} = a_{n-2}y_n + a_{n-1}x_n + a_{n-1}\sqrt{d},$$

und durch Koeffizientenvergleich bezüglich der $\mathbb{Q}$-Basis $(1, \sqrt{d})$ von $\mathbb{Q}[\alpha]$ ergibt sich

$$\begin{pmatrix} a_{n-1} & a_{n-2} \\ b_{n-1} & b_{n-2} \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} db_{n-1} \\ a_{n-1} \end{pmatrix}.$$

Da

$$\begin{pmatrix} a_{n-1} & a_{n-2} \\ b_{n-1} & b_{n-2} \end{pmatrix}^{-1} = \frac{1}{a_{n-1}b_{n-2} - a_{n-2}b_{n-1}} \begin{pmatrix} b_{n-2} & -a_{n-2} \\ -b_{n-1} & a_{n-1} \end{pmatrix}$$

und $a_{n-1}b_{n-2} - a_{n-2}b_{n-1} = (-1)^{n-1}$, folgt

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = (-1)^{n-1} \begin{pmatrix} d\,b_{n-1}b_{n-2} - a_{n-1}a_{n-2} \\ a_{n-1}^2 - d\,b_{n-1}^2 \end{pmatrix}.$$

Insbesondere sind x_n, y_n ganzzahlig, und für alle $n \geq 1$ gilt

$$(-1)^{n-1}y_n = a_{n-1}^2 - d\,b_{n-1}^2.$$

Nach Satz 4.2.18 ist die Folge $(\alpha_k)_k$ periodisch, also auch die Folge $(y_k)_k$.
Wir finden ein m und ein $k > 0$, so daß

$$y_{n+k} = y_n \text{ für alle } n \geq m.$$

Sei $e := (-1)^{m-1}y_m$. Dann ist $e = (-1)^n y_n$ für alle $n = m + l2k$, $l \geq 0$ und somit hat

$(*)$ $\qquad u^2 - dv^2 = e$

unendlich viele Lösungen, nämlich

$$\begin{aligned} u_l &= a_{m-1+2lk}, \\ v_l &= b_{m-1+2lk}, \qquad l \geq 0. \end{aligned}$$

Es gibt dann sicher zwei verschiedene Lösungen (u, v), (u', v') von $(*)$ mit

$$\begin{aligned} u &\equiv u' \bmod |e|, \\ v &\equiv v' \bmod |e|. \end{aligned}$$

Es folgt

$$uu' - dvv' \equiv u^2 - dv^2 \equiv 0 \bmod |e|$$

und

$$uv' - u'v \equiv uv - uv \equiv 0 \bmod |e|.$$

Es gibt daher $x, y \in \mathbb{Z}$ mit

$$\begin{aligned} ex &= uu' - dvv' \\ ey &= uv' - u'v. \end{aligned}$$

Man errechnet

$$\begin{aligned} e^2(x^2 - dy^2) &= (ex)^2 - d(ey)^2 = (uu' - dvv')^2 - d(uv' - u'v)^2 \\ &= (u^2 - dv^2)(u'^2 - dv'^2) = e^2, \end{aligned}$$

also

$$x^2 - dy^2 = 1.$$

Damit ist der Satz bewiesen. □

Übungen 4.2.20

(1) Benutze die Tatsache, daß $\mathbb{Z}[i]$ ein faktorieller Ring ist (vgl. Übung 11 in Abschnitt 1.2) um zu zeigen, daß jede Primzahl p mit $p \equiv 1 \bmod 4$ Summe zweier Quadratzahlen ist, d.h. $\exists\, a, b \in \mathbb{Z} : p = a^2 + b^2$.

(2) Es sei $K = \mathbb{Q}[\sqrt{-3}]$, $\omega = \dfrac{-1 + \sqrt{-3}}{2}$, $R = 0_K$. Beweise:

(a) $g = x^2 + x + 1$ ist das Minimalpolynom von ω.

(b) $R = \mathbb{Z} \oplus \mathbb{Z}\omega$. Für $n, m \in \mathbb{Z}$ sind $n + m\omega$ und $n + m\omega^2$ konjugiert, und es gilt

$$N(n + m\omega) = n^2 - nm + m^2$$

(c) Sei $\lambda = 1 - \omega$. Dann gilt

$$\lambda^2 R = 3R \text{ und } R/\lambda R \cong \mathbb{F}_3$$

(d) 5 ist irreduzibel in R, und $R/5R$ ist ein Körper mit 25 Elementen

(e) 7 besitzt eine Zerlegung $7 = \alpha\beta$ in R, so daß $R/\alpha R \cong \mathbb{R}/\beta R \cong \mathbb{F}_7$. Ist $R/7R$ ein Körper?

(3) Bestimme die Einheitengruppen $O_K^\times$ für $K = \mathbb{Q}[i]$, $K = \mathbb{Q}[\sqrt{3}i]$, $K = \mathbb{Q}[\sqrt{5}]$.

(4) Sei $u_0 = 1$, $u_1 = 1$, $u_{n+2} = u_n + u_{n+1}$ für $n \geq 0$ die Folge der Fibonacci-Zahlen. Zeige

(a) Der n-te Näherungsbruch von $[1, 1, \ldots]$ ist $\dfrac{u_{n+1}}{u_n}$, und es gilt

$$\gamma = \frac{1+\sqrt{5}}{2} = \lim_{n\to\infty} \frac{u_{n+1}}{u_n}, \ \ u_n = \left[\frac{\gamma^{n+1}}{\sqrt{5}}\right] + \frac{1+(-1)^n}{2}.$$

(b) Seien $p, q \in \mathbb{N}_+$ mit $0 < p < q$ und $q < u_{n+1}$.
Zeige: Der euklidische Algorithmus $q = b_1 p + r_1, \ p = b_2 r_1 + r_2, \ldots$ endet nach höchstens $n-1$ Divisionen, außer im Fall $p = u_n, \ q = u_{n+1}$, in welchem n Divisionen notwendig sind.

(5) (a) Entwickle $\dfrac{5+\sqrt{3}}{7}$ in einen Kettenbruch.

(b) Zeige: Für $n \in \mathbb{N}_+$ ist $\sqrt{n^2+1} = [n, \overline{2n}]$

(c) Zeige: Für $n \in \mathbb{N}_+$ ist $\sqrt{(n+1)^2-1} = [n, \overline{1, 2n}]$

(6) Finde eine Lösung $(x, y) \in \mathbb{Z}^2$ der Gleichung

$$x^2 - dy^2 = 1$$

für $d = 2, 3, 5, 15$ Man versuche auch $d = 61$

(7) (a) Es sei $a \in \mathbb{N}_+$ und $\alpha = [a, a, \ldots]$. Berechne α.

(b) Berechne $\alpha = [1, 2, 1, 2, 1, 2, \ldots]$.

(c) Es seien $a, b, c \in \mathbb{N}_+$. Zeige:

$$\alpha = [a, b, c, \ a, b, c, \ldots] \text{ und } \ \beta = \frac{1}{[c, b, a, \ c, b, a, \ldots]}$$

sind Nullstellen desselben quadratischen Polynoms in $\mathbb{Z}[x]$.

(8) (Für ***Mathematica*** -Fans) Schreibe ein Programm

(a) zur Kettenbruchentwicklung einer Zahl

(b) zur periodischen Kettenbruchentwicklung einer algebraischen Zahl vom Grad 2

(c) zur Pellschen Gleichung. Prüfe das Programm an den Gleichungen $x^2 - 61y^2 = 1$, $x^2 - 109y^2 = 1$, die Fermat einem Kollegen zur Lösung vorgelegt hat. Noch schwieriger ist $x^2 - 94y^2 = 1$.

4.3 Ideale

Wir setzen die Untersuchung der algebraischen Zahlkörper noch etwas fort. Es sei $K = \mathbb{Q}[\alpha]$ algebraischer Zahlkörper vom Grad m.

Definition 4.3.1 Für $\gamma_1, \ldots, \gamma_m \in K$ heißt

$$\Delta_{K/\mathbb{Q}}(\gamma_1, \ldots, \gamma_m) = \Delta(\gamma_1, \ldots, \gamma_m) := \det(Tr_{K/\mathbb{Q}}(\gamma_i\gamma_j)_{i,j=1,\ldots,m})$$

die **Diskriminante** von $\gamma_1, \ldots, \gamma_m$ (in $K/\mathbb{Q}$).

Satz 4.3.2 $\gamma_1, \ldots, \gamma_m$ sind $\mathbb{Q}$-linear unabhängig $\Longleftrightarrow \Delta(\gamma_1, \ldots, \gamma_m) \neq 0$.

Beweis:

(1) Seien $\gamma_1, \ldots, \gamma_m$ $\mathbb{Q}$-linear abhängig. Dann gibt es ein $(a_1, \ldots, a_m) \in \mathbb{Q}^m \backslash 0$, so daß

$$\sum_{i=1}^{m} a_i\gamma_i = 0.$$

Es folgt

$$\sum a_i Tr(\gamma_i\gamma_j) = Tr(\sum a_i\gamma_i\gamma_j) = Tr(0 \cdot \gamma_j) = 0$$

für alle $j = 1, \ldots, m$. Also gilt $\det(Tr(\gamma_i\gamma_j)) = 0$.

(2) Sei $\det(Tr(\gamma_i\gamma_j)) = 0$. Dann besitzt das lineare Gleichungssystem

$$\sum_{i=1}^{m} x_i Tr(\gamma_i\gamma_j) = 0, \quad j = 1, \ldots, m$$

eine nichttriviale Lösung $(a_1, \ldots, a_m) \in \mathbb{Q}^m \backslash 0$.

Setze $\gamma := \sum_{i=1}^{m} a_i\gamma_i$. Dann gilt

$$Tr(\gamma \cdot \gamma_j) = \sum a_i Tr(\gamma_i\gamma_j) = 0 \quad \forall\, j = 1, \ldots, m,$$

also

$$Tr(\gamma\beta) = 0 \quad \forall\, \beta \in \mathbb{Q}\gamma_1 + \cdots + \mathbb{Q}\gamma_m.$$

Wären nun $\gamma_1, \ldots, \gamma_m$ linear unabhängig, so wäre $\mathbb{Q}\gamma_1 + \cdots + \mathbb{Q}\gamma_m = K,\ \gamma \neq 0$ und somit $0 = Tr(\gamma\gamma^{-1}) = Tr(1) = m$, Widerspruch! □

Lemma 4.3.3 Sind $(\gamma_1, \ldots, \gamma_m)$, $(\gamma'_1, \ldots, \gamma'_m)$ $\mathbb{Q}$-Basen von K und ist $\gamma_i = \sum_{j=1}^{m} a_{ij}\gamma'_j,\ a_{ij} \in \mathbb{Q}$, so gilt

$$\Delta(\gamma_1, \ldots, \gamma_m) = (\det(a_{ij}))^2 \Delta(\gamma'_1, \ldots, \gamma'_m).$$

Beweis: $Tr(\gamma_i\gamma_j) = \sum_{k,l} a_{ik} Tr(\gamma'_k\gamma'_l) a_{jl}$. □

Satz 4.3.4 Seien

$$\varphi_1, \dots, \varphi_m : K \longrightarrow \mathbb{C}$$

die verschiedenen Homomorphismen von K in $\mathbb{C}$. Dann gilt

$$\Delta(\gamma_1, \dots, \gamma_m) = \Big(\det\big(\varphi_i(\gamma_j)\big)\Big)^2.$$

Beweis: Nach Satz 4.1.21 gilt

$$Tr(\gamma_i\gamma_j) = \sum_{\nu=1}^{m} \varphi_\nu(\gamma_i\gamma_j) = \sum_{\nu=1}^{m} \varphi_\nu(\gamma_i)\varphi_\nu(\gamma_j),$$

also $\det Tr(\gamma_i\gamma_j) = \Big(\det\big(\varphi_\nu(\gamma_i)\big)\Big)^2$. □

Korollar 4.3.5 Seien $\alpha_1, \dots, \alpha_m$ die Konjugierten von α. Dann gilt

$$\Delta(1, \alpha, \dots, \alpha^{m-1}) = \prod_{i<j} (\alpha_j - \alpha_i)^2.$$

Beweis:

$$\Delta(1, \alpha, \dots, \alpha^{m-1}) = \det \begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{m-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{m-1} \\ \vdots & & & \\ 1 & \alpha_m & \dots & \alpha_m^{m-1} \end{pmatrix}^2$$

ist die Vandermondesche Determinante. □

Definition 4.3.6 Eine nichtleere Teilmenge $\mathfrak{a} \subset K$ heißt **gebrochenes Ideal** in $K \Longleftrightarrow$

(1) $\beta, \gamma \in \mathfrak{a} \Longrightarrow \beta - \gamma \in \mathfrak{a}$

(2) $\beta \in \mathfrak{a},\ \gamma \in O_K \Longrightarrow \beta\gamma \in \mathfrak{a}$

(3) $\exists\ \gamma \in O_K \backslash 0$, so daß $\gamma\mathfrak{a} \subset O_K$

Ein gebrochenes Ideal $\mathfrak{a}$ heißt **ganz**, wenn $\mathfrak{a} \subset O_K$. Ein gebrochenes Ideal $\mathfrak{a}$ heißt **gebrochenes Hauptideal**, wenn ein $\beta \in K$ existiert mit $\mathfrak{a} = \beta O_K$. Wir schreiben auch $\langle\beta\rangle$ an Stelle von βO_K. Weiter nennen wir ganze Ideale auch kurz Ideale in O_K. Für Ideale in O_K ist die Bedingung (3) natürlich automatisch erfüllt.

Mit $\mathcal{J}_K$ bezeichnen wir die Menge aller gebrochenen Ideale $\mathfrak{a} \neq \{0\}$ in K und mit $\mathcal{P}_K$ bezeichnen wir die Menge der gebrochenen Hauptideale $\beta O_K,\ \beta \neq 0$.

Sind $\mathfrak{a}, \mathfrak{b} \in \mathcal{J}_K$, so ist auch

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_{i=1}^{k} \alpha_i\beta_i \;\middle|\; \alpha_i \in \mathfrak{a},\ \beta_i \in \mathfrak{b} \right\}$$

ein gebrochenes Ideal. Die Eigenschaften (1) und (2) sind klar. Zu (3): Seien $\gamma, \delta \in O_K$ mit $\gamma\mathfrak{a} \subset O_K$ und $\delta\mathfrak{b} \subset O_K$. Dann ist leicht zu sehen, daß $(\gamma\delta)(\mathfrak{a} \cdot \mathfrak{b}) \subset O_K$.

Definition 4.3.7 $\mathfrak{a} \cdot \mathfrak{b}$ heißt das **Produkt** von $\mathfrak{a}$ und $\mathfrak{b}$.

Sind $\langle\beta\rangle = \beta O_K$, $\langle\gamma\rangle = \gamma O_K$ Hauptideale, so ist auch

$$\langle\beta\rangle \cdot \langle\gamma\rangle = \beta\gamma O_K = \langle\beta\gamma\rangle$$

ein Hauptideal.
Ist $\langle\beta\rangle \neq \langle 0\rangle$, so ist $\langle\beta^{-1}\rangle$ ein Hauptideal mit

$$\langle\beta\rangle \cdot \langle\beta^{-1}\rangle = O_K.$$

Damit ist $\mathcal{P}_K$ mit der Multiplikation eine Gruppe. Da zwei Hauptideale $\langle\beta\rangle$ und $\langle\gamma\rangle$ genau dann übereinstimmen, wenn

$$\beta = \varepsilon\gamma \text{ für eine Einheit } \varepsilon \in O_K^\times,$$

induziert der Homomorphismus $K^\times \longrightarrow \mathcal{P}_K$ einen Isomorphismus

$$K^\times / O_K^\times \xrightarrow{\cong} \mathcal{P}_K.$$

Man sieht sofort, daß auch für gebrochene Ideale $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathcal{J}_K$ die Regeln

$$\begin{aligned} (\mathfrak{a} \cdot \mathfrak{b}) \cdot \mathfrak{c} &= \mathfrak{a} \cdot (\mathfrak{b} \cdot \mathfrak{c}) \\ \mathfrak{a} \cdot \mathfrak{b} &= \mathfrak{b} \cdot \mathfrak{a} \\ \mathfrak{a} \cdot O_K &= \mathfrak{a} \end{aligned}$$

erfüllt sind. Es ist nicht so einfach zu beweisen, daß jedes gebrochene Ideal $\mathfrak{a} \in \mathcal{J}_K$ ein Inverses besitzt. Zunächst definieren wir

Definition 4.3.8 Sei $\mathfrak{a} \in \mathcal{J}_K$.

$$\mathfrak{a}^{-1} := \{\beta \in K \mid \beta\mathfrak{a} \subset O_K\}$$

Wir zeigen zunächst

Lemma 4.3.9 Ist $\mathfrak{a} \in \mathcal{J}_K$, so ist auch $\mathfrak{a}^{-1} \in \mathcal{J}_K$, und es gilt $\mathfrak{a}^{-1} \cdot \mathfrak{a} \subset O_K$.

Beweis: $\mathfrak{a}^{-1} \neq \emptyset$, weil $\mathfrak{a}$ ein gebrochenes Ideal ist.

(1) $\beta\mathfrak{a} \subset O_K,\ \gamma\mathfrak{a} \subset O_K \Longrightarrow (\beta - \gamma)\mathfrak{a} \subset O_K$ und

(2) $\beta\mathfrak{a} \subset O_K,\ \gamma \in O_K \Longrightarrow \gamma\beta\mathfrak{a} \subset O_K$

sind offensichtlich erfüllt.
Außerdem gibt es ein $\gamma \in O_K \backslash 0$, so daß $\gamma\mathfrak{a} \subset O_K$. Damit ist $\gamma\mathfrak{a} \subset \mathfrak{a} \cap O_K$, also $\mathfrak{a} \cap O_K \supsetneqq \{0\}$. Wähle $\gamma \in \mathfrak{a} \cap O_K$, $\gamma \neq 0$. Dann ist $\gamma\mathfrak{a}^{-1} \subset \mathfrak{a} \cdot \mathfrak{a}^{-1} \subset O_K$, also erfüllt $\mathfrak{a}^{-1}$ auch das Axiom (3). □

Um zu zeigen, daß

$$\mathfrak{a}^{-1}\mathfrak{a} = O_K$$

für jedes gebrochene Ideal $\mathfrak{a} \in \mathcal{J}_K$ gilt, genügt es, dies für Ideale $\mathfrak{a} \subset O_K$ zu beweisen. Das sieht man so ein:

Jedes gebrochene Ideal in K ist von der Form $a\mathfrak{a}$, wobei $a \in K^\times$ und $\mathfrak{a} \subset O_K$ Ideal, $\mathfrak{a} \neq \langle 0 \rangle$. Weiter gilt

$$b \in (a\mathfrak{a})^{-1} \Longleftrightarrow ba\mathfrak{a} \subset O_K \Longleftrightarrow ba \in \mathfrak{a}^{-1} \Longleftrightarrow b \in a^{-1}\mathfrak{a}^{-1},$$

also ist $(a\mathfrak{a})^{-1} = a^{-1}\mathfrak{a}^{-1}$ und somit

$$(a\mathfrak{a})^{-1}(a\mathfrak{a}) = a^{-1}\mathfrak{a}^{-1}a\mathfrak{a} = \mathfrak{a}^{-1}\mathfrak{a}.$$

Der Nachweis, daß $\mathfrak{a}^{-1} \cdot \mathfrak{a} = O_K$ für Ideale $\mathfrak{a} \in O_K$ gilt, ist nicht ganz einfach. Es sind einige Vorbereitungen nötig. Wir erinnern zunächst an einige algebraische Grundbegriffe.

Definition 4.3.10 Es sei R ein kommutativer Ring mit Eins.

(1) Ein **Ideal** $\mathfrak{a} \subset R$ ist eine nichtleere Teilmenge mit den Eigenschaften

 (a) $a, b \in \mathfrak{a} \Longrightarrow a - b \in \mathfrak{a}$

 (b) $a \in \mathfrak{a},\ r \in R \Longrightarrow ra \in \mathfrak{a}$

(2) Ein Ideal $\mathfrak{p} \subset R$ heißt **Primideal** in $R :\Longleftrightarrow \mathfrak{p} \neq R$, und es gilt

$$\forall\, a, b \in R:\ ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p}$$

(3) Ein Ideal $\mathfrak{m} \subset R$ heißt **maximal** in $R :\Longleftrightarrow \mathfrak{m} \neq R$, und es gilt:
Ist $\mathfrak{a} \subset R$ Ideal, $\mathfrak{a} \neq R$ mit $\mathfrak{m} \subset \mathfrak{a}$, so ist

$$\mathfrak{m} = \mathfrak{a}.$$

Definition 4.3.11 Sei R ein kommutativer Ring mit Eins. $\mathfrak{a} \subset R$ ein Ideal. Dann wird der **Restklassenring** $R/\mathfrak{a}$ definiert als die Menge der Restklassen $a + \mathfrak{a}$, $a \in R$ mit den Verknüpfungen

$$(a + \mathfrak{a}) + (b + \mathfrak{a}) := (a + b) + \mathfrak{a},$$
$$(a + \mathfrak{a}) \cdot (b + \mathfrak{a}) := ab + \mathfrak{a}.$$

Man sieht leicht, daß dadurch $R/\mathfrak{a}$ ein kommutativer Ring mit Eins wird, so daß $R \longrightarrow R/\mathfrak{a}$, $a \longmapsto a + R$, ein surjektiver Ringhomomorphismus mit $\mathfrak{a}$ als Kern ist.

Lemma 4.3.12 Sei R ein kommutativer Ring mit Eins und $\mathfrak{a} \subset R$ ein Ideal.

(a) $\mathfrak{a}$ ist Primideal $\Longleftrightarrow R/\mathfrak{a}$ ist Integritätsbereich.

(b) $\mathfrak{a}$ ist maximales Ideal $\Longleftrightarrow R/\mathfrak{a}$ ist Körper.

Beweis: Der Beweis ergibt sich aus folgenden Feststellungen:

(1) $ab \in \mathfrak{a} \Longleftrightarrow (a + \mathfrak{a})(b + \mathfrak{a}) = 0,$

(2) Ideale in $R/\mathfrak{a} \overset{1-1}{\longleftrightarrow}$ Ideale $\mathfrak{b}$ in R mit $\mathfrak{a} \subset \mathfrak{b}$. $\square$

Satz 4.3.13 (1) Ist $\mathfrak{a} \in \mathcal{J}_K$, so gibt es eine $\mathbb{Q}$-Vektorraumbasis $\gamma_1, \ldots, \gamma_m$ von K, so daß $\gamma_1, \ldots, \gamma_m \in \mathfrak{a}$.

(2) Ist $\mathfrak{a} \in \mathcal{J}_K$, so ist $\mathfrak{a}$ eine freie abelsche Gruppe vom Rang m.

Genauer gilt

(3) Sei $\mathfrak{a} \subset O_K$ Ideal, $\mathfrak{a} \neq \langle 0 \rangle$.

$(\gamma_1, \ldots, \gamma_m)$ sei ein $\mathbb{Q}$-Basis von K in $\mathfrak{a}$ mit minimalem Betrag der Diskriminante $|\Delta(\gamma_1, \ldots, \gamma_m)| \in \mathbb{N}_+$ unter allen $\mathbb{Q}$-Basen von K in $\mathfrak{a}$. Dann ist $\gamma_1, \ldots, \gamma_n$ eine $\mathbb{Z}$-Basis von $\mathfrak{a}$, d.h. jedes Element $\gamma \in \mathfrak{a}$ hat eine eindeutige Darstellung

$$\gamma = \sum_{i=1}^{m} a_i \gamma_i \text{ mit } a_i \in \mathbb{Z}.$$

Beweis: zu (1): Sei $\gamma_1', \ldots, \gamma_m'$ irgendeine $\mathbb{Q}$-Basis von K. Wähle $c \in \mathbb{Z} \backslash 0$, so daß $c\gamma_1', \ldots, c\gamma_m'$ ganz algebraisch sind. Weiter sei $\beta \in \mathfrak{a}$, $\beta \neq 0$. Dann gilt $\gamma_i := \beta c \gamma_i' \in \mathfrak{a}$. Da $\beta c \neq 0$, ist auch $(\gamma_1, \ldots, \gamma_m)$ $\mathbb{Q}$-Basis von K.

zu(2): Dies folgt aus (3).

zu (3): Sei $(\gamma_1, \ldots, \gamma_m)$ eine $\mathbb{Q}$-Basis von K in $\mathfrak{a}$.

$$\begin{gathered} \mathfrak{a} \subset O_K \Longrightarrow \gamma_i \gamma_j \in O_K \Longrightarrow Tr(\gamma_i \gamma_j) \in \mathbb{Z} \Longrightarrow \\ \Delta(\gamma_1, \ldots, \gamma_m) = \det Tr(\gamma_i \gamma_j) \in \mathbb{Z} \backslash 0 \Longrightarrow \exists\ \mathbb{Q}\text{-Basis} \end{gathered}$$

$(\gamma_1, \ldots, \gamma_m)$ von K in $\mathfrak{a}$, so daß $|\Delta(\gamma_1, \ldots, \gamma_m)|$ minimal.

Annahme: $\exists\ \gamma \in \mathfrak{a}$, so daß die Darstellung

$$\gamma = \sum_{i=1}^{m} c_i \gamma_i \qquad (c_i \in \mathbb{Q})$$

keine ganzzahlige Linearkombination ist.

Sei etwa $c_1 \notin \mathbb{Z}$. Dann ist

$$c_1 = n_1 + r \;\text{ mit }\; n_1 \in \mathbb{Z},\ 0 < r < 1,\ r \in \mathbb{Q}.$$

Es folgt $\widetilde{\gamma}_1 := \gamma - n_1\gamma_1 = r\gamma_1 + c_2\gamma_2 + \cdots + c_m\gamma_m \in \mathfrak{a}$ und $(\widetilde{\gamma}_1, \gamma_2, \ldots, \gamma_m)$ ist ebenfalls $\mathbb{Q}$-Basis von K in $\mathfrak{a}$. Nach Lemma 4.3.3 gilt

$$\begin{aligned} |\Delta(\widetilde{\gamma}_1, \gamma_2, \ldots, \gamma_m)| &= \det \begin{pmatrix} r & 0 & \ldots & 0 \\ c_2 & 1 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ c_m & 0 & \ldots & 1 \end{pmatrix}^2 |\Delta(\gamma_1, \ldots, \gamma_m)| \\ &= r^2\, |\Delta(\gamma_1, \ldots, \gamma_m)| < |\Delta(\gamma_1, \ldots, \gamma_m)| \end{aligned}$$

im Widerspruch zur Minimalität von $|\Delta(\gamma_1, \ldots, \gamma_m)|$. $\square$

Definition 4.3.14 Sei $\mathfrak{a} \in \mathcal{J}_K$.

(1) $(\gamma_1, \ldots, \gamma_m)$ heißt **Ganzheitsbasis von $\mathfrak{a}$**: $\Longleftrightarrow$ $(\gamma_1, \ldots, \gamma_n)$ ist $\mathbb{Z}$-Basis von $\mathfrak{a}$.

(2) $\Delta(\mathfrak{a}) := \Delta(\gamma_1, \ldots, \gamma_n)$, wobei $(\gamma_1, \ldots, \gamma_n)$ irgendeine Ganzheitsbasis von $\mathfrak{a}$ ist, heißt die **Diskriminante von $\mathfrak{a}$.**

Da zwei Ganzheitsbasen sich um eine **unimodulare Matrix** $(a_{ij}) \in GL_n(\mathbb{Z})$ unterscheiden, ist $\Delta(\mathfrak{a})$ wohldefiniert.

(3) $\delta_K = \Delta(O_K)$ heißt auch die Diskriminante von K.

Satz 4.3.15 Ist $\mathfrak{a} \subset O_K$ Ideal, $\mathfrak{a} \neq \langle 0 \rangle$, so ist der Restklassenring $O_K/\mathfrak{a}$ endlich. Für $a \in \mathbb{N}_+$ ist $|O_K/aO_K| = a^m$.

Beweis:

(1) $\mathfrak{a} \cap \mathbb{N}_+ \neq \emptyset$, denn:
Ist $\beta \in \mathfrak{a}$, $\beta \neq 0$, so gibt ganze Zahlen $b_0, \ldots, b_{k-1} \in \mathbb{Z}$, $b_0 \neq 0$, so daß

$$\beta^k + b_{k-1}\beta^{k-1} + \cdots + b_1\beta + b_0 = 0, \text{ also } b_0 \in \mathfrak{a}.$$

(2) Wähle $a \in \mathfrak{a} \cap \mathbb{N}_+$. Dann ist $aO_K \subset \mathfrak{a}$, und somit ist $O_K/aO_K \longrightarrow O_K/\mathfrak{a}$ surjektiv. O_K/aO_K ist aber endlich von der Ordnung a^m. Um das zu sehen, wähle man eine Ganzheitsbasis $\gamma_1, \ldots, \gamma_m$ von O_K.

$$\mathbb{Z}^m \longrightarrow O_K, \ (c_1, \ldots, c_m) \longmapsto \sum c_i\gamma_i$$

induziert dann einen Isomorphismus additiver abelscher Gruppen

$$(\mathbb{Z}/a\mathbb{Z})^m \longrightarrow O_K/aO_K.$$

□

Es folgt nun

Satz 4.3.16 O_K hat folgende Eigenschaften

(1) O_K ist Integritätsring mit Quotientenkörper K.

(2) Jedes Ideal $\mathfrak{a} \subset O_K$ ist **endlich erzeugt**, d.h. $\exists\ \gamma_1, \ldots, \gamma_k \in \mathfrak{a}$, so daß

$$\mathfrak{a} = \langle \gamma_1, \ldots, \gamma_k \rangle = \left\{ \sum_{i=1}^{k} \beta_i\gamma_i \mid \beta_i \in O_K \right\}$$

(Man sagt: O_K ist **noetherscher Ring**.)

(3) Ist $\beta \in K$ und $g \in O_K[x]$ normiert mit $g(\beta) = 0$, so ist $\beta \in O_K$.

(Man sagt: O_K ist **normal**.)

(4) Jedes von Null verschiedene Primideal $\mathfrak{p} \subset O_K$ ist maximal.
(Man sagt: O_K ist **eindimensional**.)

Beweis: (1) ist klar wegen 4.3.13 (a).
(2) folgt aus 4.3.13 (b).
Zu (3): Wir wenden hier wieder Satz 4.1.4 an.
Es sei $\beta \in K$ und

$$\beta^l + \alpha_{l-1}\beta^{l-1} + \cdots + \alpha_0 = 0$$

mit ganzen algebraischen Zahlen $\alpha_i \in O_K$.
Dann ist der Unterring

$$\mathbb{Z}[\alpha_0, \ldots, \alpha_{l-1}] \subset \mathbb{I}$$

als additive abelsche Gruppe endlich erzeugt und somit ist auch

$$M = \sum_{i=0}^{l-1} \mathbb{Z}[\alpha_0, \ldots, \alpha_{l-1}]\beta^i$$

eine endlich erzeugte abelsche Gruppe.
Es gilt nun, wie man leicht sieht,

$$\beta M \subset M,$$

und daher ist β ganz algebraisch. Das beweist (3).
Zu (4): $\mathfrak{p}$ Primideal, $\mathfrak{p} \neq \langle 0 \rangle \Longrightarrow R = O_K/\mathfrak{p}$ ist ein endlicher Integritätsbereich, also ein Körper, (denn für $a \in R \backslash O$ ist $R \to R$, $b \longmapsto ab$, injektiv, also bijektiv. 1 wird also erreicht: $\exists\, b \in R : b \longmapsto 1 = ab$).
Nach Lemma 4.3.11 ist $\mathfrak{p}$ maximal. □

Lemma 4.3.17 Zu jedem von Null verschiedenen Ideal $\mathfrak{a}$ in O_K gibt es maximale Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in O_K, so daß

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset \mathfrak{a}.$$

Beweis: Annahme: Es gibt ein von Null verschiedenes Ideal in O_K, das kein Produkt von maximalen Idealen enthält. Es sei $\mathfrak{M}$ die Menge aller dieser Ideale in O_K. Es gibt ein maximales Element in $\mathfrak{M}$, denn gäbe es das nicht, so könnte man eine echte aufsteigende Kette

$$\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \ldots$$

von Idealen $\mathfrak{a}_i \in \mathfrak{M}$ konstruieren, und $\mathfrak{a} = \bigcup_{i=1}^{\infty} \mathfrak{a}_i$ wäre auch ein Ideal in O_K, welches nach 4.3.16 (2) von endlich vielen Elementen $\gamma_1, \ldots, \gamma_k \in O_K$ erzeugt wäre, die alle in einem geeigneten $\mathfrak{a}_m$ liegen müßten, was den Widerspruch

$$\mathfrak{a}_m = \mathfrak{a}_{m+1} = \ldots = \mathfrak{a}$$

nach sich zöge. Sei also $\mathfrak{a} \in \mathfrak{M}$ maximal in $\mathfrak{M}$. $\mathfrak{a}$ ist kein Primideal (nach Definition von $\mathfrak{M}$). Also gibt es Zahlen $a, b \in O_K \backslash \mathfrak{a}$ mit $ab \in \mathfrak{a}$.

$$\mathfrak{a}_1 = \langle a \rangle + \mathfrak{a}, \ \mathfrak{a}_2 = \langle b \rangle + \mathfrak{a}$$

sind dann echte Oberideale von $\mathfrak{a}$ in O_K. Da $\mathfrak{a}$ maximal in $\mathfrak{M}$ ist, gilt $\mathfrak{a}_1, \mathfrak{a}_2 \notin \mathfrak{M}$ und somit enthält sowohl $\mathfrak{a}_1$ als auch $\mathfrak{a}_2$ ein Produkt von maximalen Idealen und damit auch $\mathfrak{a}$, weil

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subset \langle ab \rangle + \mathfrak{a} \subset \mathfrak{a}.$$

Also gilt $\mathfrak{a} \notin \mathfrak{M}$ im Widerspruch zu $\mathfrak{a} \in \mathfrak{M}$. Damit ist die Behauptung bewiesen. □

Lemma 4.3.18 Ist $\mathfrak{a} \subset O_K$ Ideal, $\mathfrak{p} \subset O_K$ maximales Ideal, so ist

$$\mathfrak{a}\mathfrak{p}^{-1} \supsetneqq \mathfrak{a}.$$

Beweis:

(1) Sei $a \in \mathfrak{p}, \ a \neq 0$. Es sei $r > 0$ die kleinste Zahl, so daß maximale Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ mit

$$(*) \qquad \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset \langle a \rangle$$

existieren (beachte Lemma 4.3.17).

Dann gilt

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subset \mathfrak{p}.$$

Da $\mathfrak{p}$ ein Primideal ist, liegt eines der Ideale $\mathfrak{p}_i$ in $\mathfrak{p}$ (Übung) etwa $\mathfrak{p}_1 \subset \mathfrak{p}$. Da $\mathfrak{p}_1$ maximal ist, folgt $\mathfrak{p}_1 = \mathfrak{p}$. Wegen der Minimalität von r gilt

$$\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \not\subset \langle a \rangle$$

also gibt es ein $b \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \backslash \langle a \rangle$, und somit ist $a^{-1}b \notin O_K$, aber $a^{-1}b\mathfrak{p} = a^{-1}(b\mathfrak{p}_1) \subset O_K$, denn

$$b\mathfrak{p}_1 \subset \mathfrak{p}_2 \cdot \mathfrak{p} \cdot \ldots \cdot \mathfrak{p}_r \subset \langle a \rangle.$$

Es folgt also $a^{-1}b \in \mathfrak{p}^{-1} \backslash O_K$ und somit gilt

$$\mathfrak{p}^{-1} \supsetneqq O_K.$$

(2) Ist nun $\mathfrak{a} \subset O_K$ beliebiges Ideal, so ist $\mathfrak{a}$ als abelsche Gruppe endlich erzeugt. Ist nun $c \in \mathfrak{p}^{-1} \backslash O_K$, so folgt aus Satz 4.1.4

$$c\mathfrak{a} \not\subset \mathfrak{a},$$

also $\mathfrak{p}^{-1}\mathfrak{a} \neq \mathfrak{a}$. Da $O_K \subset \mathfrak{p}^{-1}$, ist auch $\mathfrak{a} \subset \mathfrak{p}^{-1} \cdot \mathfrak{a}$. □

Jetzt können wir folgende Verallgemeinerung des Hauptsatzes der elementaren Zahlentheorie beweisen.

Satz 4.3.19 Zu jedem von $\langle 0 \rangle$ und $\langle 1 \rangle$ verschiedenen Ideal $\mathfrak{a}$ in O_K gibt es eine bis auf die Reihenfolge der Faktoren eindeutige Darstellung

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$$

von $\mathfrak{a}$ als Produkt von Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in O_K.

Beweis:

(1) Existenz:

Es sei $\mathfrak{p}_1$ ein Primideal mit $\mathfrak{a} \subset \mathfrak{p}_1$. Ist $\mathfrak{a}$ Primideal, so ist $\mathfrak{a} = \mathfrak{p}_1$, und wir sind fertig. Andernfalls gilt nach 4.3.17

$$\mathfrak{a} \subsetneqq \mathfrak{a}\mathfrak{p}_1^{-1} = \mathfrak{a}_1 \quad \text{und} \quad \mathfrak{p}_1 \subsetneqq \mathfrak{p}_1\mathfrak{p}_1^{-1}.$$

Da $\mathfrak{p}_1$ maximal ist, gilt also $\mathfrak{p}_1\mathfrak{p}_1^{-1} = O_K$. Es folgt

$$\mathfrak{a} = O_K \cdot \mathfrak{a} = (\mathfrak{p}_1\mathfrak{p}_1^{-1})\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}_1.$$

Nun sei $\mathfrak{p}_2$ ein Primideal mit $\mathfrak{a}_1 \subset \mathfrak{p}_2$.

Ist $\mathfrak{a}_1$ Primideal, so ist $\mathfrak{a}_1 = \mathfrak{p}_2$, also $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$, und wir sind wieder fertig. Ist $\mathfrak{a}_1$ kein Primideal, so erhält man

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{a}_2 \text{ mit } \mathfrak{a}_2 = \mathfrak{a}_1\mathfrak{p}_2^{-1}.$$

Nach endlich vielen Schritten bricht dies Verfahren ab, weil es keine echt aufsteigenden Idealketten $\mathfrak{a} \subsetneqq \mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \mathfrak{a}_3 \subsetneqq \dots$ in O_K gibt, wie der Beweis von 4.3.16 lehrt.

(2) Eindeutigkeit:

Es seien $\mathfrak{p}_1, \dots, \mathfrak{p}_r,\ \mathfrak{q}_1, \dots, \mathfrak{q}_s$ maximale Ideale und es gelte

$$\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s.$$

Dann folgt $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \subset \mathfrak{p}_1$, also $\mathfrak{q}_i \subset \mathfrak{p}_1$ für ein i. Da $\mathfrak{q}_i$ maximal ist, folgt $\mathfrak{q}_i = \mathfrak{p}_1$.

Ohne Einschränkung sei $i = 1$. Durch Multiplizieren mit $\mathfrak{p}_1^{-1}$ folgt

$$\mathfrak{p}_2 \dots \mathfrak{p}_r = \mathfrak{q}_2 \dots \mathfrak{q}_s,$$

und durch Induktion folgt die Behauptung. □

Satz 4.3.20 Zu jedem gebrochenen Ideal $\mathfrak{a} \in \mathcal{J}_K$ gibt es eindeutig bestimmte Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ in O_K und ganze Zahlen $\nu_1, \dots, \nu_r \in \mathbb{Z}\setminus\{0\}$, so daß

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \dots \mathfrak{p}_r^{\nu_r}.$$

$\mathcal{J}_K$ ist mit der Multiplikation eine abelsche Gruppe.
Genauer ist $\mathcal{J}_K$ die freie abelsche Gruppe mit der $\mathbb{Z}$-Basis $\mathrm{Max} O_K = \{\mathfrak{p} \subset O_K \mid \mathfrak{p}$ maximales Ideal$\}$.

Beweis: Wegen Satz 4.3.18 müssen wir nur noch zeigen, daß $\mathcal{J}_K$ eine Gruppe ist und dafür genügt es, wie wir uns schon überlegt haben, zu zeigen, daß

$$\mathfrak{a}\mathfrak{a}^{-1} \supset O_K$$

für alle Ideale $\mathfrak{a} \subset O_K$ gilt.
Sei zunächst $\mathfrak{p}$ ein maximales Ideal. Da $\mathfrak{p} \subsetneqq \mathfrak{p}\mathfrak{p}^{-1}$, folgt $\mathfrak{p}\mathfrak{p}^{-1} = O_K$. Ist nun

$$\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r,$$

so gilt für $\mathfrak{b} := \mathfrak{p}_1^{-1} \ldots \mathfrak{p}_r^{-1}$ die Gleichung

$$\mathfrak{a} \cdot \mathfrak{b} = \mathfrak{p}\mathfrak{p}_1^{-1} \ldots \mathfrak{p}_r\mathfrak{p}_r^{-1} = O_K,$$

und wegen $\mathfrak{p}_i \supset \mathfrak{a}$ folgt $\mathfrak{p}_i^{-1} \subset \mathfrak{a}^{-1}$, also $\mathfrak{b} \subset \mathfrak{a}^{-1}$ und somit

$$O_K = \mathfrak{a} \cdot \mathfrak{b} \subset \mathfrak{a} \cdot \mathfrak{a}^{-1}.$$

□

Definition 4.3.21 Die Faktorgruppe

$$Cl_K := \mathcal{J}_K / \mathcal{P}_K$$

heißt die **Idealklassengruppe** von K.
Offensichtlich gilt $Cl_K = \{1\}$ genau dann, wenn O_K ein Hauptidealring ist.

Wir illustrieren die Theorie an einigen Beispielen

Beispiel 4.3.22 Es sei $K = \mathbb{Q}[\alpha],\ \alpha = \sqrt{-5}$. Dann sind α und $-\alpha$ konjugiert und es gilt

$$\begin{aligned} N(a+b\alpha) &= (a+b\alpha)(a-b\alpha) = a^2+5b^2, \\ Tr(a+b\alpha) &= 2a. \\ a+b\alpha \in O_K &\Longleftrightarrow N(a+b\alpha),\ Tr(a+b\alpha) \in \mathbb{Z} \Longleftrightarrow a,b \in \mathbb{Z}. \end{aligned}$$

Also ist $O_K = \mathbb{Z} + \mathbb{Z}\alpha$ und $(1,\alpha)$ ist Ganzheitsbasis von O_K. Somit ist die Diskriminante

$$\delta_K = \Delta(O_K) = \Delta(1,\alpha) = \det \begin{pmatrix} 1 & \alpha \\ 1 & -\alpha \end{pmatrix}^2 = (-2\alpha)^2 = -20.$$

Auch

$$\det \begin{pmatrix} Tr(1) & Tr(\alpha) \\ Tr(\alpha) & Tr(\alpha^2) \end{pmatrix} = \det \begin{pmatrix} 2 & 0 \\ 0 & -10 \end{pmatrix} = -20$$

ergibt die Diskriminante.
Wir wollen die Primfaktorzerlegung von $\langle 2 \rangle = 2O_K$ bestimmen. Das Ergebnis ist:

$$\langle 2 \rangle = \mathfrak{p}^2, \quad \text{wobei } \mathfrak{p} = \langle 2, 1+\alpha \rangle.$$

Zunächst beweisen wir

$$\mathfrak{p} = \langle 2, 1+\alpha \rangle = \{2\beta + (1+\alpha)\gamma \mid \beta,\gamma \in O_K\}$$

ist Primideal. Beweis: Mit

$$\beta = a + b\alpha,\ \gamma = c + d\alpha,\ a, b, c, d \in \mathbb{Z},$$

ist

$$2\beta + (1+\alpha)\gamma = 2a + c - 5d + (2b + d + c)\alpha.$$

$\mathfrak{p}$ wird also als abelsche Gruppe in $\mathbb{Z}^2 \cong \mathbb{Z} + \mathbb{Z}\alpha$ von den Spalten der Matrix $\begin{pmatrix} 2 & 0 & 1 & -5 \\ 0 & 2 & 1 & 1 \end{pmatrix}$ erzeugt. Mit elementaren Spaltenumformungen erhält man

$$\begin{pmatrix} 2 & 0 & 1 & 1 \\ 0 & 2 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & -1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix},$$

d.h. $(2,\, 1+\alpha)$ ist eine Ganzheitsbasis von $\mathfrak{p}$. Da $(1,\, 1+\alpha)$ eine Ganzheitsbasis von O_K ist, sieht man, daß $O_K/\mathfrak{p}$ nur zwei Elemente besitzt, die Restklasse von 0 und die Restklasse von 1. $O_K/\mathfrak{p}$ ist also isomorph zu $\mathbb{F}_2$. $\mathfrak{p}$ ist somit ein Primideal. Weiter ergibt sich

$$\begin{aligned} \mathfrak{p}^2 &= \langle 4,\, 2(1+\alpha),\, (1+\alpha)^2 \rangle = \langle 4,\, 2+2\alpha,\, -4+2\alpha \rangle \\ &= \langle 4,\, 2+2\alpha,\, 2\alpha \rangle = \langle 4,\, 2,\, 2\alpha \rangle = \langle 2,\, 2\alpha \rangle = \langle 2 \rangle. \end{aligned}$$

Dabei haben wir die Regel $\langle a, b \rangle = \langle a - cb, b \rangle$ benutzt. Weiter zeigen wir:

Das Ideal $\mathfrak{p}$ ist kein Hauptideal.

Beweis: Annahme: $\mathfrak{p} = \langle \eta \rangle$. Dann gibt es Zahlen $\eta_1, \eta_2 \in O_K$, so daß

$$\begin{aligned} 1 + \alpha &= \eta_1 \eta, \\ 2 &= \eta_2 \eta. \end{aligned}$$

Es folgt $4 = N(2) = N(\eta_2)N(\eta)$. Da aber

$$N(a + b\alpha) = a^2 + 5b^2 = 1 \text{ oder } \geq 4, \text{ folgt } N(\eta) = 1 \text{ oder } 4.$$

Da η keine Einheit sein kann, folgt $N(\eta) = 4$ und somit ist η_2 eine Einheit, also $\mathfrak{p} = \langle 2 \rangle$. $1 + \alpha$ ist aber kein Vielfaches von 2. Widerspruch.

O_K ist also kein Hauptidealring. Man kann zeigen, daß $Cl_K = \{[O_K], [\mathfrak{p}]\}$ gilt.

Wir berechnen die Diskriminanten von $\mathfrak{p}$ und $\langle 2 \rangle$. Da $(2, 1+\alpha)$ eine Ganzheitsbasis von $\mathfrak{p}$ ist, ist

$$\begin{aligned} \Delta(\mathfrak{p}) = \Delta(2, 1+\alpha) &= \det \begin{pmatrix} 2 & 1+\alpha \\ 2 & 1-\alpha \end{pmatrix}^2 = 4 \begin{pmatrix} 1 & \alpha \\ 1 & -\alpha \end{pmatrix}^2 \\ &= 4\delta_K = -80 \end{aligned}$$

Da weiter $(2,\, 2\alpha)$ Ganzheitsbasis von $\langle 2 \rangle$ ist, folgt

$$\begin{aligned} \Delta(\langle 2 \rangle) = \Delta(2, 2\alpha) &= \det \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^2 \Delta(1, \alpha) \\ &= 2^4 \delta_K = -320 \end{aligned}$$

Beispiel 4.3.23 Im Fall $\alpha = \sqrt{d},\ d \in \mathbb{Z},\ d \equiv 1 \bmod 4$ ist $O_K = \mathbb{Z} + \gamma\mathbb{Z},\ \gamma = \frac{1+\alpha}{2},\ \gamma' = \frac{1-\alpha}{2}$,

$$\delta_K = \Delta(1,\gamma) = (\gamma - \gamma')^2 = \alpha^2 = d.$$

Beispiel 4.3.24 $\alpha = \sqrt[3]{2},\ K = \mathbb{Q}[\sqrt[3]{2}]$
Dann ist

$$\begin{aligned}
\Delta(1,\alpha,\alpha^2) &= \det \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha\omega & \alpha^2\omega^2 \\ 1 & \alpha\omega^2 & \alpha^2\omega \end{pmatrix}^2 = \alpha^6 \ \det \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}^2 \\
&= 2^2 \mid (\omega^2 - \omega^4 - \omega + \omega^2 + \omega^2 - \omega)^2 = \\
&= 2^2 3^2 (\omega^2 - \omega)^2 = 2^2 3^2 (1 + 2\omega)^2 = -2^2 3^3 \\
&= -108. \quad \text{vgl. Beispiel 4.1.10}
\end{aligned}$$

Bemerkung 4.3.25 Es gibt eine Beziehung zwischen algebraischer Zahlentheorie und algebraischer Geometrie. Ist K ein algebraischer Zahlkörper, $R = O_K$ der Ring der ganzen algebraischen Zahlen in K, so bezeichnen wir mit

$$\operatorname{Spec} R$$

die Menge aller Primideale in R. Wir erhalten eine Abbildung

$$\pi : \operatorname{Spec} R \longrightarrow \operatorname{Spec} \mathbb{Z}$$

mit

$$\pi(\mathfrak{p}) := \mathfrak{p} \cap \mathbb{Z}.$$

Diese Abbildung kann man sich als eine n-blättrige verzweigte Überlagerung vorstellen, wobei $n = \dim_{\mathbb{Q}} K$ der Grad des Zahlkörpers ist. Ist $\vartheta \in K$ ein primitives Element von K mit Minimalpolynom $f \in \mathbb{Z}[x]$, so ist $\mathbb{Z}[\vartheta] \cong \mathbb{Z}[x]/\langle f \rangle$ und $\mathbb{Z}[\vartheta] \subset R$. R ist der ganze Abschluß von $\mathbb{Z}[\vartheta]$ in K. Zu den Ringhomomorphismen

$$\mathbb{Z} \hookrightarrow \mathbb{Z}[x] \longrightarrow \mathbb{Z}[\vartheta] \hookrightarrow R$$

gehören 'geometrische' Abbildungen:

$$\widetilde{C} \underset{\nu}{\longrightarrow} C \underset{j}{\hookrightarrow} X \underset{pr}{\longrightarrow} B.$$

Dabei ist $B = \operatorname{Spec} \mathbb{Z}$ die **arithmetische Gerade** und $X = \operatorname{Spec} \mathbb{Z}[x]$ die **arithmetische Ebene**.

$pr : X \longrightarrow B,\ pr(\mathfrak{p}) = \mathfrak{p} \cap \mathbb{Z}$ ist die Projektion mit den Geraden $\operatorname{Spec} \mathbb{F}_p[x]$ als Fasern. $C = \operatorname{Spec} \mathbb{Z}[\vartheta]$ ist die durch die 'Gleichung' $f \in \mathbb{Z}[x]$ beschriebene Kurve in X. $\widetilde{C} = \operatorname{Spec} R \underset{\nu}{\longrightarrow} C$ ist die **Normalisierung** von C. $\widetilde{C}$ ist 'glatte' Kurve.

Für jeden Punkt $x = \langle p \rangle \in \operatorname{Spec} \mathbb{Z}$ besteht die Faser $\pi^{-1}(x) \subset \operatorname{Spec} R$ aus m verschiedenen Punkten $x_i = \mathfrak{p}_i,\ i = 1, \ldots, m$. Es gilt dann die fundamentale Beziehung

$$pR = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_m^{e_m}$$

und
$$n = \sum_{i=1}^{m} e_i f_i, \qquad \text{wobei } e_i \geq 1$$
und
$$f_i := \dim_{\mathbb{F}_p}(R/\mathfrak{p}_i) \geq 1.$$
e_i heißt der **Verzweigungsindex** von π im Punkt x_i, und f_i heißt der **Trägheitsindex** von π im Punkt x_i. $k(x_i) = R/\mathfrak{p}_i$ heißt der **Restklassenkörper** von$R$ im Punkt x_i. $k(x_i)$ ist endlicher Körper mit p^{f_i} Elementen.

Die Abbildung $\pi : \widetilde{C} \longrightarrow B$ ist über dem Punkt $x = \langle p \rangle \in B$ **verzweigt**, wenn es ein maximales Ideal $\mathfrak{p} \subset R$ gibt mit $pR \subset \mathfrak{p}$ und $\nu_{\mathfrak{p}}(p) \geq 2$, wobei $\nu_{\mathfrak{p}}(p)$ den Exponenten e von $\mathfrak{p}$ in der Primfaktorzerlegung von p in R bezeichnet.

Als konkretes Beispiel betrachten wir
$$K = \mathbb{Q}[\sqrt{d}],$$
wobei $d \in \mathbb{Z}$ eine quadratfreie ganze Zahl sei.

Dann gilt für die Diskriminante
$$D = \delta_K = \begin{cases} 4d & \text{falls } d \not\equiv 1 \bmod 4 \\ d & \text{falls } d \equiv 1 \bmod 4 \end{cases}$$

Es sei $\omega := \frac{D+\sqrt{D}}{2}$. Dann ist $(1, \omega)$ eine Ganzheitsbasis von O_K und deshalb ist
$$\det \begin{pmatrix} Tr1 & Tr\omega \\ Tr\omega & Tr\omega^2 \end{pmatrix} = \det \begin{pmatrix} 2 & D \\ D & \frac{D+D^2}{2} \end{pmatrix} = D$$
die Diskriminante von K.

Nur im Fall $d \not\equiv 1 \bmod 4$ ist die Diskriminante D durch 2 teilbar und in diesem Fall ist
$$R = \mathbb{Z} + \mathbb{Z}\omega = \mathbb{Z}[\sqrt{d}] = \mathbb{Z}[x]/(x^2 - d)\mathbb{Z}[x].$$
Ist $d \equiv 1 \bmod 4$, so ist $\mathbb{Z}[\sqrt{d}]$ nicht ganz abgeschlossen in K:
$$\mathbb{Z}[\sqrt{d}] \subsetneqq R = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right].$$

In jedem Fall gilt: Die Abbildung
$$\pi : \operatorname{Spec} R \longrightarrow \operatorname{Spec} \mathbb{Z}$$
ist genau über den Primteilern $p \in \mathbb{Z}$ von D verzweigt. Ist p ein Teiler von D, so ist
$$pR = \mathfrak{p}^2, \qquad \text{wobei } \mathfrak{p} = \langle p, 1 + \omega \rangle.$$

Ist p kein Teiler von D und $p \neq 2$, so gilt folgendes ‘Zerlegungsgesetz’

p ist **träge** in R, d.h. pR ist Primideal in $R \Longleftrightarrow$
$$\left(\frac{D}{p}\right) = -1.$$

p ist **zerlegt** in R, d.h. $pR = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ mit zwei verschiedenen Primidealen $\mathfrak{p}_1, \mathfrak{p}_2$ in $R \Longleftrightarrow$
$$\left(\frac{D}{p}\right) = 1.$$
Für Beweise dieser Aussagen und mehr zur algebraischen Zahlentheorie siehe etwa [5], [4], [2], [12].

Übungen 4.3.26

(1) Sei $d \in \mathbb{Z}$ quadratfrei und $d \equiv 2, 3 \bmod 4$. $K = \mathbb{Q}[\sqrt{d}]$. Beweise: $O_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Berechne die Diskriminante von O_K.

(2) In $\mathbb{Z}[\sqrt{-5}]$ betrachte man die Ideale
$$\mathfrak{p} = \langle 2, 1+\sqrt{-5}\rangle,\ \mathfrak{q} = \langle 3, 1+\sqrt{-5}\rangle,\ \mathfrak{r} = \langle 3, 1-\sqrt{-5}\rangle.$$
   (a) Beweise: $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ sind maximale Ideale.

   (b) Zeige: $\mathfrak{p}^2 = \langle 2\rangle,\ \mathfrak{q}\mathfrak{r} = \langle 3\rangle,\ \mathfrak{p}\mathfrak{q} = \langle 1+\sqrt{-5}\rangle,\ \mathfrak{p}\mathfrak{r} = \langle 1-\sqrt{-5}\rangle$.

(3) Sei α eine algebraische Zahl vom Grad n. f sei das Minimalpolynom von α und f' die Ableitung von f.

   (a) Beweise: $\Delta(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\alpha))$

   (b) Berechne $\Delta(1, \alpha, \alpha^2)$, falls $f = x^3 + a_1x + a_0$

(4) Sei K ein algebraischer Zahlkörper vom Grad n und O_K der Ring der ganzen Zahlen in K. Ist $\mathfrak{a} \subset O_K$ ein von Null verschiedenes Ideal, so wird die **Norm von $\mathfrak{a}$** definiert als die Anzahl der Elemente des Restklassenrings $O_K/\mathfrak{a}$.
$$N(\mathfrak{a}) = |O_K/\mathfrak{a}|.$$
Berechne $N(\mathfrak{a})$ für die Ideale aus Aufgabe 2.

(5) Beweise, daß die Ideale $\mathfrak{p}, \mathfrak{q}, \mathfrak{r}$ aus Aufgabe 2 keine Hauptideale sind.

(6) Die Voraussetzungen seien wie in Aufgabe 4. Es sei $\mathfrak{a} \subset O_K$ von Null verschiedenes Ideal.

   (a) Beweise: Es gibt eine Ganzheitsbasis $(\beta_1, \ldots, \beta_n)$ von O_K und Zahlen
$$d_1, \ldots, d_n \in \mathbb{N}_+ \ \text{ mit } \ d_1 | d_2 \ldots | d_n,$$
so daß $(d_1\beta_2, \ldots,\ d_n\beta_n)$ Ganzheitsbasis von $\mathfrak{a}$ ist (Stichwort: Gaußsches Eliminationsverfahren, Elementarteiler).

   (b) $N(\mathfrak{a}) = \sqrt{\dfrac{\Delta(\mathfrak{a})}{\Delta(O_K)}}$

(7) (Für ***Mathematica*** -Fans) Schreibe ein Programm

   (a) zur Diskriminante eines Ideals

(b) zur Multiplikation von Idealen in O_K

(c) zur Bestimmung einer Ganzheitsbasis eines gebrochenen Ideals in $K = \mathbb{Q}[\sqrt{d}]$.

(8) Es sei $d \in \mathbb{Z}$ keine Kubikzahl, quadratfrei, und es gelte $d \not\equiv \pm 1 \bmod 9$. Es sei $\vartheta = \sqrt[3]{d}$ und $K = \mathbb{Q}[\vartheta]$, $R = O_K$.

Beweise:

(a) $N_{K/\mathbb{Q}}(a + b\vartheta + c\vartheta^2) = a^3 + db^3 + d^2c^3 - 3dabc$

(b) $(1, \vartheta, \vartheta^2)$ ist eine Ganzheitsbasis von R.

(c) Sei p Primzahl, die $3d$ nicht teilt. Dann gilt: $\langle p \rangle = pR$ ist maximales Ideal in R, wenn die Kongruenz

$$x^3 \equiv d \bmod p$$

nicht lösbar ist.

4.4 Endliche Körper und die prime Restklassengruppe modulo m

Neben den endlichen Körpern $\mathbb{F}_p$ sind uns auch schon andere endliche Körper in der Gestalt von Restklassenkörpern $k = R/\mathfrak{p}$ maximaler Idealer $\mathfrak{p}$ in Zahlringen $R = O_K$ begegnet.

Zunächst wollen wir zeigen, daß die multiplikative $K^\times = K\backslash\{0\}$ eines endlichen Körpers K stets zyklisch ist.

Definition 4.4.1 Es sei G irgendeine multiplikativ geschriebene Gruppe mit neutralem Element e.
Für $g \in G$ heißt

$$\operatorname{ord}(g) := \min\{n \in \mathbb{N}_+ \mid g^n = e\}$$

die Ordnung von g. Dabei wird $\min \emptyset = \infty$ vereinbart.

$\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$ ist dann eine zyklische Untergruppe der Ordnung $\operatorname{ord}(g)$ von G. Ist G eine endliche Gruppe der Ordnung m, so ist $\operatorname{ord}(g)$ ein Teiler von m.

Satz 4.4.2 Es sei G eine Gruppe der Ordnung m. Für jeden Teiler d von m gebe es höchstens d Elemente $g \in G$ mit $g^d = e$. Dann ist G zyklisch.

Beweis: Es sei $f(d)$ die Anzahl der Elemente der Ordnung d in G. Da $\operatorname{ord}(g)$ ein Teiler von m ist, folgt

$$m = \sum_{d|m} f(d).$$

Es sei d Teiler von m mit $f(d) \neq 0$. Dann gibt es also ein Element g mit $\operatorname{ord}(g) = d$. $G' = \langle g\rangle \subset G$ ist zyklische Untergruppe der Ordnung d, und für alle $h \in G'$ gilt

$$h^d = e.$$

Also ist nach Voraussetzung

$$G' = \{x \in G \mid x^d = e\}$$

und natürlich folgt dann

$$M_d = \{x \in G \mid \operatorname{ord}(x) = d\} \subset G'.$$

Also ist

$$f(d) = \# M_d$$

die Anzahl der Erzeuger der zyklischen Gruppe $G' \cong (\mathbb{Z}/d\mathbb{Z}, +)$ und somit folgt

$$f(d) = \varphi(d),$$

wobei φ die Eulersche φ-Funktion ist. Es folgt

$$\sum_{d|m} \varphi(d) = m = \sum_{\substack{d|m \\ f(d)\neq 0}} f(d) = \sum_{\substack{d|m \\ f(d)\neq 0}} \varphi(d)$$

und somit $f(d) \neq 0$ für alle $d|m$. Insbesondere ist $f(m) \neq 0$. Es gibt also ein Element der Ordnung m in G. $\square$

Satz 4.4.3 Es sei K ein Körper und G eine endliche Untergruppe von $K^\times$. Dann ist G zyklisch.

Beweis: Da das Polynom $f = x^d - 1 \in K[x]$ höchstens d Nullstellen in K besitzt, gibt es auch höchstens d Elemente $g \in G$ mit $g^d = 1$. Die Voraussetzung in Satz 4.4.2 ist also erfüllt, und damit ist G zyklisch. $\square$

Korollar 4.4.4 Ist K ein endlicher Körper, so ist $K^\times$ zyklisch. $\square$

Korollar 4.4.5 Ist K ein Körper, so ist die Untergruppe $G = \{x \in K \mid x^d = 1\}$ von $K^\times$ zyklisch und ihre Ordnung ein Teiler von d.

Beweis: G ist endliche Untergruppe von $K^\times$, also zyklisch. Ist $x \in G$, so ist $\mathrm{ord}(x)$ ein Teiler von d. $\square$

Korollar 4.4.6 Sei p Primzahl. Dann gibt es ein $r \in \mathbb{N},\ r \not\equiv 0 \bmod p$, so daß

$$\mathbb{F}_p^\times = \{1 \bmod p,\ r \bmod p,\ r^2 \bmod p, \dots, r^{p-2} \bmod p\}.$$

$\square$

Definition 4.4.7 Sei $m \in \mathbb{N}_+$. $a \in \mathbb{Z}$ heißt **Primitivwurzel modulo** m (oder auch **primitiver Rest modulo** m): $\Longleftrightarrow$ $a \bmod m$ ist Erzeuger der Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$ der primen Reste modulo m.

Genau dann, wenn $(\mathbb{Z}/m\mathbb{Z})^\times$ zyklisch ist, gibt es eine Primitivwurzel modulo m. Da $\varphi(m)$ die Ordnung von $(\mathbb{Z}/m\mathbb{Z})^\times$ ist, gibt es dann $\varphi(\varphi(m))$ verschiedene (d.h. modulo m inkongruente) Primitivwurzeln von $(\mathbb{Z}/m\mathbb{Z})^\times$. Ist nämlich a Primitivwurzel modulo m und

$$n = \mathrm{ord}(a \bmod m) \text{ die Orndung von } a \bmod m$$

in der Gruppe $(\mathbb{Z}/m\mathbb{Z})^\times$, so gilt für $a \leq d \leq m$

$$\mathrm{ord}(a^d \bmod m) = \frac{n}{(n,d)},$$

also $\mathrm{ord}(a^d \bmod m) = n \Longleftrightarrow (n,d) = 1$.

Mit ***Mathematica*** kann man die Primitivwurzeln etwa folgendermaßen bestimmen:

```
ord[a_ Integer, m_ Integer /; m > 1] :=
    Module [{t, i = 1, d = GCD[a, m]},
    If [d = 1, t = Divisors [EulerPhi [m]];
        While [Mod[PowerMod [a, t[[i]], m], m] ≠ 1,
            i++]; t[[i]],
        Print["ggT = ", d, " ≠ 1"]]]
```

$\mathrm{ord}[a, m]$ ist die Ordnung von $a \bmod m$, falls $m \geq 2$ und $\mathrm{ggT}(a, m) = 1$.

Die primen Restklassen modulo m bekommt man durch

```
primerestklassen [m_ Integer /; m > 1] :=
        Select [Range [1, n], GCD[#, n]==1 & ]
```

Die Primitivwurzeln modulo m erhält man dann als die Teilmenge

```
primitivwurzeln [m_ Integer /; m > 1] :=
       Select [ primerestklassen[m], ord[#, n]=== Euler Phi[m]&]
```

Einige Beispiele:

primitivwurzeln [37] =
{ 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35 }
= { 2, 5, 13, 15, 17, 18, -18, -17, -15, -13, -5, -2 }

primitivwurzeln [17] =
= { 3, 5, 6, 7, -7, -6, -5, -3 }

primitivwurzeln [41] =
= { 6, 7, 11, 12, 13, 15, 17, 19, -19, -17, -15, -13, -12, -11, -7, -6 }

Gibt es eine Gesetzmäßigkeit für Primzahlen $p \equiv 1 \bmod 4$?

Satz 4.4.8 Sei p eine Primzahl, $p \neq 2$. Es sei $\alpha \in \mathbb{N}_+$. Dann gilt:

$$(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$$

ist zyklisch.
Genauer gilt:

(a) Ist a Primitivwurzel modulo p, so ist a oder $a + p$ Primitivwurzel modulo p^2.

(b) Ist a Primitivwurzel modulo p^2, so auch modulo p^α.

Beweis zu (a):
$(\mathbb{Z}/p^2\mathbb{Z})^\times$ hat die Ordnung $\varphi(p^2) = p(p-1)$.
$a \bmod p^2 \longmapsto a \bmod p$ ist ein surjektiver Gruppenhomomorphismus

$$q : (\mathbb{Z}/p^2\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$$

mit

$$\ker q = \{1 + \nu p) \bmod p^2 \mid \nu = 0, 1, \dots, p-1\}.$$

Für $a \in \mathbb{Z}$ erhält man die exakte Sequenz

$$1 \longrightarrow H \longrightarrow \langle a \bmod p^2 \rangle \longrightarrow \langle a \bmod p \rangle \longrightarrow 1,$$

wobei H eine Untergruppe von $\ker q$ ist, also (weil $\mathrm{ord}(\ker q) = p$ eine Primzahl ist) $\mathrm{ord}(H) = 1$ oder $\mathrm{ord}(H) = p$. Im ersten Fall ist

(1) $\mathrm{ord}(a \bmod p^2) = \mathrm{ord}(a \bmod p)$.

Im zweiten Fall ist dagegen

(2) $\operatorname{ord}(a \bmod p^2) = p \cdot \operatorname{ord}(a \bmod p)$

Es sei nun a Primitivwurzel modulo p, d.h. $\operatorname{ord}(a \bmod p) = p-1$.
Im zweiten Fall ist also $\operatorname{ord}(a \bmod p^2) = p(p-1)$, also a Primitivwurzel modulo p^2.
Im ersten Fall gilt dagegen

$$a^{p-1} \equiv 1 \bmod p^2$$

und somit $a^p \equiv \bmod p^2$, also auch $(a+p)^p \equiv a \bmod p^2$.
Es folgt

$$(a+p)^p \not\equiv a + p \bmod p^2$$

also erst recht

$$(a+p)^{p-1} \not\equiv 1 \bmod p^2.$$

Damit gilt $\operatorname{ord}((a+p) \bmod p^2) > p-1$.
Aus der exakten Sequenz

$$1 \longrightarrow H' \longrightarrow \langle (a+p) \bmod p^2 \rangle \longrightarrow \underset{\substack{\| \\ \mathbb{F}_p^\times}}{\langle a \bmod p \rangle} \longrightarrow 1$$

folgt: $\operatorname{ord}((a+p) \bmod p^2) = \operatorname{ord} H' \cdot (p-1)$, also $\operatorname{ord} H' > 1$. Als Untergruppe von $\ker q$ muß daher $\operatorname{ord} H' = p$, also $\operatorname{ord}((a+p) \bmod p^2) = p(p-1)$ gelten. □

Zu (b): Es sei $\alpha \geq 2$. Wir beweisen die Aussage durch Induktion nach α. Für $\alpha = 2$ ist nichts zu beweisen. Sei nun $\alpha \geq 3$ und die Behauptung für $\alpha - 1$ schon bewiesen.
Es gilt nur noch zu zeigen:
Ist a Primitivwurzel modulo $p^{\alpha-1}$, so auch modulo p^α.
Wir betrachten wieder die exakte Sequenz

$$\begin{array}{ccccccccc}
1 \longrightarrow & H & \longrightarrow & \langle a \bmod p^\alpha \rangle & \longrightarrow & \langle a \bmod p^{\alpha-1} \rangle & \longrightarrow & 1 \\
& \cap & & \cap & & \| & & \\
1 \longrightarrow & \ker q_\alpha & \longrightarrow & (\mathbb{Z}/p^\alpha\mathbb{Z})^\times & \underset{q_\alpha}{\longrightarrow} & (\mathbb{Z}/p^{\alpha-1}\mathbb{Z})^\times & \longrightarrow & 1
\end{array}$$

Da $\ker q_\alpha = \{1 + \nu p^{\alpha-1} \mid \nu = 0, 1, \ldots, p-1\}$ eine Gruppe der Ordnung p ist, und

$$\operatorname{ord}(a \bmod p^\alpha) = \operatorname{ord} H \cdot \operatorname{ord}(a \bmod p^{\alpha-1}),$$

ist nur zu zeigen, daß

$$\operatorname{ord}(a \bmod p^\alpha) > \operatorname{ord}(a \bmod p^{\alpha-1})$$

gilt.
Beweis: Da $\operatorname{ord}(a \bmod p^{\alpha-1}) = (p-1)p^{\alpha-2}$, ist

$$a^{(p-1)p^{\alpha-3}} \not\equiv 1 \bmod p^{\alpha-1}.$$

Da aber $a^{(p-1)p^{\alpha-2}} \equiv 1 \bmod p^{\alpha-2}$, folgt

$$a^{(p-1)p^{\alpha-3}} = 1 + bp^{\alpha-2} \text{ mit } b \not\equiv 0 \bmod p.$$

Es folgt

$$\begin{aligned} a^{(p-1)p^{\alpha-2}} &= (1+bp^{\alpha-2})^p = 1 + pbp^{\alpha-2} + \binom{p}{2} b^2 p^{2(\alpha-2)} + \cdots \\ &\equiv 1 + bp^{\alpha-1} \bmod p^\alpha \not\equiv 1 \bmod p^\alpha. \end{aligned}$$

Also ist $\operatorname{ord}(a \bmod p^\alpha) > (p-1)p^{\alpha-2} = \operatorname{ord}(a \bmod p^{\alpha-1})$. □

Wir behandeln die Potenzen von 2.

Satz 4.4.9

(a) $(\mathbb{Z}/2\mathbb{Z})^\times = \{1 \bmod 2\},\ (\mathbb{Z}/4\mathbb{Z})^\times = \{\pm 1 \bmod 4\}$ sind zyklisch.

(b) Für $\alpha \geq 3$ ist $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \{\pm 5^\nu \bmod 2^\alpha \mid \nu = 0, \ldots, 2^{\alpha-2}-1\}$ nicht zyklisch.

Beweis zu (b):

Behauptung: $\forall\ \alpha \geq 2 : \operatorname{ord}(5 \bmod 2^\alpha) = 2^{\alpha-2}$.

Beweis: Es genügt zu zeigen, daß

$$5^{2^{\alpha-2}} = 1 + b_\alpha 2^\alpha \text{ mit } b_\alpha \not\equiv 0 \bmod 2,\ \alpha \geq 2.$$

Für $\alpha = 2$ ist dies klar, weil

$$5^{2^0} = 5 = 1 + b_2 2^2 \text{ mit } b_2 = 1.$$

$\alpha - 1 \longrightarrow \alpha,\ \alpha \geq 3:$

$$\begin{aligned} 5^{2^{\alpha-2}} &= \left(5^{2^{\alpha-3}}\right)^2 = (1 + b_{\alpha-1}2^{\alpha-1})^2 = 1 + b_{\alpha-1}2^\alpha + b_{\alpha-1}^2 2^{2\alpha-2} \\ &= 1 + (b_{\alpha-1} + b_{\alpha-1}^2 2^{\alpha-2})2^\alpha = 1 + b_\alpha 2^\alpha \end{aligned}$$

mit $b_\alpha := b_{\alpha-1} + b_{\alpha-1}^2 2^{\alpha-2}) \equiv b_{\alpha-1} \bmod 2$, weil $\alpha \geq 3$.

$5 \bmod 2^\alpha$ erzeugt also eine Untergruppe U der Ordnung $2^{\alpha-2}$ von $G = (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$. Das einzige Element der Ordnung 2 in U ist $5^{2^{\alpha-3}} \bmod 2^\alpha$, und es gilt

$$5^{2^{\alpha-3}} = 1 + b_{\alpha-1}2^{\alpha-1} \equiv 1 + 2^{\alpha-1} \bmod 2^\alpha.$$

Da $1 + 2^{\alpha-2} \not\equiv 0 \bmod 2^{\alpha-1}$ ist

$$2 + 2^{\alpha-1} = 2(1 + 2^{\alpha-2}) \not\equiv 0 \bmod 2^\alpha$$

und somit

$$\begin{aligned} 1 + 2^{\alpha-1} &\not\equiv -1 \bmod 2^\alpha, \quad \text{d.h.} \\ 5^{2^{\alpha-3}} &\not\equiv -1 \bmod 2^\alpha. \end{aligned}$$

Die Restklasse $-1 \bmod 2^\alpha \in G$ liegt also nicht in der Untergruppe U.

Damit folgt durch Abzählen

$$\begin{aligned} G &= U \cdot \{\pm 1 \bmod 2^\alpha\} \cong U \times \{\pm 1\} \\ &= \{\pm 5^\nu \bmod 2^\alpha \mid \nu = 0, \ldots, 2^{\alpha-2} - 1\} \end{aligned}$$

ist isomorph zu dem Produkt einer zyklischen Gruppe der Ordnung $2^{\alpha-2}$ und einer zyklischen Gruppe der Ordnung 2, insbesondere also nicht zyklisch. □

Wir folgern

Satz 4.4.10 Es sei $m \in \mathbb{N},\ m > 1$.
$(\mathbb{Z}/m\mathbb{Z})^\times$ ist genau dann zyklisch, wenn $m = 2, 4, p^\alpha, 2p^\alpha$, wobei p ungerade Primzahl und $\alpha \geq 1$.

Beweis: „$\Longleftarrow$“ $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/2p^\alpha\mathbb{Z})^\times$ falls p ungerade Primzahl und $\alpha \geq 1$.
„$\Longrightarrow$“ Es sei $m \in \mathbb{N},\ m \geq 12$ und m nicht von der Form p^α oder $2p^\alpha,\ \alpha \geq 1,\ p$ Primzahl.
Wir müssen zeigen, daß $(\mathbb{Z}/m\mathbb{Z})^\times$ nicht zyklisch ist. Nach dem chinesischen Restsatz ist

$$(\mathbb{Z}/m\mathbb{Z})^\times = \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times$$

wobei $m = \prod\limits_{i=1}^{r} p_i^{\alpha_i}$ die Primfaktorzerlegung von m ist, $p_1 < \ldots < p_r,\ \alpha_i > 0$.
Ist $p_1 = 2$ und $r = 2$, so muß $\alpha_1 \geq 2$ sein. In jedem Fall findet man zwei Faktoren

$$U_1 = (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times,\ U_2 = (\mathbb{Z}/p_j^{\alpha_i}\mathbb{Z})^\times$$

mit gerader Ordnung $(\varphi(p^\alpha) = (p-1)p^{\alpha-1})$.
$U_1 \times U_2$ ist dann sicher nicht zyklisch, also auch $(\mathbb{Z}/m\mathbb{Z})^\times$ nicht. □

Definition 4.4.11 Es seien $m, n \in \mathbb{N}_+,\ n \geq 2,\ a \in \mathbb{Z}$ mit $(a, m) = 1$.
a heißt **n-ter Potenzrest modulo** m: $\Longleftrightarrow$
Die Kongruenz

$$x^n \equiv a \bmod m$$

ist in $\mathbb{Z}$ lösbar.

Lemma 4.4.12 Sei m so gewählt, daß $(Z/m\mathbb{Z})^\times$ zyklisch ist. Weiter sei $d = (n, \varphi(m))$ und $a \in \mathbb{Z}$ mit $(a, m) = 1$. Dann gilt: a ist n-ter Potenzrest modulo $m \Longleftrightarrow a^{\frac{\varphi(m)}{d}} \equiv 1 \bmod m$.
Die Kongruenz $x^n \equiv a \bmod m$ hat dann d Lösungen modulo m.

Beweis: Sei $g \in \mathbb{Z}$ Primitivwurzel modulo m.

(1) Sei $x \in \mathbb{Z}$ mit $x^n \equiv a \bmod m$. Sei $\mu \in \mathbb{N}$ mit $x \equiv g^\mu \bmod m$. Dann folgt $a \equiv g^{\mu n} \bmod m$, also

$$a^{\frac{\varphi(m)}{d}} = \left(g^{\mu\frac{n}{d}}\right)^{\varphi(m)} \equiv 1 \bmod m \quad \text{(nach Euler)}.$$

(2) Gelte $a^{\frac{\varphi(m)}{d}} \equiv 1 \bmod m$.

Wähle $\nu \in \mathbb{N}$ mit $a \equiv g^\nu \bmod m$. Dann gilt also

$$g^{\frac{\nu\varphi(m)}{d}} \equiv 1 \bmod m$$

und da $\operatorname{ord}(g \bmod m) = \varphi(m)$, muß $\varphi(m)$ ein Teiler von $\frac{\nu\varphi(m)}{d}$ sein, d.h. $\frac{\nu}{d} \in \mathbb{Z}$, also $\nu = \nu' d$ mit $\nu' \in \mathbb{Z}$.

Es gibt dann ein $\mu \in \mathbb{Z}$ mit

$$\mu n \equiv \nu \bmod \varphi(m),$$

weil $d = \mathrm{ggT}(n, \varphi(m))$ ein Teiler von ν ist.
Daraus ergibt sich nun für $x := g^\mu$

$$x^n = g^{\mu n} \equiv g^\nu \equiv a \bmod m.$$

Außerdem gilt

$$x^n \equiv a \bmod m$$

hat genau so viele Lösungen $x \bmod m$ wie die Kongruenz $\mu n \equiv \nu \bmod \varphi(m)$ Lösungen $\mu \bmod \varphi(m)$ besitzt. □

Wir kommen zu den endlichen Körpern. Ist K ein endlicher Körper und p die kleinste positive Zahl mit $p \cdot 1 = 0$ in K, so ist $\mathbb{F}_p \subset K$ Unterkörper, K also ein endlichdimensionaler $\mathbb{F}_p$-Vektorraum. Ist $n = \dim_{\mathbb{F}_p} K$, so hat daher K genau $q = p^n$ Elemente.

Satz 4.4.13 Es gibt einen Körper K mit $q = p^n$ Elementen, wobei p Primzahl und $n \in \mathbb{N}_+$.

Zunächst beweisen wir

Satz 4.4.14 Sei p Primzahl, $n \in \mathbb{N}_+$ und $q = p^n$.
Für $d \in \mathbb{N}_+$ sei $F_d \in \mathbb{F}_p[x]$ das Produkt aller normierten irreduziblen Polynome vom Grad d in $\mathbb{F}_p[x]$. Es gilt

$$x^q - x = \prod_{d|n} F_d(x).$$

Beweis:
1. Behauptung: Ist $f \in \mathbb{F}_p[x]$ ein Teiler von $x^q - x$, $\operatorname{grad} f > 0$, so ist f^2 kein Teiler von $x^q - x$.
Annahme: $x^q - x = f^2 \cdot h \Longrightarrow$ (Ableiten)

$$-1 = qx^{q-1} - 1 = 2ff'h + f^2h \Longrightarrow f|1 \Longrightarrow f = \text{ const., Widerspruch.}$$

2. Behauptung: Ist f irreduzibles Polynom vom Grad d in $\mathbb{F}_p[x]$ und gilt $f|x^q - x$, so gilt $d|n$.
Beweis: $K = \mathbb{F}_p[x]/f\mathbb{F}_p[x]$ ist Körper mit $\dim_{\mathbb{F}_p} K = d$. Ist α die Restklasse von x, so ist $(1, \alpha, \ldots, \alpha^{d-1})$ eine $\mathbb{F}_p$-Basis von K und $f(\alpha) = 0$.
Da K p^d Elemente hat, gilt

$$\beta^{p^d} = \beta \quad \text{für alle} \quad \beta \in K.$$

Es gilt auch $\beta^q = \beta \quad \forall\, \beta \in K$.
Dazu betrachte die Zerlegung

$$x^q - x = f \cdot g.$$

Es folgt

$$\alpha^q - \alpha = f(\alpha)g(\alpha) = 0$$

also

$$\alpha^q = \alpha.$$

Für $\beta = \sum_{\nu=0}^{d-1} a_\nu \alpha^\nu \in K,\ a_\nu \in F_p$ gilt dann, weil q eine Potenz von p ist:

$$\beta^q = \left(\sum_{\nu=0}^{d-1} a_\nu \alpha^\nu \right)^q = \sum_{\nu=0}^{d-1} a_\nu^q \alpha^{\nu q} = \sum_{\nu=0}^{d-1} a_\nu \alpha^\nu = \beta.$$

Also ist $x - \beta$ Teiler von $x^q - x$ für alle $\beta \in K$. Also ist auch

$$x^{p^d} - x = \prod_{\beta \in K} (x - \beta)$$

ein Teiler von $x^q - x$, und somit ist $x^{p^d - 1} - 1$ ein Teiler von $x^{q-1} - 1$.
Aus dem nachfolgenden Lemma 4.4.15 folgt dann (wegen $q = p^n$)

$$p^d - 1 \mid p^n - 1$$

und somit $d|n$. Damit ist die zweite Behauptung bewiesen.
3. Behauptung: Sei d Teiler von n und f normiertes Polynom vom Grad d in $\mathbb{F}_p[x]$. Dann ist f ein Teiler von $x^q - x$.
Beweis: Sei wieder $K = \mathbb{F}_p[x]/f\mathbb{F}_p[x]$ und $\alpha \in K$ die Restklasse von x modulo f.
Da K ein Körper der Ordnung p^d ist und $\alpha \neq 0$, ist α Nullstelle von

$$x^{p^d - 1} - 1.$$

Da d Teiler von n ist, ist $p^d - 1$ Teiler von $q - 1$ und somit ist

$$x^{p^d - 1} - 1 \quad \text{Teiler von} \quad x^{q-1} - 1$$

(wie Lemma 4.4.15 zeigt). Also ist α auch Nullstelle von $x^{q-1} - 1$. Da $f\mathbb{F}_p[x]$ der Kern der Auswertungsabbildung

$$\mathbb{F}_p[x] \longrightarrow K,\ x \longmapsto \alpha$$

ist, ist also f ein Teiler von $x^{q-1} - 1$. Aus 1., 2. und 3. folgt unmittelbar die Behauptung des Satzes. $\square$
Wir haben folgendes elementare Lemma benutzt.

Lemma 4.4.15 Es sei F ein Körper, $l, m \in \mathbb{N}$.

(a) $x^l - 1 \mid x^m - 1$ in $F[x] \iff l|m$

(b) Ist $a \in \mathbb{Z}$, $a \geq 2$, so gilt : $a^l - 1 \mid a^m - 1 \iff l|m$

Beweis zu (a):
Sei $m = sl + r$ mit $0 \leq r < l$. Dann gilt im Quotientenkörper $F(x)$ von $F[x]$:

$$\frac{x^m - 1}{x^l - 1} = x^r \; \frac{x^{sl} - 1}{x^l - 1} + \frac{x^r - 1}{x^l - 1};$$

es folgt

$$\frac{x^m - 1}{x^l - 1} \in F[x] \Longleftrightarrow \frac{x^r - 1}{x^l - 1} \in F[x] \Longleftrightarrow r = 0 \Longleftrightarrow l | m$$

Zu (b): Für $l = 1$ ist das trivial; sei also $l \geq 2$. Es gilt

$$\frac{a^m - 1}{a^l - 1} = a^r \; \underbrace{\frac{a^{sl} - 1}{a^l - 1}}_{\in \mathbb{Z}} + \frac{a^r - 1}{a^l - 1}$$

also:

$$\frac{a^m - 1}{a^l - 1} \in |Z \Longleftrightarrow + \frac{a^r - 1}{a^l - 1} \in \mathbb{Z} \Longleftrightarrow r = 0,$$

weil $1 \leq a^r - 1 < a^l - 1$, falls $r > 0$. □

Korollar 4.4.16 Es sei $d \geq 1$ und N_d die Anzahl der normierten irreduziblen Polynome vom Grad d in $\mathbb{F}_p[x]$. Dann gilt

$$p^n = \sum_{d|n} d \cdot N_d$$

$$N_n = \frac{1}{n} \sum_{d|n} \mu \left(\frac{n}{d} \right) p^d.$$

Beweis: Aus Satz 4.4.14 folgt mit $q = p^n$

$$p^n = \text{grad}(x^q - x) = \sum_{d|n} \text{grad}\, F_d(x) = \sum_{d|n} dN_d.$$

Die Möbiussche Umkehrformel liefert

$$nN_n = \sum_{d|n} \mu \left(\frac{n}{d} \right) p^d.$$

□

Korollar 4.4.17 Zu jeder natürlichen Zahl $n \in \mathbb{N}_+$ gibt es ein irreduzibles Polynom $f \in \mathbb{F}_p[x]$ vom Grad n.

Beweis:

$$\sum_{d|n} \mu \left(\frac{n}{d} \right) p^d \neq 0,$$

weil $\mu(\frac{n}{d}) \in \{-1, 0, 1\}$ und $\mu(\frac{n}{d}) \neq 0$ für wenigstens einen Teiler d von n. Nach Korollar 4.4.16 ist somit $N_n \neq 0$. □

Jetzt folgt auch Satz 4.4.13:
Man wähle ein normiertes irreduzibles Polynom $f \in \mathbb{F}_p[x]$ vom Grad n.

$$K = \mathbb{F}_p[x]/f\mathbb{F}_p[x]$$

ist dann ein Körper mit p^n Elementen. □
Es gilt sogar folgender Eindeutigkeitssatz

Satz 4.4.18 Seien K, K' zwei Körper mit q Elementen. Dann gibt es einen Isomorphismus $\varphi : K \longrightarrow K'$.

Beweis: $K^\times$ ist zyklisch. Sei $\alpha \in K^\times$ eine Primitivwurzel. Es gilt dann insbesondere $K = \mathbb{F}_p[\alpha]$, wobei $\mathbb{F}_p \subset K$ der Unterkörper $\{a1_K \mid a \in \mathbb{Z}\}$ ist, p ist die Charakteristik von K und $q = p^n$, wobei $n = \dim_{\mathbb{F}_p} K$.
Es sei $f \in \mathbb{F}_p[x]$ das Minimalpolynom von α, (normiert, irreduzibel mit $f(\alpha) = 0$). Nach dem dritten Beweisschritt im Beweis zu 4.4.14 teilt f das Polynom $x^q - x$. Weiter gilt für alle $\beta \in K'$, da K' q Elemente hat,

$$\beta^q = \beta,$$

d.h.

$$x^q - x = \prod_{\beta \in K'} (x - \beta) \text{ in } K'[x].$$

Insbesondere besitzt der Faktor f von $x^q - x$ in $K'[x]$ eine Zerlegung

$$f = \prod_{i=1}^{n} (x - \beta_i)$$

mit $\beta_1, \ldots, \beta_n \in K'$. Insbesondere ist $f(\beta_1) = 0$ und $x \longmapsto \beta_1$ induziert einen Homomorphismus

$$L := \mathbb{F}_p[x]/\langle f \rangle \longrightarrow \mathbb{F}_p[\beta_1] \subset K'.$$

Aus Anzahlgründen muß $L \longrightarrow K'$ bijektiv sein. Da auch $L \cong \mathbb{F}_p[\alpha] = K$ nach Wahl von f, folgt $K \cong K'$. □
Notation: 'Der' endliche Körper mit q Elementen wird mit $\mathbb{F}_q$ bezeichnet.

Beispiel 4.4.19

(1) $\mathbb{F}_4 = \mathbb{F}_2[x]/\langle x^2 + x + 1 \rangle$

Hier ist $q = 4 = p^n$ mit $n = 2$, $p = 2$. Die Zerlegung von $x^4 - x$ nach Satz 4.4.14 ist

$$x^4 - x = F_1(x)F_2(x),$$

wobei $F_1(x) = x \cdot (x + 1)$, denn x und $x + 1$ sind die normierten irreduziblen Polynome in $\mathbb{F}_2[x]$ vom Grad 2.

$$F_2(x) = x^2 + x + 1$$

ist das einzige irreduzible Polynom vom Grad 2 in $\mathbb{F}_p[x]$.

Elemente in $\mathbb{F}_4$ sind $0,\ 1,\ \alpha,\ 1 + \alpha$ wobei $\alpha = x \bmod (x^2 + x + 1)$
α und $1 + \alpha$ sind Primitivwurzeln von $\mathbb{F}_4^\times$

$$1 = \alpha^0,\ \alpha = \alpha^1,\ \alpha^2 = \alpha + 1$$

(2) $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle x^3+x+1\rangle$

Hier ist $x^8 - x = x(x+1)(x^3+x^2+1)(x^3+x+1)$, denn x^3+x^2+1 und x^3+x+1 sind irreduzibel in $\mathbb{F}_2[x]$.

Sei $\alpha = x \bmod (x^3+x+1)$. Dann ist

$$\mathbb{F}_8 = \{0,\ 1,\ \alpha,\ 1+\alpha,\ \alpha^2,\ 1+\alpha^2,\ \alpha+\alpha^2,\ 1+\alpha+\alpha^2\}$$

und $\mathbb{F}_8^\times$ ist zyklisch mit jedem von 0 und 1 verschiedenen Element als Primitivwurzel, etwa α:

$$\begin{aligned}&\alpha^0 = 1,\ \alpha^1 = \alpha,\ \alpha^2,\ \alpha^3 = 1+\alpha,\ \alpha^4 = \alpha+\alpha^2,\\ &\alpha^5 = \alpha^2+\alpha^3 = 1+\alpha+\alpha^2,\ \alpha^6 = 1+\alpha^2,\ \alpha^7 = \alpha+\alpha^3 = 1.\end{aligned}$$

(3)

$$\begin{aligned}\mathbb{F}_9 &= \mathbb{F}_3[x]/\langle x^2+1\rangle\\ &= \{0,\ 1,\ 2,\ \alpha,\ 1+\alpha,\ 2+\alpha,\ 2\alpha,\ 1+2\alpha,\ 2+2\alpha\}.\end{aligned}$$

$\mathbb{F}_9^\times$ wird von $1+\alpha$ erzeugt:

$$\begin{aligned}(1+\alpha)^2 &= 2\alpha\\ (1+\alpha)^3 &= 1+2\alpha\\ (1+\alpha)^4 &= 2\\ (1+\alpha)^5 &= 2+2\alpha\\ (1+\alpha)^6 &= \alpha\\ (1+\alpha)^7 &= 2+\alpha\\ (1+\alpha)^8 &= 1\end{aligned}$$

Übungen 4.4.20

(1) (a) Beweise: 2 ist Primitivwurzel modulo 29.

(b) Löse die Kongruenz $x^7 \equiv 1 \bmod 29$.

(2) Sei p Primzahl

(a) Sei $p \equiv 3 \bmod 4,\ a \in \mathbb{Z},\ a \not\equiv 0 \bmod p$. Beweise:

$$x^4 \equiv a \bmod p \text{ ist lösbar } \iff \left(\frac{a}{p}\right) = 1.$$

(b) Löse $x^4 \equiv 3 \bmod 11$

(c) $x^4 \equiv -1 \bmod p$ ist lösbar $\iff p \equiv 1 \bmod 8$

(3) Sei p eine ungerade Primzahl und $g \in \mathbb{Z},\ g \not\equiv 0 \bmod p$.

(a) Für $\alpha \in \mathbb{N}_+$ gilt

$$\operatorname{ord}(g \bmod p^\alpha) = \operatorname{ord}(g \bmod p) \cdot p^\beta,$$

wobei $\beta = \max(0, \alpha - v_p(g^{p-1}-1))$.

(b) g ist Primitivwurzel modulo p^α für $\alpha \geq 2 \iff g$ ist Primitivwurzel modulo p und
$$g^{p-1} \not\equiv 1 \bmod p^2.$$

(4) Sei p eine Primzahl und d ein Teiler von $p-1$. Beweise: Die d-ten Potenzreste modulo p bilden eine Untergruppe der Ordnung $\frac{p-1}{d}$ von $\mathbb{F}_p^\times$. Berechne diese Gruppe für
$$(p,d) = (11,5),\ (17,4),\ (19,6).$$

(5) (a) Bestimme die Anzahl der normierten irreduziblen Polynome vom Grad 3 in $\mathbb{F}_p[x]$.

(b) Bestimme die irreduziblen Polynome vom Grad 3 in $\mathbb{F}_3[x]$.

(c) Zerlege $x^{27} - x$ in $\mathbb{F}_3[x]$ in irreduzible Faktoren.

(6) Sei p eine Primzahl und $k \in \mathbb{N}_+$. Beweise
$$1^k + 2^k + \cdots + (p-1)^k \equiv \begin{cases} 0 \bmod p, & \text{falls } k \not\equiv 0 \bmod (p-1) \\ -1 \bmod p, & \text{falls } k \equiv 0 \bmod (p-1) \end{cases}$$

(7) Es sei $K = \mathbb{F}_q$ der Körper mit q Elementen. $\alpha \in \mathbb{F}_q^\times$ sei ein Erzeuger der Gruppe $F_q^\times$. Für jeden Teiler d von $q-1$ sei
$$F_d = \prod_{\substack{k=0 \\ (k,q-1)=\frac{q-1}{d}}}^{q-1} (x - \alpha^k) \in K[x].$$

Zeige:

(a) $\operatorname{grad} F_d = \varphi(d)$

(b) $x^{q-1} - 1 = \prod_{d \mid q-1} F_d$

(c) $F_{q-1} = \prod_{d \mid q-1} (x^{\frac{q-1}{d}} - 1)^{\mu(d)}$

(8) (Für ***Mathematica*** -Fans) Schreibe ein Programm

(a) zur Arithmetik im Körper $\mathbb{F}_q (q = p^n)$

(b) zur Polynomdivision in $\mathbb{F}_q[x]$

(c) zur Bestimmung von quadratfreien Polynomen $f_d \in \mathbb{F}_q[x]$ zu gegebnem $f \in \mathbb{F}_q[x]$, so daß
$$f = \prod_{d=1}^{n} (f_d)^d$$
(vgl. [6] S. 46)

(d) zur Zerlegung
$$f = f_1 \cdot \ldots \cdot f_n$$
eines quadratfreien normierten Polynoms $f \in \mathbb{F}_q[x]$ in das Produkt von Polynomen $f_d \in \mathbb{F}_q[x]$, wobei f_d das Produkt aller irreduziblen normierten Polynome vom Grad d ist, die f teilen (vgl. Satz 4.4.14).

Literaturverzeichnis

[1] Artin, M.: Algebra, Birkhäuser Basel 1993

[2] Borewicz, S. I./Safarevic, I. R.: Zahlentheorie, Birkhäuser 1966

[3] Burn, R. P.: A pathway into number theory, Cambridge Univ. Press 1982

[4] Cohen, H: A course in computational algebraic number theory, GTM 138, Springer 1993

[5] Cohn, H.: A classical invitation to algebraic numbers and class fields, Springer 1978

[6] Cox, Little, O'Shea: Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra, Springer 1992

[7] Forster, O.: Analysis 1, Vieweg Studium, Grundkurs Mathematik

[8] Ireland, K. F./Rosen, M. I.: A Classical Introduction to Modern Number Theory, GTM 84, Springer 1982

[9] Koblitz, N.: A Course in Number Theory and Cryptography, Springer 1987

[10] Koblitz, N.: p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer GTM Vol. 58, Corr. 2nd printing 1996

[11] Maeder, R.E.: Informatik für Mathematiker und Naturwissenschaftler, Addison-Wesley 1993

[12] Neukirch, J.: Algebraische Zahlentheorie, Springer 1992

[13] Niven, I./Zuckerman, H. S.: Einführung in die Zahlentheorie, Mannheim, B.I. 1976

[14] Reid, M.: Undergraduate Algebraic Geometry, Cambridge Univ. Press 1990

[15] Ribenboim, P.: The New Book of Prime Number Records, Springer 1995

[16] Rose, H. E.: A Course in Number Theory , second edition, OUP 1994

[17] Rosen, K. H.: Elementary Number Theory and its Applications, Reading, Mass. Addison-Wesley 1984

[18] Scholz, A./Schoeneberg, B.: Einführung in die Zahlentheorie, Berlin, de Gruyter 1973

[19] Serre, J.-P.: A Course in Arithmetic, Springer GTM Vol. 7, Corr. 5th printing 1996

[20] Storch, U.: Zahlentheorie, OSM Vorlesungsskripten 21, 1980

[21] Weil, A.: Zahlentheorie, Ein Gang durch die Geschichte von Hammurapi bis Legendre, Birkhäuser 1992

[22] Weil, A.: Number Theory for Beginners, Springer 1979

[23] Wolfram, S.: The Mathematica book, Mathematica version 3, 3. ed.,Champaign, Ill. Wolfram Media 1996

Index