Elliptic Curves

Notes for the 2004-5 Part III course

28/01/2005 – 16/03/2005

Contents

Lecture 1

Definitions and Weierstrass equations

David Loeffler
28 / 01 / 2005

1.0 Motivation *(non-examinable)*

What is an elliptic curve? As we shall see in the next section, when we give formal definitions, an elliptic curve is more or less the same thing as an algebraic curve of genus 1.

Why is the genus important? It turns out that the genus of a curve determines its properties to a remarkable extent – in particular, by the trichotomy $g = 0$, $g = 1$ or $g \geq 2$.

Genus 0

Over an algebraically closed field k, all genus 0 curves are isomorphic to the projective line $\mathbb{P}^1_k$. So they are parametrised by rational functions. Over a non-algebraically-closed field this is not quite true, but similar strong results hold. For example, curves of genus 0 over $\mathbb{Q}$ can always be embedded into $\mathbb{P}^1$ as conic sections; and if there is a single rational point on the curve, then by considering lines through this point we can give a rational parametrisation. The question of whether there are any rational points at all is solved by the Hasse-Minkowski theorem, which states that a quadratic form (in any number of variables) has rational solutions if and only if it has solutions over $\mathbb{R}$ and all of the p-adic fields $\mathbb{Q}_p$.

Genus 1

The genus 1 curves are, therefore, in some sense the simplest nontrivial algebraic curves; and they have a very rich structure about which much is known and still more remains to be found. For example, a genus 1 curve over $\mathbb{Q}$ can have no rational points, finitely many, or infinitely many; but if there are any (so the curve

is elliptic), the rational points form an abelian group, and this is always finitely generated (the Mordell-Weil theorem). It is an open problem whether the rank of this group can be arbitrarily large; but there are algorithms to determine it for a given curve. As for the torsion subgroup, it was recently shown by Mazur that there can never be more than 16 rational points of finite order, and there exists a simple algorithm to find them all.

Genus 2 and higher

The curves of genus ≥ 2 are much more difficult to work with, and the theory is much less complete. One result that illustrates the difference between this case and the genus 1 case is Faltings' theorem, which states that for curves defined over $\mathbb{Q}$, the set of rational points is finite; but no practical algorithm is yet known for finding them.

1.1 Definitions: Elliptic curves and the generalised Weierstrass equation

The results of this section properly belong to algebraic geometry, so we will not prove them here. Proofs may be found in Wilson's IIB Algebraic Curves notes, or in Silverman's book. Hereafter k represents some field (which is not necessarily algebraically closed and may have positive characteristic).

Definition 1.1. *An **elliptic curve** over k is a nonsingular projective algebraic curve E of genus 1 over k with a chosen base point $\mathcal{O} \in E$.*

Remark. There is a somewhat subtle point here concerning what is meant by a point of a curve over a non-algebraically-closed field. This arises because in algebraic geometry, it is common to identify points of a variety with maximal ideals in its k-algebra of regular functions; but if $k \neq \bar{k}$, this algebra has some maximal ideals which do not correspond to points of the original curve, but to Galois orbits of points satisfying the equations of the curve but with coordinates in extension fields L/k. In certain cases, such as the second example below, every maximal ideal is of this type. However, we don't want to allow $\mathcal{O}$ to be such a point; it's got to be a proper point defined over the base field k. I attempted to sidestep this issue in the lectures by using the phrase "k-rational point", but it seems this only resulted in more confusion. I hope this remark goes some way towards explaining this.

Examples:

1. The curve in $\mathbb{P}^2_{\mathbb{Q}}$ defined by the homogenous cubic $Y^2Z = X^3 - XZ^2$ is a nonsingular curve of genus 1; taking $\mathcal{O} = (0 : 1 : 0)$ makes it into an elliptic curve.

2. The cubic $3X^3 + 4Y^3 + 5Z^3$ is a nonsingular projective curve of genus 1 over $\mathbb{Q}$, but it is not an elliptic curve, since it does not have a single rational point. In fact, it has points over $\mathbb{R}$ and all the $\mathbb{Q}_p$, but no rational points, and thus shows that the Hasse-Minkowski principle does not hold for elliptic curves.

(We will see why this is when we encounter the Shafarevich-Tate group later in the course.)

We shall see later that every genus 1 curve can be embedded into $\mathbb{P}^2$ as a cubic. Since there are many plane cubics, we shall consider a particular class of cubic curves which will turn out to be sufficient:

Definition 1.2. *A **generalised Weierstrass equation** over k is an equation of the form*

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

where the coefficients $a_i \in k$.

Observe that such an equation defines a curve with a single point at infinity, $\mathcal{O} = (0 : 1 : 0)$. So it certainly has a rational point. It is easily seen that the curve is nonsingular at $\mathcal{O}$; but it may be singular elsewhere. Conversely, any cubic satisfying these conditions must be in Weierstrass form.

Definition 1.3. *For a Weierstrass equation as above, define the following quantities:*

$$b_2 = a_1^2 + 4a_2 \qquad b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$$
$$b_4 = 2a_4 + a_1a_3 \qquad \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$
$$b_6 = a_3^2 + 4a_6$$

*Then Δ is the **discriminant** of the generalised Weierstrass equation.*

Proposition 1.4. *The Weierstrass equation defines a nonsingular curve if and only if $\Delta \neq 0$.*

Proof. (sketch) This result is not difficult if the characteristic of k is not 2. We have checked that the unique point at infinity is nonsingular, so we work with the corresponding affine curve. The change of variables $y' = \frac{1}{2}(y - a_1x - a_3)$ reduces the equation to the simpler form $y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$, where the b_i's are as defined above. This is evidently nonsingular if and only if the cubic on the right has no repeated roots; but the discriminant of the cubic is 16Δ. □

(For a proof valid in characteristic 2, see Silverman, appendix A.)

Proposition 1.5. *Any elliptic curve E over k is isomorphic to the curve in $\mathbb{P}^2_k$ defined by some generalised Weierstrass equation, with the base point $\mathcal{O}$ of E being mapped to $(0 : 1 : 0)$. Conversely any non-singular generalised Weierstrass equation defines an elliptic curve, with this choice of basepoint.*

Proposition 1.6. *Two Weierstrass equations define isomorphic curves if and only if they are related by a change of variables of the form*

$$x' = u^2x + r$$
$$y' = u^3y + u^2sx + t$$

with $u, r, s, t \in k$, $u \neq 0$.

We shall assume from now on that all our elliptic curves are embedded in $\mathbb{P}^2_k$ via a generalised Weierstrass equation. We shall use the notation $E(k)$ for the set of points in $\mathbb{P}^2_k$ lying on the curve E. (That is, the set of k-rational points; see the remark following the definition, above.) Note that this will include the point $\mathcal{O}$ at infinity. Where L/k is a field extension, we define $E(L)$ in the obvious way, as the set of points in $\mathbb{P}^2_L$ lying on E.

I'll conclude with a lemma that will be needed in the next lecture. (Warning: this is stated in a rather misleading manner in Coates's 2003 notes.)

Proposition 1.7. *Let C be any cubic curve in $\mathbb{P}^2_k$. If k is algebraically closed, any line in $\mathbb{P}^1_k$ intersects C at precisely three points, counted with multiplicity. If k is not algebraically closed, then this need not be the case, but if a line intersects C at two points it must intersect it at a third.*

(This fact will be vital to the definition of the group law in the next lecture.)

Lecture 2

The Group Law on an Elliptic Curve

Tom Ward
31 / 01 / 2005

Definition of the Group Law

Let E be an elliptic curve over a field k. Last lecture we learned that we may embed E into $\mathbb{P}^2_k$ as a smooth plane cubic, given by the generalised Weierstrass equation ($\star$):

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

($a_i \in k$) with a unique point at infinity $\mathcal{O} = (0 : 1 : 0)$.

We also saw (at the end of the last lecture) that any line intersecting E at two points must also meet it at a third; in particular, if I have two points P, Q on E, I can draw a line through them, and I know this will intersect the curve at some third point.

I can also draw a tangent to E at a point P, and I know that it will meet E in precisely **one** other point (since the tangent at P intersects E at P with multiplicity 2.)

Keep this in mind as you consider the following proposition.

Proposition 2.1. *There exists a binary operation $\oplus$ on $E(k)$ such that:*
(i) $P \oplus Q = Q \oplus P$
(ii) $P \oplus \mathcal{O} = P$
(iii) If a line L meets E at points P, Q, R, then $(P \oplus Q) \oplus R = \mathcal{O}$
(iv) Given $P \in E(k)$, there exists $R \in E(k)$ such that $P \oplus R = \mathcal{O}$
(Then we write $R = \ominus P$)
(v) $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$
*Therefore, $(E(k), \oplus)$ is an **Abelian Group.***

The proof I will give of this proposition uses a powerful result from algebraic geometry (the Riemann-Roch Theorem for curves,) and we postpone it to the end of this section. You could provide a more elementary proof by working with the formulas for $P \oplus Q$ that we derive in the next section; but it would be hard work, and the algebraic geometric proof is more illuminating.

How To Add Points on the Curve

Given $P, Q \in E(k)$ explicitly, we naturally want to know if we can find a formula for the point $P \oplus Q$. This is easily done, and we'll see an example in a moment.

Firstly, we want to be able to invert points. For this we need to know when a line L meets E at the point $\mathcal{O}$ at infinity.

Lemma 2.2. *The lines in the plane that meet E at the point $\mathcal{O} = (0 : 1 : 0)$ at infinity, are precisely the lines $x = \xi$ (for $\xi \in$k.)*

Proof. Any line L in the plane is given by an equation:

$$L : \alpha x + \beta y + \gamma = 0$$

($\alpha, \beta, \gamma \in k$)
with α, β not both zero.

This line has projective equation

$$L : \alpha X + \beta Y + \gamma Z = 0$$

Therefore, $\mathcal{O}$ lies on $L \Leftrightarrow \beta = 0$

In this case, $\alpha \neq 0$ so dividing by α gives us an equation for L of the form $x = \xi$. □

Example: E: $y^2 + y = x^3 - x$ (an elliptic curve over $\mathbb{Q}$)

$P = (0, 0)$

$Q = (-1, -1)$

We want to find $P \oplus Q$.

The line going through P and Q is clearly $y = x$. This must meet E somewhere else. Put $y = x$ into the equation for E:

$$\begin{array}{rrcl} & x^2 + x & = & x^3 - x \\ \Rightarrow & x^3 - x^2 - 2x & = & 0 \\ \Rightarrow & x & = & 0 \text{ or } -1 \text{ or } 2. \end{array}$$

So the line meets E at $R = (2, 2)$ as well.

By the definition of $\oplus$, $P \oplus Q \oplus R = \mathcal{O}$.

So R = -($P \oplus Q$), and we want to invert R.

The line $x = 2$ meets E at R, and the lemma tells us it meets E at $\mathcal{O}$ too. It will also meet E at a third point, S say. Then $R \oplus S \oplus \mathcal{O} = \mathcal{O}$,

so $R \oplus S = \mathcal{O}$,

so $S = \ominus R = P \oplus Q$.

Put $x = 2$ into the equation for E: we get

$$\begin{array}{rrcl} & y^2 + y & = & 6 \\ \Rightarrow & y & = & 2 \text{ or } -3 \\ \Rightarrow & P \oplus Q & = & (2, -3) \end{array}$$

In this way we can come up with a general formula for adding two points:

Proposition 2.3.

If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ are points on E, where E has equation ($\star$) as before, the following formulae hold:

(i) $\ominus P = (x_1, -(a_1x_1 + a_3) - y_1)$
(ii) If $x_1 = x_2$ *but* $P_1 \neq P_2$*, then* $P_1 \oplus P_2 = \mathcal{O}$
(iii) If $x_1 \neq x_2$ *and* $P_1 \neq P_2$*, then the line through* P_1 *and* P_2 *is* $y = \lambda x + \nu$*, where:*

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

$$\nu = \frac{x_2y_1 - x_1y_2}{x_2 - x_1}$$

Also, if $P_1 = P_2$*, then the tangent to* E *at* P_1 *is* $y = \lambda x + \nu$*, where:*

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

$$\nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

Finally, if the line through P_1 *and* P_2 *(respectively the tangent at* $P_1 = P_2$*) is* $y = \lambda x + \nu$*, then* $P_1 \oplus P_2 = (x_3, y_3)$ *where:*

$$x_3 = \lambda^2 + a_1\lambda a - a_2 - x_1 - x_2$$

$$y_3 = (a_1 - \lambda)x_3 - \nu - a_3$$

Example:
$E : y^2 + y = x^3 - x$ again. Let $P = (0, 0)$
We find $2P = (1, 0)$, $3P = (-1, -1)$, $4P = (2, -3)$, $5P = (\frac{1}{4}, -\frac{5}{8})$, $6P = (6, 14)$ and $7P = (-\frac{5}{9}, \frac{8}{27})$.
In fact, P has infinite order in $E(\mathbb{Q})$.

Proof of the Formulae (boring bits left to the reader!):

(i) We use the lemma as we did in the earlier example: the line $x = x_1$ meets E at $P_1, \mathcal{O}, and \ominus P_1$, so put $x = x_1$ into the equation $(\star)$ for E and solve for the y co-ordinate of $\ominus P_1$.

(ii) If $x_1 = x_2$ but $P_1 \neq P_2$, then (by the lemma) P_1 and P_2 lie on a line through $\mathcal{O}$, so $P_1 = \ominus P_2$

(iii) For $P_1 \neq P_2$, solve the simultaneous equations $y_1 = \lambda x_1 + \nu$ and $y_2 = \lambda x_2 + \nu$.

For the tangent at P_1, differentiate equation $(\star)$ to find the gradient λ, then find ν.

For the co-ordinates of $P_1 \oplus P_2$, put $y = \lambda x + \nu$ into equation $(\star)$. Solving for x and y, we get the co-ordinates of the point $\ominus(P_1 \oplus P_2)$. Using formula (i) to invert it gives the final formula.

Results About the Group $E(k)$

Theorem 2.4. ***The Mordell-Weil Theorem***
Let E *be an elliptic curve over* $\mathbb{Q}$*. then* $E(\mathbb{Q})$ *is a finitely generated abelian group.*

Knowing this theorem, we may write $E(\mathbb{Q}) \cong T \times \mathbb{Z}^g$
where T is the torsion subgroup of $E(\mathbb{Q})$; and we define the **rank** of E to be g.

Examples:

(i) (rank$=0$) $E : y^2 + y = x^3 - x^2$, with $\Delta = -11$: $E(\mathbb{Q}) = \langle (0,0) \rangle \cong \frac{\mathbb{Z}}{5\mathbb{Z}}$

(ii) (rank$=1$) $E : y^2 + y = x^3 - x$, with $\Delta = 37$: $E(\mathbb{Q}) = \langle (0,0) \rangle \cong \mathbb{Z}$

(iii) (rank$=2$) $E : y^2 + y = x^3 - x^2 - 2x$, with $\Delta = 389$: $E(\mathbb{Q}) = \langle (0,0), (1,0) \rangle \cong \mathbb{Z}^2$

(iv) (rank$=3$) $E : y^2 + y = x^3 - 7x + 6$, with $\Delta = 5077$: $E(\mathbb{Q}) = \langle (0,2), (1,0), (2,0) \rangle \cong \mathbb{Z}^3$

Conjecture: There exist elliptic curves of arbitrarily high rank.

Points of Order 2

Lemma 2.5. *Let E be an elliptic curve over k, given by equation $(\star)$ as before. Let $P = (x_1, y_1) \in E(k)$*

Then P has order 2 in $E(k) \Leftrightarrow 2y_1 + a_1 x_1 + a_3 = 0$

Proof. P has order 2 $\Leftrightarrow$ the tangent at P meets $\mathcal{O}$
$\Leftrightarrow$ the tangent is of the form $x = \xi$
$\Leftrightarrow$ $(\frac{dy}{dx})_P = \infty$
$\Leftrightarrow$ $2y_1 + a_1 x_1 + a_3 = 0$ (using formula (iii)) .

□

Now, $(2y + a_1 x + a_3)^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6$ (the b_i are the same as in lecture 1)
so P has order 2 $\Leftrightarrow$ this cubic vanishes at P.

The cubic has discriminant 16Δ.

If char(k) $\neq$ 2 then the cubic has 3 distinct roots in $\overline{k}$ (the algebraic closure of k.)

Therefore there are **3 non-trivial points of order 2** in $E(\overline{k})$.

Let $E_2(\overline{k})$ be the subgroup of $E(\overline{k})$ generated by the points of order 2. Then the above result can be written:

$$E_2(\overline{k}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

If char(k)=2, then P has order 2 $\Leftrightarrow b_1 x_1^2 + b_6 = 0$

If $\mathbf{b_2 \neq 0}$ then we have one solution, and so

$$E_2(\overline{k}) \cong \frac{\mathbb{Z}}{2\mathbb{Z}}$$

If $\mathbf{b_2 = 0}$ then $b_6 \neq 0$ (because $b_6 = 0$ would imply $\Delta = 0$,)

therefore there are no non-trivial points of order 2 in $E(k)$

(Note: If $E(k)$ has a non-trivial point of order 2, it is said to be **ordinary**. If not, E is said to be **supersingular**.)

A Proof of the Group Law

This section assumes knowledge of some algebraic geometry, specifically the theory of divisors on curves and the Riemann-Roch theorem. Background for this would be provided, for example, by reading Prof Wilson's Algebraic Curves course notes from the web (and it is his notation that I use.) The address is http://www.dpmms.cam.ac.uk/~pmhw/.

Prof Wilson gives a proof of the group law on page 19 of these notes. I here present Dr Milne's proof from his internet notes. Essentially they use the same arguments, but in my opinion Milne's proof, while being less neat, is clearer.

The group law is "not an accident" in the sense that there is a subgroup of the divisor class group of E that naturally induces a group structure on $E(k)$, as we shall see.

A Proof of the Group Law Let V be a smooth, projective curve over a field k, and D a divisor on V. Define

$$\mathcal{L}(D) = \{f \in k(V) : (f) + D \geq 0\} \cup \{0\}$$

$$l(D) = \dim_k \mathcal{L}(D)$$

We let K_V denote the canonical divisor on V, and g the genus of V.

Theorem 2.6. ***Riemann-Roch***

$$l(D) = 1 - g + \deg(D) + l(K_V - D)$$

Now let E be a smooth, projective curve of genus 1, and fix a point $\mathcal{O}$ on E (so E is an elliptic curve.)

Riemann-Roch with $D = K_E$ tells us $\deg(K_E) = 2g - 2 = 0$.

So, if D is a divisor on E with $\deg(D) > 0$ then $\deg(K_E - D) < 0$ and therefore $l(K_E - D) = 0$.

Therefore, if $\deg(D) > 0$, Riemann-Roch tells us:

$$l(D) = \deg(D)$$

From now on, we let D be a divisor of degree 0. Then $\deg(D+\mathcal{O}) = 1$ so $l(D+\mathcal{O}) = 1$ (by the above remarks.)

Therefore we have $f \in k(E)$, **unique** up to multiplication by a constant, such that $(f) + D + \mathcal{O} \geq 0$.

But $\deg((f) + D + \mathcal{O}) = 1$ so this divisor must be a point P. Hence, there exists a **unique** point $P \in E$ such that

$$(f) + D + \mathcal{O} = P$$

$$\Rightarrow D \sim P - \mathcal{O}$$

(where $\sim$ denotes linear equivalence of divisors.)

Therefore, if we define

$$Cl^0(E) = \frac{\{\text{Divisors of degree 0 on } E\}}{\sim}$$

we have shown there exists a bijection

$$E(k) \to Cl^0(E)$$

$$P \mapsto P - \mathcal{O}$$

Since $Cl^0(E)$ is an abelian group, $E(k)$ inherits an abelian group structure from it via this bijection.

Claim: This group structure agrees with the operation $\oplus$

Proof. It is sufficient to show that if $P \oplus Q = R$ then $(P - \mathcal{O}) + (Q - \mathcal{O}) \sim (R - \mathcal{O})$

$P \oplus Q = R$ means we have a line L_1 meeting E at P, Q and S, and a line L_2 meeting E at S, R, and $\mathcal{O}$ (for some point S.)

The lines L_i can be regarded as linear forms, that is, homogeneous polynomials of degree one. Set $h = \frac{L_1}{L_2} \in k(E)$. h has zeroes at the zeroes of L_1, and poles at the zeroes of L_2. Therefore we can write down the principal divisor of h on E:

$$\begin{array}{rrcl} & (h) & = & P + Q + S - S - \mathcal{O} - R \\ \Rightarrow & 0 & \sim & P + Q - \mathcal{O} - R \\ \Rightarrow & R - \mathcal{O} & \sim & (P - \mathcal{O}) + (Q - \mathcal{O}) \end{array}$$

so we are done. □

Lecture 3

Elliptic Curves over $\mathbb{C}$

David Geraghty
02 / 02 / 2005

The contents of this lecture are not strictly part of the course but it would be a shame to complete the course without briefly describing the very rich theory of elliptic curves over $\mathbb{C}$. Due to time constraints I have not been able to provide many proofs but they can all be found in chapter VI of Silverman.

3.1 An elliptic curve over $\mathbb{C}$ is a Riemann surface

Let E be an elliptic curve over $\mathbb{C}$. Since the characteristic of $\mathbb{C}$ is not equal to 2 or 3, we can assume that E has a generalised Weierstrass equation of the form

$$y^2 = x(x-1)(x-\lambda)$$

where $\lambda \neq 0, 1$ (since E is nonsingular). We can regard $E \subset \mathbb{P}^2(\mathbb{C})$ as the Riemann surface of the function

$$f(z) = \sqrt{z(z-1)(z-\lambda)}.$$

What does this surface look like topologically? Since f is double valued, we take two copies of $\mathbb{P}^1(\mathbb{C})$ with appropriate branch cuts (which give single valued branches of f). Then we glue along the branch cuts to get the Riemann surface. Note that if we make branch cuts along the lines from 1 to λ and from 0 to ∞ then we can define a single valued holomorphic branch of f. Fattening out the cuts gives a sphere with two discs removed. Glueing two such punctured spheres together along the boundaries of the discs gives a torus. *Editor's note: This was accompanied by a diagram in the original version, which James Cranch has kindly xfigged, but I can't seem to get it to successfully import.)*

Notes:

1. Any elliptic curve over $\mathbb{C}$ is topologically equivalent to a torus. However different elliptic curves will in general be non isomorphic as Riemann surfaces.
2. In the last lecture we saw that the addition on E is given by everywhere locally defined rational functions. This endows E with the structure of a

1-dimensional complex Lie group i.e. E is both a Riemann surface and a group, and the group operations are given by holomorphic maps of Riemann surfaces.

3.2 Another way to construct a torus

Let $\Lambda \subset \mathbb{C}$ be a **lattice**, that is, a discrete additive subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$ basis for $\mathbb{C}$. Equivalently, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ for some $\omega_1, \omega_2 \in \mathbb{C}$ which are linearly independent over $\mathbb{R}$. Then the quotient space $\mathbb{C}/\Lambda$ is a Riemann surface which topologically is just a torus.

Notes:

1. If $\Lambda_1, \Lambda_2 \subset \mathbb{C}$ are lattices, then $\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2$ are homeomorphic but not necessarily isomorphic as Riemann surfaces.
2. By definition, $\Lambda \subset \mathbb{C}$ is an additive subgroup, so ordinary addition on $\mathbb{C}$ descends to give a 'group law' on $\mathbb{C}/\Lambda$. The group operations are obviously given by holomorphic functions and therefore $\mathbb{C}/\Lambda$ is a 1-dimensional complex Lie group.

3.3 Main result

Our main result for today will be the following:

Theorem 3.1. *Let E be an elliptic curve over $\mathbb{C}$. Then E is isomorphic as a complex Lie group to $\mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$. Conversely, given any lattice $\Lambda \subset \mathbb{C}$, there exists an elliptic curve E over $\mathbb{C}$ such that $\mathbb{C}/\Lambda$ and E are isomorphic as complex Lie groups.*

Assuming this for the moment we can prove the following proposition, which has consequences for elliptic curves over $\mathbb{Q}$:

Proposition 3.2. *Let E be an elliptic curve over $\mathbb{C}$ and let $m \geq 1$ be an integer. Then*

1. *As abstract groups*

$$\begin{aligned} E_m(\mathbb{C}) &:= \{P \in E(\mathbb{C}) \mid mP = \mathcal{O}\} \\ &= \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \end{aligned}$$

2. *The multiplication-by-m map*

$$\begin{aligned} [m] : E &\longrightarrow E \\ P &\longmapsto mP \end{aligned}$$

has degree m^2.

Proof. 1. We know that $E_m(\mathbb{C})$ isomorphic to $\mathbb{C}/\Lambda$, for some lattice $\Lambda \subset \mathbb{C}$. Hence

$$E_m(\mathbb{C}) \simeq (\mathbb{C}/\Lambda)_m \simeq (\frac{1}{m}\Lambda/\Lambda) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

2. By the Riemann-Hurwitz formula we have

$$2g(E) - 2 = \deg[m](2g(E) - 2) + R$$

where R denotes the ramification and g denotes the genus. Since the genus $g(E)$ equals 1 we get that $R = 0$, that is, $[m]$ is unramified. Therefore the degree of $[m]$ is equal to the number of points in the inverse image of $\mathcal{O}$. This is just m^2 by part 1.

□

Remark. If E is an elliptic curve over $\mathbb{Q}$, then $E(\mathbb{Q})$ is a sub*group* of $E(\mathbb{C})$. To see this, observe that the formula for addition on an elliptic curve is given by rational functions with coefficients in $\mathbb{Q}$. Hence

$$E_m(\mathbb{Q}) \leq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

as abstract groups. This agrees with what we found in the $m = 2$ case in the last lecture.

3.4 To go from $\mathbb{C}/\Lambda$ to a corresponding elliptic curve $E/\mathbb{C}$

We now turn our attention to theorem 3.1. To begin with, we sketch the proof of the second statement in the proposition.

Let $\Lambda \subset \mathbb{C}$ be a fixed lattice. We make the following definitions:

Definition 3.3. *An **elliptic function** (relative to Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ such that*

$$f(z + w) = f(z) \quad \forall z \in \mathbb{C}, w \in \Lambda$$

Definition 3.4. *The **Weierstrass $\wp$-function** (relative to Λ) is defined by the series*

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

The Weierstrass $\wp$-function will allow us to construct an elliptic curve which is isomorphic to $\mathbb{C}/\Lambda$. First we need the following result which is stated without proof:

Proposition 3.5. *The series defining $\wp(z)$ converges absolutely and uniformly on compact subsets of $\mathbb{C} - \Lambda$. It defines a meromorphic function on $\mathbb{C}$ having a double pole with residue 0 at each lattice point and no other poles. Furthermore, $\wp(z)$ is an even elliptic function.*

By expanding $(z - w)^{-2} - w^{-2}$ about $z = 0$ we see that the Laurent series for $\wp(z)$ about $z = 0$ is

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k}$$

where

$$G_{2k} = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{w^{2k}}.$$

Therefore we see that

$$\begin{aligned}\wp(z) &= \frac{1}{z^2} + 3G_4 z^2 + \text{h.o.t.} \\ \wp(z)^3 &= \frac{1}{z^6} + 9G_4\frac{1}{z^2} + 15G_6 + \text{h.o.t.} \\ \wp'(z)^2 &= \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 + \text{h.o.t.}\end{aligned}$$

where h.o.t. means 'higher order terms'. By taking a suitable linear combination of these functions we can remove the negative part, and indeed the constant term, of the Laurent series. The appropriate linear combination is

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6.$$

Observe that $f(z)$ is elliptic, holomorphic on $\mathbb{C} - \Lambda$ (since $\wp(z)$ is), holomorphic and vanishing at 0 (by construction) and thus holomorphic on all of $\mathbb{C}$ (by Λ-periodicity). Let ω_1, ω_2 be a $\mathbb{Z}$ basis for Λ and let D be the *fundamental parallelogram*

$$D = \{r_1\omega_1 + r_2\omega_2 \mid 0 \leq r_1, r_2 < 1\}.$$

Then D contains exactly one coset representative for each element of $\mathbb{C}/\Lambda$. Therefore, since $f(z)$ is elliptic, we have

$$f(\mathbb{C}) = f(D) = f(\overline{D}).$$

But $\overline{D}$ is compact and f is continuous so f is bounded. So by Liouville's theorem, and the fact that f vanishes at $z = 0$, we have that $f(z) = 0$ for all z i.e. we have an algebraic relation between $\wp$ and $\wp'$:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$$

where $g_2 = 60G_4$ and $g_3 = 140G_6$. We are now in a position to state the result which gives us the second part of theorem 3.1:

Proposition 3.6. *Using the above notation:*

1. *The polynomial $4x^3 - g_2x - g_3$ has distinct roots.*
2. *Let E be the elliptic curve over $\mathbb{C}$ given by the equation*

$$y^2 = 4x^3 - g_2x - g_3.$$

Then the map

$$\begin{aligned}\phi : \mathbb{C}/\Lambda &\longrightarrow E \subset \mathbb{P}^2(\mathbb{C}) \\ z &\longmapsto [\wp(z) : \wp'(z) : 1]\end{aligned}$$

is an isomorphism of complex Lie groups.

To go from $E/\mathbb{C}$ to $\mathbb{C}/\Lambda$ for some lattice Λ

We now sketch the proof of the first statement of theorem 3.1. Let E be an elliptic curve over $\mathbb{C}$. We may assume that E is given by the equation

$$y^2 = x(x-1)(x-\lambda).$$

As we observed at the beginning of the lecture, E is homeomorphic to the torus. Therefore, we can take two paths α and β on E which form a $\mathbb{Z}$ basis for $H_1(E, \mathbb{Z})$. Let ω be the differential 1-form

$$\omega = \frac{dx}{y}.$$

Then ω is an everywhere regular differential form on E (for a proof, see Wilson's notes pg's 16/17). We define two complex numbers

$$\omega_1 = \int_\alpha \omega \quad \text{and} \quad \omega_2 = \int_\beta \omega$$

called *periods* of E and let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. It can be shown that ω_1, ω_2 are linearly independent over $\mathbb{R}$ and hence Λ is a lattice. Fix a point $P_0 \in E(\mathbb{C})$ and define the map

$$\begin{aligned} \psi : E(\mathbb{C}) &\longrightarrow \mathbb{C}/\Lambda \\ P &\longmapsto \int_\gamma \omega + \Lambda \end{aligned}$$

where γ is any path on E joining P_0 to P. If δ is another such path, then $\gamma\delta^{-1}$ is homologous to $n\alpha + m\beta$ for some $n, m \in \mathbb{Z}$. This implies

$$\int_\gamma \omega = \int_\delta \omega + n\omega_1 + m\omega_2$$

and so ψ is well defined. It turns out that ψ is an isomorphism of complex Lie groups, as required!

Remark. By working on the surface $E(\mathbb{C})$ we have been able to interpret the integral

$$\int \frac{dx}{y} = \int \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}.$$

Integrals of this form arise when one attempts to compute arc length on an ellipse. It was in this context that elliptic curves first arose and this explains why they are called 'elliptic' curves.

Lecture 4

Heights and the Mordell-Weil Theorem

Giora Moss
04 / 02 / 2005

Transcribed by David Loeffler – so kudos should go to Mr. Moss but abuse to me.

Our aim in this section is to show that an elliptic curve can't have 'too many' points. We will do this by introducing a measure of the size of a point, which will allow us to prove that there aren't too many 'small' points. To do this we first need a notion of the 'size' of a rational number.

Definition 4.1. *Let $\alpha \in \mathbb{Q}^\times$, $\alpha = \frac{m}{n}$, $m, n \in \mathbb{Z}$, $(m, n) = 1$. Then the* **height** *$H(\alpha) = \max(|m|, |n|)$. Defining $H(0) = 1$, we have an integer-valued function on $\mathbb{Q}$ such that for any k there are only finitely many α such that $H(\alpha) < k$.*

Definition 4.2. *Let E be an elliptic curve over $\mathbb{Q}$; then if $P = (x_P, y_P) \in E(\mathbb{Q})$ we define $H(P) = H(x_P)$. Setting $H(\mathcal{O}) = 1$, we again have the property that there are only finitely many P such that $H(P) < k$.*

The main theorem of this section is the following, which shows that our notion of height interacts well with the group law on the curve.

Theorem 4.3. *There exists constants $c_1, c_2 > 0$ (depending on the curve E) such that*

$$c_1 < \frac{H(P \oplus Q)H(P \ominus Q)}{H(P)^2 H(Q)^2} < c_2.$$

Remark. If we define $h(P) = \log H(P)$, then this tells us that h satisfies the parallelogram law to within $O(1)$.[1]

To prove this, we need several more lemmas:

Definition 4.4. *If $\alpha, \beta \in \mathbb{Q}$ with $\alpha = \frac{m}{t}$, $\beta = \frac{n}{t}$, $(m, n, t) = 1$, then we define $H(\alpha, \beta) = \max(|m|, |n|, |t|)$.*

[1] A logical question to ask now is "is this because h is within $O(1)$ of some genuine quadratic form $\hat{h}$?" It turns out that such an $\hat{h}$, the **canonical height**, does exist, and may be defined (following Tate) as $\lim_{n\to\infty} 4^{-n} h(2^n P)$. This has many pleasant properties, among them that $\hat{h}(P) = 0$ if and only if P is a torsion point.

Lemma 4.5. *There are constants $d_1, d_2 > 0$ such that for all α, β we have*

$$d_1 < \frac{H(\alpha+\beta, \alpha\beta)}{H(\alpha)H(\beta)} < d_2.$$

Proof. Exercise. [Editorial comment: the best upper and lower bounds are in fact 2 and $\frac{\sqrt{5}-1}{2}$ respectively. This statement is much less interesting than it might sound!] □

Lemma 4.6. *We have*

$$x_{P\oplus Q} + x_{P\ominus Q} = \frac{(x_P + x_Q)(b_4 + 2x_P x_Q) + b_2 x_P x_Q + b_6}{(x_P - x_Q)^2}$$
$$x_{P\oplus Q} x_{P\ominus Q} = \frac{x_P^2 x_Q^2 - b_4 x_P x_Q - b_6(x_P + x_Q) - b_8}{(x_P - x_Q)^2}$$

Proof. Since we're working over $\mathbb{Q}$ we can assume WLOG that the curve is given by the equation $y^2 = x^3 + \frac{1}{4}b_2x^2 + \frac{1}{2}b_4x + \frac{1}{4}$; note that this change is made by adjusting y alone, and the x coordinates of points are unaffected.

Now substituting in the equations of the line through P and Q we can derive the stated formulae. □

Lemma 4.7. *In $\mathbb{Q}[x_P, x_Q]$ the three polynomials $(x_P - x_Q)^2$, $(x_P + x_Q)(b_4 + 2x_P x_Q) + b_2 x_P x_Q + b_6$ and $x_P^2 x_Q^2 - b_4 x_P x_Q - b_6(x_P + x_Q) - b_8$ have no common zero with coordinates in $\bar{\mathbb{Q}}$.*

Proof. If there is such a common zero, then $x_p = x_q = x$ and the other two polynomials reduce to $q_1(x) = 4x^3 + b_2x^2 + 2b_4x + b_6 = 0$ and $q_2(x) = x^4 - b_4x^2 - 2b_6x - b_8 = 0$. But $x_{2P} = q_2(x_P)/q_1(x_P)$. Since there are 3 nontrivial 2-torsion points no cancellation can occur. □

We shall write $x_P + x_Q = U = \frac{U_1}{U_3}$ and $x_P x_Q = \frac{U_2}{U_3}$ for integers U_i where $(U_1, U_2, U_3) = 1$.

Lemma 4.8. *We have $x_{P\oplus Q} + x_{P\ominus Q} = \frac{A_1}{A_3}$, $x_{P\oplus Q} x_{P\ominus Q} = \frac{A_2}{A_3}$, where the A_i are defined by*

$$A_1 = U_1U_3b_4 + 2U_1U_2 + b_2U_2U_3 + b_6U_3^2$$
$$A_2 = U_2^2 - b_4U_2U_3 - b_6U_1U_3 - b_8U_3^2$$
$$A_3 = U_1^2 - 4U_2U_3$$

Proof. Calculation. □

It follows that:

Lemma 4.9. *Regarded as polynomials in the U_i, the A_i have no common zero except $(0, 0, 0)$.*

We can now apply the Nullstellensatz to see that the A_i must generate an ideal whose radical is the ideal (U_1, U_2, U_3). Hence:

Lemma 4.10. *There exists an integer p and polynomials $G_{ij} \in \mathbb{Q}[U_1, U_2, U_3]$ of degree p such that*

$$U_i^{p+2} = \sum_j G_{ij} A_j$$

or equivalently polynomials $g_{ij} \in \mathbb{Z}[U_1, U_2, U_3]$ and a positive integer d such that

$$d\, U_i^{p+2} = \sum_j g_{ij} A_j.$$

Proof. The only statement requiring proof is that the G_{ij} have rational coefficients; but this is obvious, since *a priori* they are defined over $\bar{\mathbb{Q}}$ and so their coefficients generate a finite extension of $\mathbb{Q}$. Applying the trace map we obtain polynomials with rational coefficients. □

Lecture 5

Heights and Mordell-Weil, continued

Giora Moss
07 / 02 / 2005

Let's assume from now on that $P \neq \pm Q$.

Observe that $H(x_{P\oplus Q} + x_{P\ominus Q}, x_{P\oplus Q}x_{P\ominus Q}) = \max(|A_1|, |A_2|, |A_3|)/\gamma$, where $\gamma = (A_1, A_2, A_3)$. Using the Nullstellensatz identity above, we see that $\gamma | d$, so γ is bounded by a quantity independent of the particular points we are considering.

Lemma 5.1. *There exist constants c_1, c_2 such that*

$$c_1 H(U,V)^2 \leq \max(A_1, A_2, A_3) \leq c_2 H(U,V)^2.$$

Proof. It is clear that there is some c_1 such that $\max(|A_1|, |A_2|, |A_3|) \leq c_1 H(U,V)^2$. For the other direction, we use the identities of Lemma 4.10; we have

$$|dU_i^{p+2}| \leq c_3 \max(|A_1|, |A_2|, |A_3|) H(U,V)^p,$$

so

$$d\, H(U,V)^{p+2} \leq d\,(|U_1|^{p+2} + |U_2|^{p+2} + |U_3|^{p+2}) \leq c_2 \max(|A_1|, |A_2|, |A_3|) H(U,V)^p$$

and the result follows. □

Since $1 \leq \gamma \leq d$, we have

$$c_1' H(U,V)^2 \leq H(x_{P\oplus Q} + x_{P\ominus Q}, x_{P\oplus Q}x_{P\ominus Q}) \leq c_2' H(U,V)^2$$

for some new constants c_1', c_2'.

Now applying Lemma 4.5, the result of Theorem 4.3 follows, modulo the cases where $P = \pm Q$, which we now consider. Since $H(P) = H(-P)$ it is sufficient to show that there are constants d_1, d_2 such that

$$d_1 \leq \frac{H(2P)}{H(P)^4} \leq d_2.$$

We can freely ignore the finitely many points where $60P = \mathcal{O}$, so we assume

that $\mathcal{O}$, $\pm P$, $\pm 2P$, $\pm 3P$, $\pm 4P$, $\pm 5P$ are all distinct. So the quantities

$$\lambda_1 = \frac{H(3P)H(P)}{H(2P)^2H(P)^2} \qquad \lambda_2 = \frac{H(4P)H(2P)}{H(P)^2H(3P)^2}$$
$$\lambda_3 = \frac{H(5P)H(3P)}{H(P)^2H(4P)^2} \qquad \lambda_4 = \frac{H(5P)H(P)}{H(2P)^2H(3P)^2}$$

are all bounded above and below by nonzero constants. But

$$\lambda_1\lambda_2^2\lambda_3\lambda_4^{-1} = \frac{H(3P)H(P)}{H(2P)^2H(P)^2}\cdot\frac{H(4P)^2H(2P)^2}{H(P)^4H(3P)^4}\cdot\frac{H(5P)H(3P)}{H(P)^2H(4P)^2}\cdot\frac{H(2P)^2H(3P)^2}{H(5P)H(P)} = \frac{H(2P)^2}{H(P)^8},$$

and (4.3) is finally proved.

We are now in a position to prove the Mordell-Weil theorem under a certain plausible assumption, which we shall prove in the next lecture.

Theorem 5.2. *Assume that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. Then $E(\mathbb{Q})$ is finitely generated.*

Proof. Let $Q_1, \ldots, Q_n$ be the elements of $E(\mathbb{Q})/2E(\mathbb{Q})$, and suppose R is any point on the curve. Set $P_1 = R$. We construct a sequence P_j as follows: P_j has an expression in the form $Q_{i_j} + 2S$ for some $i_j \in \{1, \ldots, n\}$ and $S \in E(\mathbb{Q})$; take $P_{j+1} = S$ and repeat the process.

So for each m we obtain

$$R = Q_{i_1} + 2Q_{i_2} + \cdots + 2^{m-2}Q_{i_{m-2}} + 2^{m-1}P_m.$$

However, for some constants c, d, e, f we can write

$$\begin{aligned} H(P_m)^4 &\le cH(2P_m) \\ &= cH(P_{m-1} \ominus Q_{i_{m-1}}) \\ &\le d\,\frac{H(P_{m-1})^2H(Q_{i_{m-1}})^2}{H(P_{m-1} \oplus Q_{i_{m-1}})} \\ &\le eH(P_{m-1})^2 \le f\left[\frac{H(P_{m-1})}{2}\right]^4 \end{aligned}$$

So at least one of $H(P_m) \le \frac{1}{2}H(P_{m-1})$ and $H(P_m) \le \sqrt{f}$ must hold. The former cannot be true for every m; so $E(\mathbb{Q})$ is generated by the finite set $\{Q_1, \ldots, Q_n\} \cup \{P \in E(\mathbb{Q}) | H(P) \le \sqrt{f}\}$. □

Lecture 6

The curve E' *(missing)*

David Rufino
09 / 02 / 2005

I have mislaid my copy of the notes for this one – DL

Lecture 7

Completion of the proof of Mordell-Weil

Zacky Choo
11 / 02 / 2005

In this lecture, covering the next 4 sections of these notes, will be concerned in completing the proof of the Mordell-Weil theorem, in the case of curves with a rational point of order 2. In the following lecture, we will look at some examples, explicitly calculating the rank of some elliptic curves.

7.1 Notation and Recapitulation

O	point at infinity
$E(\mathbb{Q})$	set of rational points on an elliptic curve plus O.
$2E(\mathbb{Q})$	$\{P \oplus P \vert P \in E(\mathbb{Q})\}$
$(\mathbb{Q}^\times)^2$	the multiplicative group of nonzero square rational numbers.

Recall from lecture 5, that we have shown that if $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, then $E(\mathbb{Q})$ is a finitely generated abelian group. From this time forth, we *assume* that E has at least one point of order 2. This implies that we can write E and E' (the dual of E) as follows,

$$E : y^2 = x^3 + ax^2 + bx$$
$$E' : y^2 = x^3 + a'x^2 + b'x$$

where $a' = -2a$ and $b' = a^2 - 4b$, as defined in lecture 6. Also in lecture 6, we defined the maps $\phi : E \to E'$, given by

$$\phi(P) = \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right) & \text{if } P = (x,y), P \notin \{O, (0,0)\} \\ O & \text{if } P \in \{O, (0,0)\} \end{cases},$$

and $\psi : E' \to E$, the natural analogue. We then proved that ϕ and ψ are group homomorphisms, $\psi\phi(E(\mathbb{Q})) = 2(E(\mathbb{Q}))$, and the following two statements.

1. $(0,0) \in \phi(E(\mathbb{Q})) \Leftrightarrow b' = a^2 - 4b \in (\mathbb{Q}^\times)^2$
2. If $u \neq 0$, then $(u,v) \in (E'(\mathbb{Q}))$ lies in $\phi(E(\mathbb{Q})) \Leftrightarrow u \in (\mathbb{Q}^\times)^2$

which has the natural analogue for ψ.

7.2 The Map α

Our aim is to show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. To this end, we will relate this group with other groups like $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ via an exact sequence, then apply the index formula. As one can guess, the exact sequence will have maps like ϕ and ψ, but we lack one more map, which we will call α.

Definition 7.1. *Given an elliptic curve $E' : y^2 = x^3 + a'x^2 + b'x$, as above, define the following map*

$$\alpha_{E'} : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

where $\alpha_{E'}(O) = 1$, $\alpha_{E'}(0,0) = b'$ and $\alpha_{E'}(x,y) = x$ if $x \neq 0$. Also, we define $\alpha_E : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ to be the natural analogue.

Lemma 7.2. *$\alpha_{E'}$ is a group homomorphism, with kernel precisely $\phi(E(\mathbb{Q}))$.*

Proof. We need to show that $\forall$ P, Q in $E(\mathbb{Q})$, $\alpha_{E'}(P \oplus Q) = \alpha_{E'}(P)\alpha_{E'}(Q)$.

We first show that $\alpha_{E'}(\ominus P) = \alpha_{E'}^{-1}(P)$. This is trivial if $P \in \{O, (0,0)\}$. Since we are working in $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, $\alpha_{E'}^{-1}(P) = \alpha_{E'}(P)$. Then we note that if $x \neq 0$, $\ominus(x,y) = (x,-y)$, thus $\alpha_{E'}^{-1}(P) = x = \alpha_{E'}(\ominus P)$.

It then suffices to show that $\forall$ P, Q in $E(\mathbb{Q})$,

$$\alpha_{E'}(P)\alpha_{E'}(Q)\alpha_{E'}(R) = \alpha_{E'}(P \oplus Q \oplus R) = 1$$

where $\ominus R = P \oplus Q$.

Suppose P, Q and R have co-ordinates (x_1, y_1), (x_2, y_2) and (x_3, y_3) respectively, and that they lie on the line $y = mx + c$, then the x_i's are the roots of the following equation,

$$(mx + c)^2 = x^3 + ax^2 + bx$$

This implies that $c^2 = x_1x_2x_3$. Thus if $x_i \neq 0$ for $i = 1, 2, 3$, $\alpha_{E'}(P)\alpha_{E'}(Q)\alpha_{E'}(R) = x_1x_2x_3 = 1$. If WLOG, $R = (0,0)$, then $c = 0$ and $x_1x_2 + x_1x_3 + x_2x_3 = a^2 - 4b = b'$, therefore $\alpha_{E'}(P)\alpha_{E'}(Q)\alpha_{E'}(R) = x_1x_2b' = (b')^2 = 1$.

To get the statement regarding the kernel, apply the statements about ϕ from the previous section/lecture. □

Corollary 7.3. *$\alpha_{E'}$ induces an injection $E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$.*

7.3 The Image of α

Note that by the Corollary, we know that $|E'(\mathbb{Q})/\phi(E(\mathbb{Q}))| = |\text{Im}(\alpha_{E'})|$. In particular, if we can show that the image of $\alpha_{E'}$ is finite, we can ultimately show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Lemma 7.4. *Let (x,y) be any point with co-ordinates in $\mathbb{Q}$ satisfying*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}.$$

Then $\exists$ $m, n, e \in \mathbb{Z}$, $e \geq 1$, $(m,e) = (n,e) = 1$ such that $x = \dfrac{m}{e^2}, y = \dfrac{n}{e^3}$.

Proof. We start with $x = \frac{m}{r}, y = \frac{n}{s}$ s.t. $(m, r) = (n, s) = 1$ (always possible) and consider the factorisation of r and s.
Let p be a prime.
Let p^a be the exact power of p in r, and p^b be the exact power of p in s.
Note that $a > 0 \Leftrightarrow b > 0$.
The exact power of p in the denominator of $x^3 + a_2x^2 + a_4x + a_6$ is p^{3a}.
If $a \geq b$, the power of p in the denominator of $y^2 + a_1xy + a_3y$ is at most p^{2a}, contradiction.
So $b > a$, and the exact power of p in the denominator of $y^2 + a_1xy + a_3y$ is p^{2b}.
Therefore, $2b = 3a$, so $\exists\, d_p \in \mathbb{N}$ s.t. $b = 3d_p$ and $a = 2d_p$.
Finally, let $e = \prod_p p^{d_p}$. Thus $r = e^2$ and $s = e^3$. □

Lemma 7.5. *Let $n' = \varpi(b') =$ number of distinct prime divisors of b'. Let $p_1, p_2, \ldots, p_{n'}$ be the distinct primes dividing b'. Let W' be the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ generated by $p_1, p_2, \ldots, p_{n'}$. Then Im$(\alpha_{E'}) \subset W'$.*

Proof. Let $(x, y) \in E'(\mathbb{Q})$, $x = \frac{m}{e^2}, y = \frac{n}{e^3},\ e \geq 1,\ \ (m, e) = (n, e) = 1, x \neq 0$.
Then plugging this into the equation for E', we get

$$n^2 = m(m^2 + a'me^2 + b'e^4)$$

Let p be a prime.
If $p|m$ and $p \not| (m^2 + a'me^2 + b'e^4)$, $\Rightarrow p|n^2 \Rightarrow p^2|n^2 \Rightarrow p^2|m$.
If $p|m$ and $p|(m^2 + a'me^2 + b'e^4)$, $\Rightarrow p|b'e^4 \Rightarrow p|b'$.
Hence, $m = w^2\varepsilon p_1^{\delta_1}p_2^{\delta_2}\ldots p_{n'}^{\delta_{n'}}$,
where $\varepsilon = \pm 1,\ w \in \mathbb{Z},\ \delta_i \in \{0, 1\},\ \forall\, 1 \leq i \leq n'$. □

Corollary 7.6. *$|Im(\alpha_{E'})| \leq 2^{n'+1}$ and hence $|E'(\mathbb{Q})/\phi(E(\mathbb{Q}))| \leq 2^{n'+1}$.*

7.4 The Exact Sequence

First off, note that everything we have proven for $\alpha_{E'}$ has a direct analogue for α_E. Now finally, we put together all we know about ϕ, ψ and α to give us the following theorem.

Theorem 7.7. *Let $n = \varpi(b)$ and $n' = \varpi(b')$. Then*

$$|E(\mathbb{Q})/2E(\mathbb{Q})| \leq 2^{n+n'+1+p} \quad \textit{where} \quad p = \begin{cases} 1 & \textit{if } b' \in (\mathbb{Q}^\times)^2 \\ 0 & \textit{if } b' \notin (\mathbb{Q}^\times)^2 \end{cases}$$

Proof. The sequence $E(\mathbb{Q}) \xrightarrow{\phi} E'(\mathbb{Q}) \xrightarrow{\psi} E(\mathbb{Q})$ induces the following exact sequence:

$$0 \to \underset{\subset E(\mathbb{Q})}{\{O, (0,0)\}} \hookrightarrow E(\mathbb{Q})_2 \xrightarrow{\phi} \underset{\subset E'(\mathbb{Q})}{\{O, (0,0)\}} \xrightarrow{\alpha'} \frac{E'(\mathbb{Q})}{\phi E(\mathbb{Q})} \xrightarrow{\psi} \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \xrightarrow{\alpha_E} Im(\alpha_E) \to 0$$

where $E(\mathbb{Q})_2$ is the set of points of order 2 in $E(\mathbb{Q})$
and α' is much akin to $\alpha_{E'}$ and can be explicitly described as bringing O to O and $(0, 0)$ to O or $(0, 0)$, depending on whether $(0, 0)$ is in Im(ϕ), which, in turn,

depends on whether b' is in $(\mathbb{Q}^\times)^2$.
Searching for the points of order 2 on $E : y^2 = x^3 + ax^2 + bx$, we check that $|E(\mathbb{Q})_2| = 4$ if $a^2 - 4b \in (\mathbb{Q}^\times)^2$ and $|E(\mathbb{Q})_2| = 2$ if $a^2 - 4b \notin (\mathbb{Q}^\times)^2$

Note that $\text{Im}(\alpha_{E'}) \cong \dfrac{E'(\mathbb{Q})}{\phi E(\mathbb{Q})}$ and $\text{Im}(\alpha_E) \cong \dfrac{E(\mathbb{Q})}{\psi E'(\mathbb{Q})}$, thus by the index formula,

$$\left|\frac{E'(\mathbb{Q})}{2E(\mathbb{Q})}\right| = |E(\mathbb{Q})_2|\frac{|Im(\alpha_E)||Im(\alpha_{E'})|}{2\times 2} \leq 2^{n+n'+1+p}.$$

□

Corollary 7.8. *If $E(\mathbb{Q})$ has at least one point of order 2, then $E(\mathbb{Q})$ is a finitely generated abelian group.*

Notation: We write $E(\mathbb{Q}) = \Delta \times \mathbb{Z}^{g_E}$, where Δ is the torsion group and g_E is the finite rank of E.

Theorem 7.9. *The rank g_E is given by the formula*

$$2^{g_E} = \frac{|Im(\alpha_E)||Im(\alpha_{E'})|}{4}.$$

Proof.

$$\frac{E(\mathbb{Q})}{2E(\mathbb{Q})} = \frac{\Delta}{2\Delta} \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{g_E} = E(\mathbb{Q})_2 \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{g_E}.$$

□

7.5 Determination of Im(α)

Given an elliptic curve E that has at least one point of order 2, we have seen from the last theorem that if we are able to determine $\text{Im}(\alpha_E)$ and $\text{Im}(\alpha_{E'})$, then we can determine the rank g_E. In this section, we will explain how we can explicitly determine $\text{Im}(\alpha_E)$ and $\text{Im}(\alpha_{E'})$.

Recall that we can write E and E' as follows:

$$\begin{aligned} E: &\quad y^2 = x^3 + ax^2 + bx \\ E': &\quad y^2 = x^3 + a'x^2 + b'x \end{aligned}$$

Lemma 7.10. *The equation $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ has a solution for some $b_1, b_2, N, M, e \in \mathbb{Z}$, $e > 0$, $b_1b_2 = b$, if and only if $(\dfrac{b_1M^2}{e^2}, \dfrac{b_1MN}{e^3}) \in E(\mathbb{Q})$.*

Proof. Consider $y^2 = x^3 + ax^2 + bx$.

$$\begin{aligned} y^2 &= \frac{b_1M^2}{e^2}\left(\frac{b_1^2M^4}{e^4} + \frac{ab_1M^2}{e^2} + b\right) \\ &= \frac{b_1^2M^2}{e^6}\left(b_1M^4 + aM^2e^2 + b_2e^4\right) = \frac{b_1^2M^2N^2}{e^6}. \end{aligned}$$

□

The lemma implies that if $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ has a solution, then b_1 is in Im(α_E). However, the converse is not immediately obvious. This is easily fixed by the following lemma.

Lemma 7.11. *Suppose $(x, y) \in E(\mathbb{Q})$ and $\alpha_E(x, y) = b_1$, then the equation $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ has a solution for some $N, M, e \in \mathbb{Z}$, $e > 0$, $b_1b_2 = b$.*

Proof. First off, note that by Lemma 7.5 on page 26, we know that b_1 divides b. By Lemma 7.4 on page 25, and using our hypothesis, we can write

$$x = \frac{b_1M^2}{e^2}, y = \frac{n}{e^3}, \text{where } e > 0, (M, e) = (n, e) = (b_1, e) = 1$$

We plug this into $y^2 = x^3 + ax^2 + bx$, and after some algebraic manipulation, we get $n^2 = b_1^2M^2(b_1M^4 + aM^2e^2 + b_2e^4)$. Note that all the variables are integers, and we thus deduce the lemma. □

Remark. Using a similar method, we can show that given $(x, y) \in E(\mathbb{Q})$, and setting $b_1 = (b, m)$, we can find a solution for $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ such that $(M, e) = (N, e) = (b_1, e) = (b_2, M) = (N, M) = 1$.

Corollary 7.12. *The equation $N^2 = b_1M^4 + aM^2e^2 + b_2e^4$ has a solution for some $b_1, b_2, N, M, e \in \mathbb{Z}$, $e > 0$, $b_1b_2 = b$, if and only if b_1 is in Im(α_E).*

Remark. The Corollary is still true if we replace α_E by $\alpha_{E'}$ and b by b'.

Lecture 8

Examples of rank calculations

Zacky Choo
14 / 02 / 2005

We note from Lemma 7.5 on page 26 that $\mathrm{Im}(\alpha_E)$ (resp. $\mathrm{Im}(\alpha_{E'})$) is contained in a finite set generated by -1 and the prime divisors of b (resp. b'). Corollary 7.12 on the page before will be the main tool in the determination of the image of α, and while it is sufficient, a few remarks would help simplify our working.

Remark. Note that $1, b \in \mathrm{Im}(\alpha_E)$ since $\alpha_E O = 1$ and $\alpha_E(0,0) = b$. Also since α_E is a group homomorphism, $\mathrm{Im}(\alpha_E)$ obeys group laws, that is, if $x, y \in \mathrm{Im}(\alpha_E)$, then so is xy. Again, the remark holds true if we replace α_E by $\alpha_{E'}$ and b by b'.

Example 1 $E : y^2 = x^3 - x$ First we determine $\mathrm{Im}(\alpha_E)$. $b = -1 \Rightarrow \mathrm{Im}(\alpha_E) \subset \{\pm 1\}$
By the remark above, $\mathrm{Im}(\alpha_E) = \{\pm 1\}$, thus $|\mathrm{Im}(\alpha_E)| = 2$. Next, we determine $\mathrm{Im}(\alpha_{E'})$. We have $E' : y^2 = x^3 + 4x$. $b' = 4 \Rightarrow \mathrm{Im}(\alpha_{E'}) \subset \{\pm 1, \pm 2\}$.

We need only consider the equation $N^2 = b_1 M^4 + aM^2e^2 + b_2 e^4$ for $b_1 = -1, 2$ by the above remark, but we'll just check all the cases anyway.

$b_1 = 1$	$: N^2 = M^4 + 4e^4$	$N = 2, M = 0, e = 1$
$b_1 = -1$	$: N^2 = -M^4 - 4e^4$	No solutions, by considering positivity
$b_1 = 2$	$: N^2 = 2M^4 + 2e^4$	$N = 2, M = e = 1$
$b_1 = -2$	$: N^2 = -2M^4 - 2e^4$	No solutions, by positivity

Therefore, $|\mathrm{Im}(\alpha_{E'})| = \{1, 2\} = 2$.
Then by Theorem 7.9 on page 27, $2^{g_E} = (2 \times 2)/4 \Rightarrow g_E = 0$.

Example 2 $E : y^2 = x^3 - 17x$. $b = -17 \Rightarrow \mathrm{Im}(\alpha_E) \subset \{\pm 1, \pm 17\}$. We need only consider $N^2 = b_1 M^4 + aM^2e^2 + b_2 e^4$ for $b_1 = -1$. $b_1 = -1$ $: N^2 = -M^4 + 17e^4$ $N = 4, M = e = 1$
Therefore, $|\mathrm{Im}(\alpha_E)| = |\{\pm 1, \pm 17\}| = 4$.

$E' : y^2 = x^3 + 4 \cdot 17x$. $b' = 4 \cdot 17 \Rightarrow \mathrm{Im}(\alpha_{E'}) \subset \{\pm 1, \pm 2, \pm 17, \pm 2 \cdot 17\}$. We need only consider the generators $b_1 = -1, 2$. [Note $17 \equiv b' \bmod (\mathbb{Q}^\times)^2$].

$b_1 = -1$	$: N^2 = -M^4 - 4 \cdot 17e^4$	No solutions by positivity
$b_1 = 2$	$: N^2 = 2M^4 + 2 \cdot 17e^4$	$N = 6, M = e = 1$

Therefore, $|\mathrm{Im}(\alpha_{E'})| = |\{1, 17, 2, 2 \cdot 17\}| = 4$. Therefore, $g_E = 2$.

Example 3 $E : y^2 = x^3 - 226x \quad b = -2 \cdot 113 \Rightarrow \text{Im}(\alpha_E) \subset \{\pm 1, \pm 2, \pm 113, \pm 2 \cdot 113\}$. We need only consider $b_1 = -1, 2$.

$b_1 = -1 \quad : N^2 = -M^4 + 226e^4 \qquad N = 15, M = e = 1$

$b_1 = 2 \qquad : N^2 = -2M^4 + 113e^4 \quad N = 9, M = 2, e = 1$

Therefore, $|\text{Im}(\alpha_E)| = 8$.

$E' : y^2 = x^3 + 4 \cdot 226x$. $b' = 2^3 \cdot 113 \Rightarrow \text{Im}(\alpha_{E'}) \subset \{\pm 1, \pm 2, \pm 113, \pm 2 \cdot 113\}$. We need only consider $b_1 = -1, 2$. [Note $2 \cdot 113 \equiv b' \bmod (\mathbb{Q}^\times)^2$].

$b_1 = -1 \quad : N^2 = -M^4 - 2^3 \cdot 113e^4$ No solutions by positivity

$b_1 = 2 \qquad : N^2 = 2M^4 + 4 \cdot 113e^4 \qquad N = 22, M = 2, e = 1$

Therefore, $|\text{Im}(\alpha_{E'})| = 4$. Therefore, $g_E = 3$.

Example 4 $E : y^2 = x^3 + px$, where p is a prime, $p \equiv 5 \bmod 8$. $b = p \Rightarrow \text{Im}(\alpha_E) \subset \{\pm 1, \pm p\}$. We need only consider $b_1 = -1$. $b_1 = -1 \quad : N^2 = -M^4 - pe^4$ No solutions

Therefore, $|\text{Im}(\alpha_E)| = |\{1, p\}| = 2$.

$E' : y^2 = x^3 - 4px$. $b' = -4p \Rightarrow \text{Im}(\alpha_E) \subset \{\pm 1, \pm 2, \pm p, \pm 2p\}$. We need only consider the generators $b_1 = -1, 2$ and p. Note $-p = b' \bmod (\mathbb{Q}^\times)^2$, so it is sufficient to check when $b_1 = 2$ and p. (Checking at $b_1 = -1$ is equivalent to checking at $b_1 = p$). Suppose $b_1 = 2$, then consider $N^2 = 2M^4 - 2pe^4$.

$$\Rightarrow N^2 \equiv 2M^4 (\text{mod } p) \Rightarrow \left(\frac{2M^2}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{N^2}{p}\right) = 1$$

However, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = -1$, i.e., contradiction. Suppose $b_1 = p$, then consider $N^2 = pM^4 - 4e^4$ Therefore, depending on whether this equation has a solution, $|\text{Im}(\alpha_{E'})| = |\{1, -p\}| = 2$ or $|\text{Im}(\alpha_{E'})| = |\{\pm 1, \pm p\}| = 4$, which implies $g_E = 0$ or 1. We know that there exist solutions of $N^2 = pM^4 - 4e^4$ for the first few primes.

p	N	M	e
5	1	1	1
13	1	3	1
29	1	5	1
37	3	151	3
53	1	7	1

Conjecture: For all $E : y^2 = x^3 + px$, $p \equiv 5 \bmod 8$, $g_E = 1$.

Lecture 9

Introduction to the P-adic numbers

Chernyang Lee
16 / 02 / 2005

Transcribed and edited by David Loeffler from Chernyang's photocopied notes.

The p-adic numbers can be approached from two perspectives: as completions, or as formal power series.

9.1 Valuations

Let p be a rational prime. Then we define the p-adic valuation ν_p on $\mathbb{Q}$ to be the map $\nu_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ defined by $\nu_p(0) = +\infty$ and $\nu_p(p^n \frac{r}{s}) = n$, where $n \in \mathbb{Z}$ and $(r, p) = (s, p) = 1$. It's easily checked that $\nu_p(xy) = \nu_p(x) + \nu_p(y)$.

Define the p-adic absolute valuation $|\cdot|_p$ by $|x|_p = p^{-\nu_p(x)}$. So $|xy|_p = |x|_p|y|_p$.

Proposition 9.1. *Defining $d_p(x, y) = |x - y|_p$, $(\mathbb{Q}, d_p)$ is a metric space.*

Proof. We must check the following are satisfied:

1. $d_p(x, y) \geq 0$ with equality iff $x = y$: clear.
2. $d_p(x, y) = d_p(y, x)$: clear.
3. $d_p(x, z) \leq d_p(x, y) + d_p(y, z)$: we shall show that a stronger result in fact holds, that $d_p(x, z) \leq \max(d_p(x, y), d_p(y, z))$. This is an easy check from the definition, since if p^r divides $x - y$ and $y - z$ it certainly divides $x - z$.

□

A space satisfying the stronger condition of (3) above is known as an *ultrametric space*. It's clear that equality occurs unless $d_p(x, y) = d_p(y, z)$, so in an ultrametric space "all triangles are isosceles". Ultrametric spaces have a number of useful properties that make analysis in these spaces much easier than in $\mathbb{R}$:

9.1.1 Crucial property of ultrametric spaces

a sequence $\{a_n\}$ in an ultrametric space (X, d) is Cauchy if and only if $d(a_n, a_{n+1}) \to 0$; and if $a_n \to a$ and $b \neq a$, then $d(a_n, b) = d(a, b)$ for all sufficiently large n.

Proof. 1. The "only if" is trivial; so assume $d(a_n, a_{n+1}) \to 0$. By induction, for all $m \geq n$ we have $d(a_n, a_m) \leq \max\{d(a_n, a_{n+1}), d(a_{n+1}, a_{n+2}), \ldots, d(a_{m-1}, a_m)\}$, which is $< \epsilon$ for all sufficiently large n. Hence $\{a_n\}$ is Cauchy.

2. Since $d(a_n, a) \to 0$, for all sufficiently large n we have $d(a_n, a) < d(a, b)$, so $d(a_n, b) = d(a, b)$ by the isosceles triangles remark above.

□

Completion of $(\mathbb{Q}, d_p)$

If $\{x_n\}, \{y_n\}$ are both Cauchy sequences in $(\mathbb{Q}, d_p)$ we write $\{x_n\} \equiv \{y_n\}$ if $d_p(x_n, y_n) \to 0$. It's easy to check that this is an equivalence relation, and if R is the ring of Cauchy sequences with pointwise addition and multiplication, the set of sequences equivalent to 0 is a maximal ideal. So the quotient is a field – the p-adic numbers $\mathbb{Q}_p$.

We extend the absolute value $|\cdot|_p$ to $\mathbb{Q}_p$ in the obvious way, as $\lim |x_n|_p$ – this is well-defined and extends the valuation on $\mathbb{Q}$ by the second half of the above result.

We can now define

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid |x|_p \leq 1\}$$
$$\mathfrak{M}_p = \{x \in \mathbb{Q}_p \mid |x|_p < 1\}$$

Proposition 9.2. *$\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. $\mathfrak{M}_p$ is the unique maximal ideal of $\mathbb{Z}_p$, so $\mathbb{Z}_p$ is a local ring, the ring of p-adic integers.*

Proof. Again this is routine verification; the fact that $\mathbb{Z}_p$ is a subring follows as the extended absolute value still satisfies $|x+y|_p \leq \max(|x|_p, |y|_p)$ and $|xy|_p = |x|_p|y|_p$, and that $\mathbb{Z}_p$ is local follows since every element not in $\mathfrak{M}_p$ is invertible in $\mathbb{Z}_p$. □

9.2 Explicit representation of $\mathbb{Q}_p$ as formal power series

Again let p be a rational prime; then we can define a p-adic number to be a formal power series

$$\alpha = \sum_{n=-M}^{\infty} a_m p^m$$

where a_i are integers such that $0 \leq a_i \leq p-1$.

When this is a finite formal sum, then in an obvious sense it represents a rational number; but not all rationals are of this form (indeed, only those whose denominator are a power of p). However we shall see that every rational does have a unique expansion in this form, which eventually repeats to the right.

Let T be the ring of such formal series, with the obvious algebraic operations suggested by the notation. Then we can define a valuation $\|\cdot\|_p$ on T by $\|\alpha\| = p^{-m}$ where a_m is the first nonzero coefficient of α.

To any α we associate the sequence of truncated sums $S_i = \sum_{-M}^{i} a_i p^i$. The sequence $\{S_i\}$ is then Cauchy with respect to the valuation $\|\cdot\|$ and tends to α.

Now, we have seen that there is a natural map from the rationals with denominator a power of p into a dense subset of T; and the two valuations agree on

this set. It's an easy exercise to check that such rationals are dense in $\mathbb{Q}$ in the topology induced by $|\cdot|_p$, and since T is evidently complete with respect to the valuation $\|\cdot\|_p$ and in, we obtain an isomorphism between $\mathbb{Q}_p$ and our ring T of formal series.

Thus we can equate $\mathbb{Q}_p$ with T; then we have the identifications

$$\mathbb{Z}_p = \left\{ \alpha \in T \mid \alpha = \sum_{i \geq 0} a_i p^i \right\}$$
$$\mathfrak{M}_p = \left\{ \alpha \in T \mid \alpha = \sum_{i > 0} a_i p^i \right\} = p\mathbb{Z}_p$$

9.2.1 The sequence corresponding to a p-adic integer

Interpreting $\alpha \in \mathbb{Z}_p$ as the limit of the sequence $S_0, S_1, \ldots$ as defined above (where the S_i are now integers), we clearly have $S_i = S_{i+1} \bmod p^{i+1}$. For convenience we shall write this as $s_i = \alpha \bmod p^{i+1}$.

Conversely, given any sequence of integers S_i satisfying this compatibility requirement, they form a Cauchy sequence in $\mathbb{Q}_p$, so they determine a unique p-adic integer α such that $\alpha = S_n \bmod p^{n+1}$. So we have an alternative definition of $\mathbb{Q}_p$ as the inverse limit of the groups $\mathbb{Z}/p^n\mathbb{Z}$ with the obvious reduction maps $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$.

9.2.2 Hensel's lemma (simplest form)

Theorem 9.3. *Given a polynomial $f(t) \in \mathbb{Z}[t]$, and some $s_0 \in \mathbb{Z}$ such that $f(s_0) = 0 \bmod p$, with $f'(s_0) \neq 0 \bmod p$, then there is some $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha = s_0 \bmod p$.*

Proof. We shall construct by induction a sequence s_i such that $f(s_i) = 0 \bmod p^{i+1}$ and $s_i = s_{i-1} \bmod p^i$. Then this defines an element of $\mathbb{Z}_p$ with $f(\alpha) = 0 \bmod p^n$ for all n, so $f(\alpha) = 0$.

The base case is given by hypothesis; so we assume case $n = k$ is true. Then

$$\begin{aligned} f(s_k + cp^{k+1}) &= f(s_k) + p^{k+1} c f'(s_k) \bmod p^{k+2} \\ &= p^{k+1}(t + cf'(s_k)) \bmod p^{k+2} \text{ for some } t. \end{aligned}$$

Now by hypothesis $f'(s_k) = f'(s_0) \neq 0 \bmod p$, so it is invertible mod p and we may choose c such that $f(s_k + cp^{k+1}) = 0 \bmod p^{k+2}$. So it is choose $s_{k+1} = s_k + cp^{k+1}$. □

Remark. Observe that there is only one possible choice of $c(\mathrm{mod} p)$ at each stage, so there is a *unique* solution in $\mathbb{Z}_p$ reducing to the given root in $\mathbb{F}_p$.

9.3 Algebraic extensions of $\mathbb{Q}_p$

If $L/\mathbb{Q}_p$ is a finite algebraic extension of degree n, we can define a valuation on L by

$$|\beta|_p = \left|N_{L/\mathbb{Q}_p}\beta\right|^{1/n};$$

Then the following facts are true:

1. This really is a valuation, and it is the unique extension of $|\cdot|_p$ to L.
2. $\mathcal{O}_L = \{\beta \in L \mid |\beta|_p \leq 1\}$ is a subring of L and is the integral closure of $\mathbb{Z}_p$ in L.
3. $\mathcal{O}_L$ is a local ring, and its unique maximal ideal is $\mathcal{P}_L = \{\beta \in L \mid |\beta|_p < 1\}$, which is the unique prime of L above p.
4. The quotient $\mathcal{O}_L/\mathcal{P}_L$ (the residue field of L) is a finite algebraic extension of $\mathbb{F}_p$ of the same degree as $L/\mathbb{Q}_p$.

For a proof, see Milne's online notes "Algebraic Number Theory", Thm 7.29 (p105).

Remark. Although this is stated for a finite extension, we can perform the construction in an arbitrary algebraic extension; simply define $|x|_p$ via the valuation corresponding to some finite extension $L/\mathbb{Q}_p$ containing x. By the tower law for norms, it does not matter which L we choose, and we thus obtain a valuation on the algebraic closure $\overline{\mathbb{Q}_p}$.

Now, if L is such an extension of $\mathbb{Q}_p$, then L has only one prime, so there are two possibilities for how p factors in L. Either $p\mathcal{O}_L$ is prime, in which case it must be $\mathcal{P}_L$; or it is $\mathcal{P}_L^e$ for some $e > 1$. In the first case we say the extension $L/\mathbb{Q}_p$ is *nonramified*; in the second case it is *ramified*.

One common application of this result is to the splitting of primes in number fields. If K is a number field and p is a rational prime, then p will factorise in K as a product $\prod \mathfrak{P}_i^{e_i}$ of prime ideals of K. We can complete K at any of these primes $\mathfrak{P}_i$ to obtain a complete field $K_{\mathfrak{P}_i}$ which is an algebraic extension of $\mathbb{Q}_p$, corresponding to adjoining to $\mathbb{Q}_p$ a root of one of the irreducible factors in $\mathbb{Q}_p[X]$ of the minimal polynomial of a primitive element of K.

Now, it is not too hard to see that the ramification index of the extension $K_{\mathfrak{P}_i}/\mathbb{Q}_p$ is precisely e_i. In particular $K_{\mathfrak{P}_i}/\mathbb{Q}_p$ is nonramified if and only if $\mathfrak{P}_i/p$ does not ramify in $K/\mathbb{Q}$. So studying extensions of $\mathbb{Q}_p$ allows us to isolate the ramification at a particular prime; this will be important when we study the extensions of $\mathbb{Q}$ arising from torsion points.

Example: Let p be a prime congruent to 3 or 5 mod 8. Then 2 is not a square modulo p, so it is not a square in $\mathbb{Q}_p$ and the extension $\mathbb{Q}_p(\sqrt{2})/\mathbb{Q}$ is of degree 2. It is nonramified, since if we had $2\mathcal{O}_L = \mathcal{P}_L^2$, then 2 would have to ramify in the extension of number fields $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, which it does not. On the other hand, $\mathbb{Q}_p(\sqrt{p})$ is a ramified extension of ramification index 2.

9.3.1 Classification of unramified extensions

Now, we shall prove a theorem which explicitly classifies the possible nonramified extensions of $\mathbb{Q}_p$.

Theorem 9.4. *There is a bijection*

$$\{\textit{finite nonramified extensions } K/\mathbb{Q}_p\} \longleftrightarrow \{\textit{finite extensions } k/\mathbb{F}_p\}$$
$$K \longleftrightarrow k = \textit{residue field of } K$$

Moreover, this is inclusion-preserving (so $K \subset K' \iff k \subset k'$); and all the nonramified extensions are Galois over $\mathbb{Q}_p$.

Proof. We first show that the map sending an nonramified extension to its residue field is surjective.

Let $k/\mathbb{F}_p$ be a finite extension; then by the primitive element theorem, $k = \mathbb{F}_p(a)$ some a. Suppose $f(X) \in \mathbb{Z}_p[X]$ is any lifting of the minimal polynomial $\bar{f}(X) \in \mathbb{F}_p[X]$ for a. Then by Hensel's lemma applied to the local field $\overline{\mathbb{Q}_p}$, whose residue field is the algebraic closure $\overline{\mathbb{F}_p}$, there is a unique $\alpha \in \overline{\mathbb{Q}_p}$ such that $\alpha = a \bmod \mathcal{P}$, where $\mathcal{P}$ is the maximal ideal of the ring of integers of $\overline{\mathbb{Q}_p}$. Then the residue field of $\mathbb{Q}_p(\alpha)$ is clearly $\mathbb{F}_p(a) = k$; and since $\bar{f}$ is irreducible in $\mathbb{F}_p[X]$, $\mathbb{Q}_p(\alpha)/\mathbb{Q}$ is nonramified.

Now, suppose K_1 and K_2 are nonramified extensions of $\mathbb{Q}_p$ with isomorphic residue fields. Then K_1K_2 is an nonramified extension of $\mathbb{Q}_p$, and its residue field is still k. But since $[K_1K_2 : \mathbb{Q}_p] = [k : \mathbb{F}_p] = [K_1 : \mathbb{Q}_p]$, we must have $K_1 \supset K_2$, and similarly $K_2 \supset K_1$, so K_1 and K_2 are isomorphic.

It is clear that this map is a lattice isomorphism, so it remains to prove the statement that nonramified extensions of $\mathbb{Q}_p$ are Galois. However, it is known that finite extensions of $\mathbb{F}_p$ are always Galois; so given $K/\mathbb{Q}_p$, we know that its residue field k is Galois. Let's write $K = \mathbb{Q}_p(\alpha)$ where α has minimal polynomial f. Now $\bar{f} \in \mathbb{F}_p(X)$ must split completely in k, since k is Galois; but each of the roots in k must lift to a root in K, by Hensel's lemma. So f splits completely in K, and $K/\mathbb{Q}_p$ is Galois. □

Remark. It's easily shown that if L_1 and L_2 are nonramified extensions of $\mathbb{Q}_p$, then the composite L_1L_2 is nonramified; hence the union of all nonramified extensions of $\mathbb{Q}_p$ is a field, denoted by $\mathbb{Q}_p^{nr}$ – the maximal nonramified extension of $\mathbb{Q}_p$. This is then a local field and its residue field is the full algebraic closure $\overline{\mathbb{F}_p}$.

Lecture 10

Introduction to formal groups

James Cranch
18 / 02 / 2005

10.0 Motivation *(non-examinable)*

In an attempt to understand the group structure on an elliptic curve, we might be tempted to treat it analogously to a Lie group, and thus attempt to form its Lie algebra.

While modern algebraic geometry permits us to make this construction, the results are disappointing. Indeed, since the group law of an elliptic curve is abelian, we only get a trivial Lie algebra.

On the other hand, there is another natural local construction we can make in algebraic geometry: given an elliptic curve E over a field K we can take the local ring at the identity $\mathcal{O}_{E,0}$. In general, local rings contain much more detailed information about an object than tangent spaces.

Thus it is desirable to try to model the group structure within the local ring. This lecture develops some machinery which will be necessary to interpret the result; next lecture sees us apply these techniques to elliptic curves.

10.1 Complete rings, local rings and Hensel's lemma

Here are the basic definitions:

Definition 10.1. *If R is a noetherian integral domain, and $\mathcal{I}$ an ideal, we define a norm*

$$|x|_{\mathcal{I}} = \exp(-\max\{n | x \in \mathcal{I}^n\}).$$

*We then define the **completion** of R with respect to $\mathcal{I}$ to be the completion with respect to this norm.*

*A ring is **local** if it has only one maximal ideal.*

If R is local, and $\mathcal{M}$ is its maximal ideal, we denote its completion with respect to this norm by $\hat{R}$; this is also local with maximal ideal $\overline{\mathcal{M} \cdot \hat{R}}$.

And here are some important examples:

- All fields are local rings (with maximal ideal (0)). **Warning**: Do not confuse local rings with local fields.
- If R is an integral domain, and P a prime ideal then the *localisation*

$$R_P = \{r/s \in \text{Frac}(R) : r \in R, s \notin P\}$$

  is a local ring with maximal ideal $PR_P \subset R_P$.
- As a particular case of the above, the localisation $\mathbb{Z}_{(p)}$ can be completed to form the p-adic ring $\mathbb{Z}_p$.
- The ring $F[X]$, for F a field, is local with maximal ideal $XF[X]$. Its completion is the *formal power series ring* $F[[X]]$.

Armed with this, we can state the major technical tool in this area:

Theorem 10.2. *("Hensel's Lemma") Let R be a ring which is complete with respect to some ideal $\mathcal{I}$. Suppose that $F(X) \in R[X]$, $a \in R$ and $n \geq 1$ are such that $F(a) \in \mathcal{I}^n$ and $F'(a) \in R^\times$. Then, if $\alpha \equiv F'(a) \pmod{\mathcal{I}}$ then the sequence*

$$w_0 = a, \qquad w_{m+1} = w_m - F(w_m)/\alpha$$

converges to an element $b \in R$ such that $F(b) = 0$ and $b \equiv a \pmod{\mathcal{I}^n}$. Furthermore, if R is an integral domain, then b is uniquely determined.

Proof. Omitted (see Silverman, IV.1.2). □

10.2 Formal groups

We start with the definition:

Definition 10.3. *Let R be a ring. A **one-parameter commutative formal group law** $(\mathcal{F}, F)$, (hereafter simply a **formal group law**, or **FGL**), is a power series $F(X, Y) \in R[[X, Y]]$ such that:*

- $F(X, 0) = X$,
- $F(X, Y) = F(Y, X)$, *and*
- $F(X, F(Y, Z)) = F(F(X, Y), Z)$.

Here is a proposition gathering two immediate further "grouplike" properties of these things:

Proposition 10.4. *If $(\mathcal{F}, F)$ is a formal group law, then:*

1. *$F(X, Y) = X + Y +$ higher order terms, and*
2. *There is a power series $i(X) \in R[[X]]$ such that $F(X, i(X)) = 0$.*

Proof. (Sketch) Part 1 is immediate from the first two conditions. For part 2, build $i(X)$ term-by-term. □

Now, here are a couple of simple examples of these things:

- The *additive* formal group law, denoted $\hat{\mathbb{G}}_{\mathrm{a}}$, is given by $F(X,Y) = X + Y$. The inverse is given by $i(X) = -X$.
- The *multiplicative* formal group law, denoted $\hat{\mathbb{G}}_{\mathrm{m}}$, is given by $F(X,Y) = X + Y + XY$. The inverse is given by $i(X) = -X \cdot (1+X)^{-1} = -X + X^2 - X^3 + \cdots$.

Definition 10.5. *Suppose $(\mathcal{F}, F)$ and $(\mathcal{G}, G)$ are formal group laws defined over a ring R. A **homomorphism** f between F and G is a power series $f \in R[[X]]$ such that $f(F(X,Y)) = G(f(X), f(Y))$.*

The classic example of a homomorphism is the "multiplication-by-n" endomorphism $[n]$ of a formal group. This is analogous to the multiplication-by-n endomorphism of an ordinary group.

It is defined in the natural way as:

$$\begin{aligned} [0](X) &= 0 \\ [n+1](X) &= F([n](X), X) \\ [n-1](X) &= F([n](T), i(X)) \\ \text{and thus eg. } [1](X) &= X \\ [2](X) &= F(X,X) \\ [3](X) &= F(F(X,X),X) \\ [-1](X) &= i(X) \\ [-2](X) &= F(i(X), i(X)) \end{aligned}$$

10.3 Groups from formal groups

A formal group is just a power series with pleasant properties. It is well-known that power series in general need not converge as functions. However, if $(\mathcal{F}, F)$ is a formal group defined over a complete local ring R with maximal ideal $\mathcal{M}$, then F *does* define an honest group on $\mathcal{M}$:

Proposition 10.6. *The operations $x +_{\mathcal{F}} y = F(x,y)$ (for $x, y \in \mathcal{M}$) and $-_{\mathcal{F}} x = i(x)$ (for $x \in \mathcal{M}$) define a group structure on $\mathcal{M}$.*

Proof. If we take successive partial sums of either of these series, we get a Cauchy sequence. This is because, for all n, differences between partial sums are eventually within $\mathcal{M}^n$ and thus tend to 0 by definition of the norm on R.

Moreover, the limit is in $\mathcal{M}$, by comments made earlier. □

Definition 10.7. *We call this group the **associated group** of $\mathcal{F}$, and denote it by $\mathcal{F}(\mathcal{M})$.*

Observe also that $\mathcal{M}^n$ form subgroups for all n.

Here's some examples:

- The associated group of $\hat{\mathbb{G}}_{\mathrm{a}}$ is $\mathcal{M}$ under addition. Thus, letting k be the "residue field" $R/\mathcal{M}$, there is an exact sequence

$$0 \to \hat{\mathbb{G}}_{\mathrm{a}}(\mathcal{M}) \to R \to k \to 0.$$

- The associated group of $\hat{\mathbb{G}}_{\mathrm{m}}$ is (after translating up by 1) $1 + \mathcal{M}$ under multiplication. So there is another exact sequence

$$0 \to \hat{\mathbb{G}}_{\mathrm{m}}(\mathcal{M}) \to R^{\times} \to k^{\times} \to 0.$$

Lecture 11

Formal groups continued

James Cranch
21 / 02 / 2005

11.1 The Formal Group Law of an Elliptic Curve

Now we examine the local group structure of an elliptic curve E near the identity. It would be clumsy to attempt this without having the identity in full view, so we make a change of coordinates:

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}; \quad \text{ie.} \quad (X : Y : Z) \mapsto (-X : -Z : Y)$$

Now, if we look at the affine piece with coordinates z, w, we find the identity is at the origin. Furthermore, the generalised Weierstrass equation for E becomes:

$$w = z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3 = f(z, w).$$

It is immediate from this to calculate that the tangent to the curve at the origin is $w = 0$: this makes us believe that near the origin a point is uniquely determined by z.

Indeed, we can write w as a formal power series in terms of z by using the formula above, and repeatedly substituting $f(z, w)$ for w:

$$\begin{aligned}
w &= f(z, w) \\
&= z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3 \\
&= z^3 + (a_1 z + a_2 z^2)f(z, w) + (a_3 + a_4 z)f(z, w)^2 + a_6 f(z, w)^3 \\
&= z^3 + (a_1 z + a_2 z^2)(z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3) \\
&\quad + (a_3 + a_4 z)(z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3)^2 \\
&\quad + a_6(z^3 + (a_1 z + a_2 z^2)w + (a_3 + a_4 z)w^2 + a_6 w^3)^3 \\
&= \cdots
\end{aligned}$$

Proposition 11.1. *This process converges to give a power series $w(z)$, satisfying $f(z, w(z)) = w(z)$.*

Proof. This is Hensel's lemma, applied to the ring $R = \mathbb{Z}[a_1, \ldots, a_6][[z]]$, which is complete with respect to the ideal Rz. For the polynomial $F(w)$ we use $f(z, w) - w$, and we take $a = 0$, $\alpha = -1$. □

Indeed, we can compute the first few terms, using that every w contributes no z terms with a power less than three. Plugging in a bit we get

$$w(z) = z^3 + a_1 z^4 + (a_1^2 + a_2) z^5 + (a_1 z^3 + 2a_1 a_2 + a_3) z^6 + \cdots .$$

In general we will write:

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \cdots).$$

Now we have a one-variable parametrisation near the identity of an elliptic curve, it is just a matter of algebraic manipulation to derive the formal group law F. It is important to see how this is done, and so we shall see an algorithm.

We let z_1, z_2 symbolise variables for our parametrisation, and – writing $w_1 = w(z_1), w_2 = w(z_2)$ – we see that $(z_1, w_1), (z_2, w_2)$ will symbolise indeterminate points on the curve.

To take the sum of these points, we would construct the line through them. To do this we would calculate the slope

$$\lambda = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{z_2^n - z_1^n}{z_2 - z_1},$$

and by factorising the terms on the right, we see this lies in $\mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]$.

We also let $c = w_1 - \lambda z_1$, so that the line through them has equation

$$w = \lambda z + c.$$

Substituting this into the transformed generalised Weierstrass equation we obtained earlier for w in terms of w and z gives a cubic in z:

$$(\lambda z + c) = z^3 + (a_1 z + a_2 z^2)(\lambda z + c) + (a_3 + a_4 z)(\lambda z + c)^2 + a_6(\lambda z + c)^3.$$

The three solutions (of which we know two already), representing the three points on the line, have z-coordinates whose sum is the z^2 term of the cubic divided by the z^3 term, so the inverse of the sum of z_1 and z_2 is given by

$$i(F(z_1, z_2)) = \frac{a_1\lambda + a_2 c + a_3\lambda^2 + 2a_4\lambda c + 3a_6\lambda^2 c}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} - z_1 - z_2.$$

(Beware: I believe there is an error in Silverman's book here!)

This also lies in $\mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]]$ (this depends on the fact that λ has no constant term: we can expand the reciprocal of the denominator as a power series in z_1, z_2.)

But now we're done: we can iterate this construction to get

$$F(z_1, z_2) = -i(F(i(F(z_1, z_2)), 0)).$$

So at last we have that:

Proposition 11.2. *This gives a formal group law F.*

Proof. Clear from the construction. □

Following this calculation through, we get that the first few terms are

$$F(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) - \cdots .$$

11.2 Elliptic curves over the p-adics

In this section, we let E be an elliptic curve over $\mathbb{Q}_p$, specified by a generalised Weierstrass equation with coefficients $a_1, \ldots, a_6$ in $\mathbb{Z}_p \subset \mathbb{Q}_p$.

Examples of such things can be obtained, of course, by taking an elliptic curve over $\mathbb{Q}$ with coefficients in $\mathbb{Z}$ and performing a base change by the embedding $\mathbb{Q} \subset \mathbb{Q}_p$.

The operations done above use only integer operations, so we get a formal group law F for E over $\mathbb{Z}_p$ by the recipe above. The associated group structure is defined on $p\mathbb{Z}_p$ and is denoted $\hat{E}(p\mathbb{Z}_p)$. It is a p-adic Lie group.

The remainder of this lecture and the next is devoted to analysing the structure.

We start with a lemma:

Lemma 11.3. *Let $(x_0, y_0) \in E(\mathbb{Q}_p)$, and let $z_0 = -x_0/y_0$. The following are equivalent:*

1. $\mathrm{ord}_p(x_0) < 0$
2. $\mathrm{ord}_p(y_0) < 0$
3. $\mathrm{ord}_p(z_0) > 0$, *ie.* $z_0 \in p\mathbb{Z}_p$.

Proof. We'll demonstrate that (1) implies (2) and (3) and then that each of (2) and (3) imply (1).

- (1) $\Rightarrow$ (2), (3): Consider the generalised Weierstrass equation for E in the form:
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x \qquad (a_1, \ldots, a_6 \in \mathbb{Z}_p)$$
If $-r = \mathrm{ord}_p(x_0)$ then the right-hand-side has valuation $-3r$, and if $-s = \mathrm{ord}_p(y_0)$ then the left-hand-side has valuation $-2s$. The equality of these valuations says $2r = 3s$, so there is a $d > 0$ such that $r = 2d, s = 3d$. Thus $\mathrm{ord}_p(z_0) = \mathrm{ord}_p(x_0) - \mathrm{ord}_p(y_0) > 0$.
- (2) $\Rightarrow$ (3): Immediate from argument above.
- (3) $\Rightarrow$ (1): The inverse of our earlier coordinate change is $x = z/w$. We have a power series for w in terms of z:
$$w = z^3(1 + A_1z + a_2z^2 + \cdots)$$
and so we can express x in terms of z as
$$x = \frac{1}{z^2}\left(1 - (A_1z + A_2z^2 + \cdots) + (A_1z + A_2z^2 + \cdots) - \cdots\right).$$
We evaluate at $z = z_0$ to conclude.

□

Corollary 11.4. *Let $E_1(\mathbb{Q}_p)$ be defined by*
$$E_1(\mathbb{Q}_p) = \{0\} \cup \{(x_0, y_0) \in E(\mathbb{Q}_p) | \, \mathrm{ord}_p(x_0) < 0, \mathrm{ord}_p(y_0) < 0\}.$$
It is a subgroup of $E(\mathbb{Q}_p)$.

Proof. Need only to show that it is closed under addition. Pick two points $(x_1, y_1), (x_2, y_2) \in E_1(\mathbb{Q}_p)$. We may pass from (x_i, y_i) to $z_i = -x_i/y_i$, which by the lemma is in $p\mathbb{Z}_p$. Our results on the formal group law show that $F(z_1, z_2) \in p\mathbb{Z}_p$. By applying the lemma again, we conclude that $(x_1, y_1) \oplus (x_2, y_2) \in E_1(\mathbb{Q}_p)$. □

Finally, we get our promised interpretation of the p-adic formal group law:

Corollary 11.5. *The map $(x_0, y_0) \mapsto -x_0/y_0 = z_0$ defines an isomorphism of groups*

$$E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p).$$

Lecture 12

Points of finite order

Vladimir Dokchitser
23 / 02 / 2005

(Notes taken by James Cranch)

12.0 Motivation

We have proved the Mordell-Weil theorem in the case of an elliptic curve with a point of order 2, which says that $E(\mathbb{Q})$ is a finitely generated abelian group. It can thus be written as $E(\mathbb{Q}) = \Delta \times \mathbb{Z}^g$, where Δ is finite.

Zacky's lectures discussed how to find g, the Mordell-Weil rank of the elliptic curve. We are developing machinery now to find Δ.

To determine this, we will find it useful to pass to $\mathbb{Q}_p$. David Geraghty's lecture 3 provided some evidence that the structure of elliptic curves over complete fields is rich. Thus, now, E is an elliptic curve given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in \mathbb{Z}_p).$$

Last lecture, we introduced the subgroup $E_1(\mathbb{Q}_p)$ of $E(\mathbb{Q}_p)$ defined by

$$E_1(\mathbb{Q}_p) = \{(x, y) \in E(\mathbb{Q}_p) | \operatorname{ord}_p(x_0), \operatorname{ord}_p(y_0) < 0\},$$

in other words, it is a subgroup of points of $E(\mathbb{Q}_p)$ that are p-adically close to infinity.

We also saw last time that it is isomorphic to $\hat{E}(p\mathbb{Z}_p)$, the group associated to the formal group on the elliptic curve. This is just $p\mathbb{Z}_p$, but with a funny addition law $+_E$ given by $x +_E y = F(x, y)$ where F is a power series in $\mathbb{Z}_p[[X, Y]]$:

$$F(X, Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \text{higher order terms}.$$

Of course $E(\mathbb{Q}_p)$ is uncountable, so we can't expect to exhibit a finite presentation for it, or anything like that. We must be more subtle.

Recall that, associated to our other examples of formal group laws, the additive and multiplicative formal group laws, we had the following exact sequences:

$$0 \to \hat{\mathbb{G}}_a(p\mathbb{Z}_p) \cong p\mathbb{Z}_p \to \mathbb{Z}_p \to \mathbb{F}_p \to 0, \quad \text{and} \quad 0 \to \hat{\mathbb{G}}_m(p\mathbb{Z}_p) \cong (1+p\mathbb{Z}_p)^\times \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \to 0.$$

These can be interpreted as exact sequences characterising elements that are close to the identity in each of these formal groups.

Analogously, in good conditions, we will end up with the exact sequence

$$0 \to E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p) \to E(\mathbb{Q}_p) \to \tilde{E}(\mathbb{F}_p) \to 0,$$

where $\tilde{E}$ is some elliptic curve over $\mathbb{F}_p$. This will be unraveled over the next two lectures.

12.1 Points of finite order on $\hat{E}(p\mathbb{Z}_p)$.

Recall the multiplication-by-m map $[m] : \hat{E}(p\mathbb{Z}_p) \to \hat{E}(p\mathbb{Z}_p)$. This is given by a power series $[m](X) = mX + O(X^2)$.

We will start with

Lemma 12.1. *If $(m, p) = 1$ then $[m] : \hat{E}(p\mathbb{Z}_p) \to \hat{E}(p\mathbb{Z}_p)$ is injective.*

Proof. This is clear, since $\mathrm{ord}_p([m]x) = \mathrm{ord}_p(x)$. □

In many cases, we can get a lot more than that.

Lemma 12.2. *If $f(X) = aX + O(X^2)$ is a power series in $\mathbb{Z}_p[[X]]$ and $a \in \mathbb{Z}_p^\times$ is a unit, then there is a power series $g(X) \in \mathbb{Z}_p[[X]]$ such that $f(g(X)) = X$.*

Proof. Set $g_1(X) = a^{-1}X$. Note that $f(g(X)) = X + O(X^2)$. Having defined g_{n-1}, we inductively define

$$g_n(X) = g_{n-1}(X) + \lambda_n X^n,$$

for some λ_n yet to be chosen. We want that:

$$f(g_n(X)) = X + O(X^{n+1}).$$

This determines the value of λ_n we choose thus:

$$\begin{aligned} f(g_n(X)) &= f(g_{n-1}(X) + \lambda_n X^n) \\ &\equiv f(g_{n-1}(X)) + a\lambda_n X^n \pmod{X^{n+1}} \\ &\equiv X + bX^{n-1} + a\lambda_n X^n \pmod{X^{n+1}}, \end{aligned}$$

for some b, so we take $\lambda_n = -b/a$.

Set $g(X) = \lim g_n(X)$, observing that the limit exists, and note that $f(g(X)) = X$. □

Remark. Since it has a right inverse, this proves that f is surjective as a map on power series. As g is of the same form, it too is surjective.

Hence $g(f(X)) = X$; and so g and f are mutually inverse isomorphisms, and thus in particular g is unique.

Corollary 12.3. *If $(m, p) = 1$, then $[m] : \hat{E}(p\mathbb{Z}_p) \to \hat{E}(p\mathbb{Z}_p)$ is surjective, and thus an isomorphism (since we showed it injective earlier).*

Remark. This shows that $\hat{E}(p\mathbb{Z}_p)$ has no m-torsion for $(m, p) = 1$, and that every element is uniquely m-divisible.

Remark. The above proof works over any local field, and the condition becomes that m must be coprime to the residue characteristic.

Now, we present the key theorem of this lecture:

Theorem 12.4. *Suppose $E/\mathbb{Q}_p$ is an elliptic curve, given by*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (a_i \in \mathbb{Z}_p).$$

If $p = 2$, suppose also that $2|a_1$.

Then $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p)$ has no elements of order p.

Remark. This is false over more arbitrary local fields, such as algebraic extensions of $\mathbb{Q}_p$.

Proof. Make a change of variables:

$$y' = y + \frac{a_1}{2}x, \qquad x' = x.$$

This is, of course, where we use the assumption when $p = 2$.

We get

$$E' : y'^2 + a_3'y' = x'^3 + a_2'x'^2 + a_4'x' + a_6',$$

and $E_1(\mathbb{Q}_p)$ is taken isomorphically to $E_1'(\mathbb{Q}_p)$.

Thus we may suppress the awful prime notation, and just assume that $a_1 = 0$.

We recall the first few terms of the formal group law

$$F(X, Y) = X + Y - a_1XY - a_2(X^2Y + XY^2) + \cdots$$

and note that the XY term vanishes.

Now, if $x, y \in p^n\mathbb{Z}_p$ then

$$x +_{\mathcal{E}} y = F(x, y) \equiv x + y \pmod{p^{3n}\mathbb{Z}_p}$$

By repeated application of this, if $x \in p^n\mathbb{Z}_p$, then

$$[p](x) \equiv px \pmod{p^{3n}\mathbb{Z}_p}.$$

and thus if $x \neq 0$, and $\mathrm{ord}_p(x) = n$ then $\mathrm{ord}_p([p](x)) = n+1$ and thus $[p](x) \neq 0$. □

Corollary 12.5. *If $E/\mathbb{Q}$ is an elliptic curve, with coefficients a_i in $\mathbb{Z}$, and $2|a_1$, then $E_1(\mathbb{Q}_p)$ has no points of finite order for any p. In particular, then, any point of finite order on $E(\mathbb{Q})$ has integer coordinates.*

Remark. The theorem is also true over any unramified extension of $\mathbb{Q}_p$, for the same reasons, but is dramatically false otherwise.

Remark. It is possible to prove that $[p] : \hat{E}(p\mathbb{Z}_p) \to \hat{E}(p\mathbb{Z}_p)$ can be expressed as $[p](X) = pf(X) + g(X^p)$ for $f, g \in \mathbb{Z}_p[[X]]$, or equivalently that

$$\frac{d}{dX}[p](X) \equiv 0 \pmod{p}.$$

Lecture 13

Minimal Weierstrass Equations

Mahesh Kakde
25 / 02 / 2005

Let E be an elliptic curve over $\mathbb{Q}$ given by the Generalised Weierstrass Equation (GWE)

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Under the change of variables $x = u^2x'$ and $y = u^3y'$, the coefficients get changed as follows:

$$u^ia_i' = a_i \quad \text{for} \quad i = 1, 2, 3, 4, 6.$$

Hence E can be defined by a GWE over $\mathbb{Z}$. The advantage of having a GWE over $\mathbb{Z}$ is that we can reduce the coefficients mod some prime p and obtain a GWE over the finite field $\mathbb{F}_p$. Reducing mod p is a subtle business since it depends on the choice of the equation defining the given curve E: two equations with coefficients in $\mathbb{Z}$ may define curves which are isomorphic over $\mathbb{Q}$ but whose reductions mod p are not isomorphic as curves over $\mathbb{F}_p$.

Example: Consider $E : y^2 = x^3 - 432$. The discriminant $\Delta(E) = -2^{12}3^9$. So the plane cubic curve $\tilde{E}_2 : y^2 = x^3$ obtained by reducing mod 2 has discriminant 0 in $\mathbb{F}_2$ and hence is singular. However after making the change of variables $x = 4x'$ and $y = 8y' - 4$ we get an isomorphic curve $E' : y'^2 - y' = x'^3 - 7$ with discriminant $\Delta(E') = -3^9$. Hence its reduction mod 2 gives a nonsingular plane cubic curve.

The problem here is that the first equation defining E is not a "Minimal Weierstrass Equation" at 2.

Definition 13.1. *Let $E/\mathbb{Q}_p$ be an elliptic curve. A GWE defining E is said to be a Minimal Weierstrass Equation (MWE) at p if $ord_p(\Delta)$ is minimum among all the GWE's defining E subject to the condition that all the coefficients are in $\mathbb{Z}_p$. If Δ is the discriminant of a minimal Weierstrass equation then $ord_p(\Delta)$ is the valuation of minimal discriminant.*

Remark: The existence of a MWE is obvious. And we have the following uniqueness theorem.

Theorem 13.2. *A MWE is unique up to the following change of variables: $x = u^2x' + r$ and $y = u^3y' + u^2sx' + t$, where $u \in \mathbb{Z}_p^\times$, $r, s, t \in \mathbb{Z}_p$.*

Proof. : Since $\Delta = u^{12}\Delta'$ and $ord_p(\Delta) = ord_p(\Delta')$, $u \in \mathbb{Z}_p^\times$. Transformation for b_6 and b_8 gives that $4r^3$ and $3r^4$ are in $\mathbb{Z}_p$. Hence r is in $\mathbb{Z}_p$. Now Transformation for a_2 gives $s \in \mathbb{Z}_p$ and transformation for a_6 gives $t \in \mathbb{Z}_p$. □

Hence the curve obtained obtained by reducing the coefficients of a MWE is unique up to the standard change of variables over $\mathbb{F}_p$ (i.e. $x = u^2x' + r$ and $y = u^3y' + u^2sx' + t$).

13.1 Criteria for minimality

For the standard change of variables $\Delta = u^{12}\Delta'$, i.e. valuation of the discriminant changes by multiples of 12. Similarly it can be checked that valuation of c_4 and c_6 change by multiples of 4 and 6 respectively.

Proposition 13.3. *A GW E defining $E/\mathbb{Q}_p$ with coefficients in $\mathbb{Z}_p$ is minimal if either of the following two conditions holds:*

1. $ord_p(\Delta) < 12$
2. $ord_p(c_4) < 4$ *(which one easily checks is equivalent to $ord_p(c_6) < 6$).*

Proof. Clear from above discussion. □

Remark. If $p \neq 2, 3$ then it is an easy exercise to check that the converse is true. If $p = 2$ then the following example shows that the converse need not be true (if I did not make any mistake): $y^2 = x^3 + 3x^2 - 16x$.

Thus we can canonically reduce an elliptic curve $E/\mathbb{Q}_p$ to a cubic curve over $\tilde{E}_p$ defined over $\mathbb{F}_p$ (I will drop the subscript p whenever there is no ambiguity, which usually arises when we are considering $E/\mathbb{Q}$ as an elliptic curves over $\mathbb{Q}_p$ for various p's and then reducing them mod p). This curve need not be nonsingular in general. If it is then we say that E has a **good reduction at** p. Else we say that E has **bad reduction at** p. Clearly E has good reduction at p if and only if the valuation of minimal discriminant is 0.

13.2 Reduction mod p on points

Let $\sim$ denote the natural surjection $\mathbb{Z}_p \to \mathbb{F}_p$. We define the reduction mod p map $\mathbb{P}^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p)$ as follows. Take a point $(X : Y : Z)$ in $\mathbb{P}^2(\mathbb{Q}_p)$ and scale it so that all the coordinates are in $\mathbb{Z}_p$ and at least one of them is in $\mathbb{Z}_p^\times$. Then map $(X : Y : Z)$ to $(\tilde{X} : \tilde{Y} : \tilde{Z})$. This gives a well defined map, again denoted by $\sim$, from $\mathbb{P}^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p)$.

Let $E/\mathbb{Q}_p$ be an elliptic curve defined by the MWE $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ and let $\tilde{E}$ be the curve obtained by reduction mod p given by the equation $y^2 + \tilde{a_1}xy + \tilde{a_2}y = x^3 + \tilde{a_2}x^2 + \tilde{a_4}x + \tilde{a_6}$. Clearly, $\sim$: $P^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p)$ maps $E(\mathbb{Q}_p)$ into $\tilde{E}(\mathbb{F}_p)$.

Let E have good reduction at p. Hence $\tilde{E}$ is an elliptic curve over $\mathbb{F}_p$. Recall,

$$\begin{aligned} E_1(\mathbb{Q}_p) &= \{P = (x,y) \in E(\mathbb{Q}_p) : ord_p(x) < 0\} \cup \{O\} \\ &= \{P = (x,y) \in E(\mathbb{Q}_p) : ord_p(y) < 0\} \cup \{O\} \\ &= \{P = (x,y) \in E(\mathbb{Q}_p) : ord_p(x/y) > 0\} \cup \{O\}. \end{aligned}$$

Hence $E_1(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : \tilde{P} = \tilde{O}\}$, where $\tilde{O}$ is the identity of $\tilde{E}(\mathbb{F}_p)$.

Proposition 13.4. *Let $E/\mathbb{Q}_p$ be an elliptic curve with good reduction at p. Then we get the following short exact sequence of abelian groups:*

$$0 \to E_1(\mathbb{Q}_p) \longrightarrow E(\mathbb{Q}_p) \longrightarrow \tilde{E}(\mathbb{F}_p) \to 0$$

where the map on the right is the reduction mod p map $\sim$.

Proof. Since $\sim$: $\mathbb{P}^2(\mathbb{Q}_p) \to \mathbb{P}^2(\mathbb{F}_p)$ takes lines to lines the map on the right is a group homomorphism. Now the map on the left is just the kernel of this homomorphism. So it only remains to prove that $\sim$ is surjective. Let $f(x,y)$ be the difference of the two sides of the MWE defining E. Then

$$((\partial/\partial x)\tilde{f}(\alpha,\beta), (\partial/\partial y)\tilde{f}(\alpha,\beta)) \neq 0$$

for any (α,β) such that $\tilde{f}(\alpha,\beta) = 0$. Suppose $(\partial/\partial x)\tilde{f}(\alpha,\beta) \neq 0$; then choose any $y_0 \in \mathbb{Z}_p$ such that $\tilde{y_0} = \beta$ and solve the equation $f(x,y_0) = 0$ using Hensel's Lemma. The case where $\partial\tilde{f}/\partial y \neq 0$ is similar. □

Application Let $E/\mathbb{Q}_p$ have good reduction at p. Recall that $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p)$ and $\hat{E}(p\mathbb{Z}_p)$ does not have any torsion points (if $p = 2$, then under the hypothesis that $a_1 \in 2\mathbb{Z}_2$). Hence (under the same hypothesis) $E_1(\mathbb{Q}_p)$ does not have any torsion points. So we conclude from the from the short exact sequence in the proposition that torsion subgroup $\Delta(E)$ of $E(\mathbb{Q}_p)$ injects in $\tilde{E}(\mathbb{F}_p)$. This gives a quick method for finding the torsion subgroup of elliptic curves defined over $\mathbb{Q}$ (which we know by Mordell-Weil to be finite).

Examples

1. $E : y^2 + y = x^3 - x + 1$. Discriminant $\Delta = -13.47$. So the equation is a MWE and E has good reduction at 2. One can check by hand that $\tilde{E}(\mathbb{F}_2)$ is trivial. Since $a_1 = 0$, we conclude that the torsion subgroup of $E(\mathbb{Q})$ is trivial.
2. $E : y^2 = x^3 + 3$. Its discriminant is $\Delta = -3^5 2^4$. So the equation is a MWE. E has good reduction at all $p \geq 5$ and $|\tilde{E}(\mathbb{F}_5)| = 6$ and $|\tilde{E}(\mathbb{F}_7)| = 13$. Hence the torsion subgroup of $E(\mathbb{Q})$ is trivial.
3. Sometimes we need to find the structure of the group $\tilde{E}(\mathbb{F}_p)$ – just knowing the order is not enough. Consider $E : y^2 = x^3 + x$. It has discriminant $\Delta = -64$. $(0,0) \in E(\mathbb{Q})$ is a point of order 2. $\tilde{E}(\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z}$, while $\tilde{E}(\mathbb{F}_5) \cong (\mathbb{Z}/2\mathbb{Z})^2$, hence the torsion subgroup of $E(\mathbb{Q})$ is $\mathbb{Z}/2\mathbb{Z}$. (Exercise: 4 divides the order of $\tilde{E}(\mathbb{F}_p)$ for all $p \geq 3$).

Lecture 14

Reduction mod p II and torsion points over algebraic extensions

David Loeffler
28 / 02 / 2005

We shall now change tack slightly; having seen how to determine the m-torsion points over $\mathbb{Q}$, we shall now consider the effect of extending the base field by adjoining points of finite order in the quotient $E(\overline{\mathbb{Q}})/E(\mathbb{Q})$.

Recall from lecture 9 that the maximal unramified extension of $\mathbb{Q}_p$ is denoted by $\mathbb{Q}_p^{nr}$. We shall also occasionally use the notation $\mathbb{Q}(R)$, where $R \in E(\overline{\mathbb{Q}})$, to mean the field generated over $\mathbb{Q}$ by the coordinates of R. For A an abelian group, A_m is the m-torsion subgroup (the kernel of multiplication by m)

We shall initially consider this problem locally, before passing to the global case.

Theorem 14.1. *Let $E/\mathbb{Q}_p$ be an elliptic curve with good reduction at p, and $m \in \mathbb{N}$ with $(m, p) = 1$.*

1. *There are isomorphisms*

$$\begin{array}{ccc} E(\mathbb{Q}_p)_m & \xrightarrow{\sim} & \tilde{E}_p(\mathbb{F}_p)_m \\ \dfrac{E(\mathbb{Q}_p)}{mE(\mathbb{Q}_p)} & \xrightarrow{\sim} & \dfrac{\tilde{E}_p(\mathbb{F}_p)}{m\tilde{E}_p(\mathbb{F}_p)} \end{array}$$

2. *If $R \in E(\overline{\mathbb{Q}_p})$ is such that $mR \in E(\mathbb{Q}_p)$, then $\mathbb{Q}_p(R)/\mathbb{Q}_p$ is unramified.*

3. *The group $E(\mathbb{Q}_p^{nr})$ is m-divisible, and contains $E(\overline{\mathbb{Q}_p})_m$.*

Proof.

(1) Recall that the group $E_1(\mathbb{Q}_p)$ which is the kernel of the reduction-mod-p map is torsion-free and m-divisible. A very tidy proof can be obtained by using the Snake Lemma on the diagram obtained by applying the map $[m]$ to every term of the exact sequence $0 \to E_1(\mathbb{Q}_p) \to E(\mathbb{Q}_p) \to \tilde{E}_p(\mathbb{F}_p) \to 0$. However, using something as powerful as the Snake Lemma here is rather unsporting, so we shall prove the result directly.

Let α and β be the maps on the two groups mentioned, arising from reduction mod p on points; it is clear that both are well-defined, since the reduction of an m-torsion point is certainly an m-torsion point.

In the first case, α is clearly injective since E_1 is torsion-free. But if $\tilde{P}$ is a point of $E_p(\mathbb{F}_p)_m$, arising as the reduction of some $P \in E(\mathbb{Q}_p)$, then we must have $mP \in E_1$. As E_1 is m-divisible, we can write $mP = mT$ for some $T \in E_1$; hence $P - T \in E(\mathbb{Q}_p)_m$. But $\alpha(P - T) = \tilde{P} - \tilde{T} = \tilde{P}$, so α is surjective.

In the second case it is the surjectivity that is obvious; so we must prove the injectivity. Let P be a point such that $\tilde{P} \in mE_p(\mathbb{F}_p)$; we must show $P \in mE(\mathbb{Q}_p)$. However, if $\tilde{P} = m\tilde{Q}$, then $P - mQ \in E_1$, so as before $P - mQ = mT$ and $P = m(Q + T) \in mE(\mathbb{Q}_p)$ as required.

(3) (We shall prove this first, then deduce 2.) In the above result, we may freely replace $\mathbb{Q}_p$ and $\mathbb{F}_p$ by any finite unramified extension and its residue field; passing to the inductive limit over all such fields, we obtain

$$\begin{array}{ccc} E(\mathbb{Q}_p^{nr})_m & \xrightarrow{\sim} & \tilde{E}_p(\overline{\mathbb{F}_p})_m \\ \dfrac{E(\mathbb{Q}_p^{nr})}{mE(\mathbb{Q}_p^{nr})} & \xrightarrow{\sim} & \dfrac{\tilde{E}_p(\overline{\mathbb{F}_p})}{m\tilde{E}_p(\overline{\mathbb{F}_p})} \end{array}$$

However, we can identify both of these groups. It will follow from our study of isogenies in the next lecture that the map $[m]$ is a non-constant separable morphism of degree m^2 on the irreducible curve $\tilde{E}_p$ over the algebraically closed field $\overline{\mathbb{F}_p}$; so by the Finiteness Theorem of algebraic geometry, it is surjective (the second group is trivial) and the first group (its kernel) has order m^2. But there cannot be more than m^2 points in $E(\overline{\mathbb{Q}_p})_m$, so $E(\overline{\mathbb{Q}_p})_m = E(\mathbb{Q}_p^{nr})_m$.

(2) By part (3) we know that there is some $R' \in E(\mathbb{Q}_p^{nr})$ such that $mR' = P$, since $E(\mathbb{Q}_p^{nr})$ is an m-divisible group. However, we then have $m(R' - R) = 0$, so $S = R - R' \in E(\overline{\mathbb{Q}_p})_m$; from the second part of (3), $S \in E(\mathbb{Q}_p^{nr})$, so $R = R' + S \in E(\mathbb{Q}_p^{nr})$. □

Now, we return to the case of number fields. Suppose $R \in E(\overline{\mathbb{Q}})$ is an m-division point – that is, $mR \in E(\mathbb{Q})$. The remarks on algebraic extensions of $\mathbb{Q}_p$ in lecture 9 imply:

Corollary 14.2. *Let S be the set of primes where E has bad reduction. Then the field extension $\mathbb{Q}(R)/\mathbb{Q}$ is unramified except in S and at the primes dividing m.*

This is a fairly stringent condition to place on the extension $\mathbb{Q}(R)/\mathbb{Q}$. We also have another condition, and the two between them are sufficient to pin down the field $\mathbb{Q}(R)$ to one of a finite set of extensions.

Lemma 14.3. $[\mathbb{Q}(R) : \mathbb{Q}] \leq m^2$.

Proof. Suppose $P = mR \in E(\mathbb{Q})$. Then there are at most m^2 points R' such that $mR' = P$, since the difference between any two is an m-torsion point, and $|E(\overline{\mathbb{Q}})_m| = m^2$ (either by the algebraic-geometry methods above, or by identifying E with the quotient of $\mathbb{C}$ with a certain lattice). However, any embedding

$\sigma : \mathbb{Q}(R) \hookrightarrow \overline{\mathbb{Q}}$ must map R to one of these m^2 points, and it is determined by the image of R. Since there are exactly $[\mathbb{Q}(R) : \mathbb{Q}]$ such embeddings, the result follows. □

Theorem 14.4 (Hermite). *For any finite set T of primes and any $n \in \mathbb{N}$, there are only finitely many extensions of $\mathbb{Q}$ which are unramified outside T and have degree at most n.*

We now consider the extension obtained by adjoining *all* m-division points.

Corollary 14.5. *Let $L = \mathbb{Q}\left[\left\{R \in E(\overline{\mathbb{Q}}) \ : \ mR \in E(\mathbb{Q})\right\}\right]$. Then L is a finite extension of $\mathbb{Q}$, unramified outside S and the primes dividing m.*

Proof. The only statement requiring proof is that $[L : \mathbb{Q}]$ is finite; but the previous two results imply that every m-division point is defined over one of a finite set of extensions, so we may take L to be their composite, which is therefore finite. □

Remark. This result is immediate from Mordell-Weil, without using Hermite's result, since we need only use a finite set of points (the m-torsion points and one m-division point of each of some finite set of generators); but we will in fact use this result in proving the general case of Mordell-Weil.

Lecture 15

Isogenies

Bjarki Holm
02 / 03 / 2005

(Notes taken by James Cranch)

15.1 Introduction

We begin with the key definition.

Definition 15.1. *Let K be algebraically closed and perfect*[1]*. Let E_1 and E_2 be elliptic curves over K, with base points 0_1 and 0_2. An **isogeny** between E_1 and E_2 is a morphism*

$$\phi : E_1 \longrightarrow E_2$$

*of varieties such that $\phi(0_1) = 0_2$. We say that E_1 and E_2 are **isogenous** if there exists an isogeny between them with $\phi(E_1) \neq \{0_2\}$.*

Note that any rational map $E_1 \dashrightarrow E_2$ is a morphism.

If L is a subfield of K and E_1 and E_2 are defined over L, then a morphism ϕ is defined over L if it is given by homogeneous polynomials with coefficients on L.

Definition 15.2. *The **coordinate ring** of an elliptic curve over K is given by*

$$K[E] = K[X, Y]/(y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6).$$

*The **function field** is defined to be the field of fractions of $K[E]$:*

$$K(E) = \operatorname{Frac} K[E].$$

Remark. Giving an isogeny $\phi : E_1 \to E_2$ is equivalent to giving an element of $E_2(K(E_1))$.

15.2 Isogenies are surjective

Proposition 15.3. *Let K be algebraically closed and perfect, and let E_1 and E_2 be defined over K, with $\phi : E_1 \to E_2$ a non-constant isogeny. Then $\phi(E_1(K)) = E_2(K)$, or in other words ϕ is surjective.*

[1] A field is **perfect** if all its finite extensions are separable, or equivalently if it has characteristic 0 or has characteristic p and contains the p-th powers of every element.

Proof. This follows immediately from the general statement, from elementary algebraic geometry, that a morphism $\phi : C_1 \to C_2$ of curves is either constant or surjective. □

Now let $\phi : E_1 \to E_2$ be a non-constant isogeny defined over K. Then composition with ϕ induces an injection of function fields:

$$\begin{array}{rcl} \phi^* K(E_2) & \longrightarrow & K(E_1) \\ f & \longmapsto & f \circ \phi \end{array}$$

Since $K(E_1) \subseteq \phi^*(K(E_2))$ and both $K(E_1)$ and $K(E_2)$ have transcendence degree 1 over K, and are finitely generated extensions of K, we get that $K(E_1)$ is a finite algebraic extension of $\phi^*(K(E_2))$; in symbols, $[K(E_1) : \phi^*(K(E_2))] < \infty$.

Definition 15.4. *We say that ϕ is **separable** if the extension $K(E_1)/\phi^*(K(E_2))$ is separable, and we denote the degrees by:*

$$\begin{array}{rcll} \deg(\phi) & = & [K(E_1) : \phi^*(K(E_2))], & \textit{the } \textbf{\textit{degree}}; \\ \deg_s(\phi) & = & [K(E_1) : \phi^*(K(E_2))]_s, & \textit{the } \textbf{\textit{separable degree}}; \\ \deg_i(\phi) & = & [K(E_1) : \phi^*(K(E_2))]_i, & \textit{the } \textbf{\textit{inseparable degree}}; \end{array}$$

In the above, the separable degree $[L : K]_s$ of a field extension L/K is the degree $[K' : K]$ of the maximal subfield K' of L that is separable over K. With the same notation, the inseparable degree $[L : K]_i$ is the degree $[L : K']$.

15.3 Isogenies are group homomorphisms

Since we have established group laws for elliptic curves, we might suspect that isogenies are in fact group homomorphisms.

Theorem 15.5. *An isogeny $\phi : E_1 \to E_2$ is a group homomorphism, ie. $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$.*

Proof. This is obvious if ϕ is the constant map: $\phi(E_1) = 0_2$. Thus we assume ϕ is non-constant, and thus a finite map. We now introduce some tools from elementary algebraic geometry.

Definition 15.6. *A finite formal linear combination of points $D = \sum_{P \in E} n_P(P)$ on a curve E is called a **divisor**. If D has the form $D = \operatorname{div}(f) = \sum_{P \in E} \operatorname{ord}_P(f)(P)$ for some $f \in \bar{K}(E)^\times$, then it is said to be **principal**.*

*We set the **degree** to be $\deg(D) = \sum_{P \in E} n_P$, and let $\mathrm{Div}^0(E)$ be the group of divisors of degree zero under pointwise addition. Note that a principal divisor always has degree zero.*

*The **(reduced) Picard group** or **divisor class group** is then defined to be the quotient of $\mathrm{Div}^0(E)$ by the subgroup of principal divisors.*

We now state without proof a few standard results from algebraic geometry:

1. ϕ induces a homomorphism

$$\phi_* : \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2)$$

by sending the divisor $\sum_{P \in E_1} n_P(P)$ to $\sum_{P \in E_1} n_P(\phi(P))$.

2. We have group isomorphisms

$$\begin{aligned} \kappa_i : E_i &\longrightarrow \mathrm{Pic}^0(E_1) \\ P &\longmapsto \text{class of } (P) - (O_i) \end{aligned}$$

for $i = 1, 2$.

Now, since $\phi(0_1) = 0_2$, we get a commutative diagram:

$$\begin{array}{ccc} E_1 & \xrightarrow[\kappa_1]{\sim} & \mathrm{Pic}^0(E_1) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_*} \\ E_2 & \xrightarrow[\kappa_2]{\sim} & \mathrm{Pic}^0(E_2) \end{array}$$

Since κ_1, κ_2^{-1} and ϕ_* are group homomorphisms, we may read off at once that ϕ is too. □

Remark. Analogous to the fundamental exact sequence from class field theory is the exact sequence

$$0 \longrightarrow \bar{K}^\times \longrightarrow \bar{K}(E)^\times \longrightarrow \mathrm{Div}^0(E) \longrightarrow \mathrm{Pic}^0(E) \longrightarrow 0.$$

15.4 Isogenies have finite kernels

The following is a fact from algebraic geometry: if $\phi : E_1 \to E_2$ is a non-constant rational map, then for every $Q \in E_2(K)$, the cardinality of $\phi^{-1}(Q)$ is finite, and for all but finitely many $Q \in E_2(K)$, we have $\#(\phi^{-1}(Q)) = \deg_s(\phi)$.

Lemma 15.7. *If $\phi : E_1 \to E_2$ is a non-constant isogeny over an algebraically closed field K, then $\#(\phi^{-1}(Q)) = \deg_s(\phi)$ for all $Q \in E_2(K)$.*

Proof. From above, $\#(\phi^{-1}(Q)) = \deg_s(\phi)$ for almost all $Q \in E_2$. But for any $Q, Q' \in E_2$, if we choose some $R \in E_1$ with $\phi(R) = Q' - Q$, then the fact that ϕ is a homomorphism implies a one-to-one correspondence:

$$\begin{aligned} \phi^{-1}(Q) &\longleftrightarrow \phi^{-1}(Q') \\ P &\longmapsto P \oplus R. \end{aligned}$$

Thus $\#(\phi^{-1}(Q))$ is the same for all $Q \in E_2$, and the result follows. □

Corollary 15.8. *This implies $\ker(\phi)$ is finite, and has order $\deg_s(\phi)$.*

15.5 Quotients of elliptic curves

Proposition 15.9. *Let E be an elliptic curve and let Φ be a finite subgroup of E. Then there is a unique elliptic curve $E' = E/\Phi$ and a separable isogeny $\phi : E \to E'$, such that $\ker(\phi) = \Phi$.*

Proof. Omitted. □

Remark. Suppose that E is defined over some subfield L of K; let $\bar{K}$ be the separable closure of L in K. If ϕ is $\mathrm{Gal}(\bar{K}/L)$-invariant (ie. for all $P \in \Phi$ and all $\sigma \in \mathrm{Gal}(\bar{K}/L)$, $\sigma P \in \Phi$). Then we can find E' and ϕ as above, defined over L (see Silverman, p.79). Moreover, the points of E' are set-theoretically the quotient of those of E by ϕ.

15.6 Complex multiplication

Definition 15.10. *If E_1 and E_2 are two elliptic curves, then we define the **group of isogenies** to be*

$$\mathrm{Hom}(E_1, E_2) = \{\textit{isogenies } E_1 \to E_2\}.$$

It is a group under pointwise addition.

*If E is an elliptic curve, we define the **endomorphism ring** of E to be*

$$\mathrm{End}(E) = \mathrm{Hom}(E, E).$$

It is a ring with multiplication given by composition.

There is an inclusion of $\mathbb{Z}$ into $\mathrm{End}(E)$ given by $m \mapsto [m]_E$ (the multiplication-by-m map).

Definition 15.11. *We say E has **complex multiplication** if $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$.*

Example. *Suppose $\mathrm{char}(K) \neq 2$ and $K = \bar{K}$, and let E/K be the elliptic curve*

$$E : y^2 = x^3 - x.$$

Then, in addition to this copy of $\mathbb{Z}$, $\mathrm{End}(E)$ contains an element $[i]_E$ with $i^2 = -1$, given by

$$[i]_E : (x, y) \longmapsto (-x, iy).$$

This defines an embedding $\mathbb{Z}[i] \hookrightarrow \mathrm{End}(E)$. In fact, if $\mathrm{char}(K) = 0$ then this is all:

$$\mathrm{End}(E) \cong \mathbb{Z}[i], \qquad \textit{via} \quad m + ni \mapsto [m]_E + ([n]_E \circ [i]_E).$$

Here are the basic properties of the group of isogenies and the endomorphism ring in general:

Proposition 15.12. *$\mathrm{Hom}(E_1, E_2)$ is torsion-free (since $[m]$ is never zero for $m \neq 0$). Thus, in particular, the map $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ is indeed injective.*

Proof. Suppose ϕ is a nonzero torsion element of order m. Then $[m] \circ \phi = [0]$. But taking degrees,

$$(\deg[m])(\deg \phi) = 0.$$

Since $[m]$ is non-constant, both degrees on the left hand side are positive: a contradition. □

Proposition 15.13. *$\mathrm{End}(E)$ has no zero divisors.*

Proof. As above, if $\phi \circ \psi = [0]$, then

$$(\deg \phi)(\deg \psi) = 0,$$

so one of the factors is the zero map. □

Proposition 15.14.

$$\mathrm{rank}_{\mathbb{Z}}(\mathrm{End}(E)) \leq 4.$$

Proof. Omitted. (It is hard). □

Example. *If* $\mathrm{char}(K) \equiv 3 \pmod 4$ *then equality may be achieved.*

Lecture 16

Dual isogenies and the structure of the torsion subgroup

Cornelius Probst
04 / 03 / 2005

16.1 Introduction

Some lectures ago, we tried to determine

$$\Delta(\mathbb{Q}) = E_{\text{tors}}(\mathbb{Q}) = \bigcup_m E_m(\mathbb{Q})$$

in

$$E(\mathbb{Q}) = \Delta \times \mathbb{Z}^{\text{rank}(E)}$$

Our approach was to look at $E\big(\mathbb{Q}_p\big)$. Provided $\big(E/\mathbb{Q}_p\big)$ has good reduction, we found an injection $E_m\big(\mathbb{Q}_p\big) \hookrightarrow \widetilde{E}_m\big(\mathbb{F}_p\big)$. Assuming again good reduction, we then stated results like

$$E_m\big(\overline{\mathbb{Q}_p}\big) = E_m\big(\mathbb{Q}_p^{nr}\big) \simeq \widetilde{E}_m\big(\overline{\mathbb{F}_p}\big) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z},$$

this time provided that $(m, p) = 1$.

For the proof, we needed the fact that multiplication by m has degree m^2. We didn't show $\widetilde{E}_m\big(\overline{\mathbb{F}_p}\big) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ either.

The main objective of this lecture is to complete these proofs. We achieve this by introducing the *dual isogeny*.

16.2 Revision of last lecture

(R1) We defined $\text{Hom}(E_1, E_2) := \{\text{isogenies } \varphi : E_1 \to E_2\}$

(R2) We defined the degree of an isogeny as

$$\begin{aligned} \deg\colon \text{Hom}(E_1, E_2) &\longrightarrow \mathbb{Z} \\ \varphi &\mapsto \big[K(E_1) : \varphi^*\left(K(E_2)\right)\big] \end{aligned}$$

(R3) An isogeny respects the group structure of $E(K)$, i.e. is a group homomorphism.

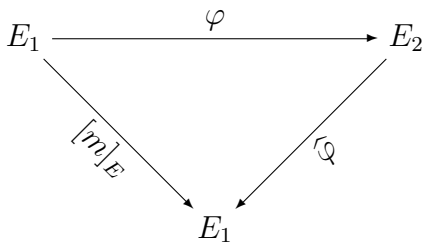
(R4) We proved: If $\varphi : E_1 \longrightarrow E_2$ is an isogeny of elliptic curves, then for all $Q \in \mathrm{E}_2$:

$$\left|\varphi^{-1}(Q)\right| = \deg_{\mathrm{s}}(\varphi)$$

(R5) We found that $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ via the $[m]$-map, and that $\mathrm{End}(E)$ has neither torsion as an additive group nor zero divisors.

16.3 The dual isogeny and deg[m]

Theorem 16.1. *Given a non-constant isogeny $\varphi : E_1 \to E_2$ of degree m, there exists a unique isogeny $\widehat{\varphi} : E_1 \to E_2$ such that $\widehat{\varphi} \circ \varphi = [m]_E$; hence the following diagram commutes:*



Proof. We omit existence. The proof for this uses advanced algebraic geometry and can be found in Silverman, III, 6, Thm. 6.1.
To show uniqueness, assume that $\widehat{\varphi}_1$ and $\widehat{\varphi}_2$ both satisfy the above condition. We then have

$$\widehat{\varphi}_1 \circ \varphi = [m]_E = \widehat{\varphi}_2 \circ \varphi,$$

which implies

$$[0] = \widehat{\varphi}_1 \circ \varphi - \widehat{\varphi}_2 \circ \varphi = (\widehat{\varphi}_1 - \widehat{\varphi}_2) \circ \varphi.$$

As φ is assumed to be non-constant, we conclude that $\widehat{\varphi}_1 - \widehat{\varphi}_2 = [0]$, which finally forces the desired equality $\widehat{\varphi}_1 = \widehat{\varphi}_2$. □

Definition 16.2 (The dual isogeny). *Let $\varphi : E_1 \to E_2$ be an isogeny. The* dual isogeny to φ *is the isogeny $\widehat{\varphi} : E_2 \to E_1$ given by the above theorem. If $\varphi = [0]$, we set $\widehat{\varphi} = [0]$.*

Theorem 16.3 (Properties of the dual isogeny).

(a) $\varphi \circ \widehat{\varphi} = [m]_{E'}$

(b) Let $\lambda : E_2 \to E_3$ be another isogeny and $n := deg(\lambda)$, so that we have

$$E_1 \xrightarrow{\varphi} E_2 \xrightarrow{\lambda} E_3.$$

Then taking

$$E_1 \xleftarrow{\widehat{\varphi}} E_2 \xleftarrow{\widehat{\lambda}} E_3$$

gives the dual isogeny, hence $\widehat{\lambda \circ \varphi} = \widehat{\varphi} \circ \widehat{\lambda}$.

(c) Let $\psi : E_1 \to E_2$ be another isogeny. Then $\widehat{\varphi + \psi} = \widehat{\psi} + \widehat{\varphi}$

(d) For all $m \in \mathbb{Z}$, we have $\widehat{[m]} = [m]$ and $deg[m] = m^2$.

(e) $deg(\widehat{\varphi}) = deg(\varphi)$

(f) $\widehat{\widehat{\varphi}} = \varphi$

Proof.

(a) The diagram

$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi} & E_2 \\ {\scriptstyle [m]}\downarrow & & \downarrow{\scriptstyle [m]} \\ E_1 & \xrightarrow{\varphi} & E_2 \end{array}$$

commutes because of (R3). In particular, $\varphi \circ [m]_{E_1} = [m]_{E_2} \circ \varphi$.

(b) We note that $\left(\widehat{\varphi} \circ \widehat{\lambda}\right) \circ (\lambda \circ \varphi) = \widehat{\varphi} \circ \left(\widehat{\lambda} \circ \lambda\right) \circ \varphi = \widehat{\varphi} \circ [n]_{E_2} \circ \varphi \underset{(R3)}{=} \widehat{\varphi} \circ \varphi \circ [n]_{E_1} = [m]_{E_1} \circ [n]_{E_1} = [mn]_{E_1}$. Now apply the uniqueness of $\widehat{\lambda \circ \varphi}$.

(c) Omitted. As usual, the reference is Silverman (III, 6, Thm. 6.2).

(d) The *first statement* is true for $i = 0; 1$. Using the above result, we obtain by induction:

$$\widehat{[i+1]} = \widehat{[i]} + \widehat{[1]} = [i] + [1] = [i+1]$$

for all $i \in \mathbb{N}$. Using $\widehat{[-1]} = [1]$ and (b), we get the result for all $i \in \mathbb{N}$:

$$\widehat{[-i]} = -\widehat{[i]} = \widehat{[-1]} \circ [i] = [i].$$

To show the *second statement*, let $d := \deg[m]$. Then one sees immediately

$$[d] = \widehat{[m]}[m] = [m^2],$$

which implies $d = m^2$ because of (R5). We remark that there is an elementary, but "highly computational" proof for the latter statement. See Silverman, Exercise 3.7 for details.

(e) Again, let $d := \deg[m]$. Then, using (d):

$$\left[m^2\right] = \left[\deg[m]\right] = \left[\deg\widehat{\varphi} \circ \varphi\right] = \left[\deg\widehat{\varphi} \cdot \deg\varphi\right] = \left[m \cdot (\deg\widehat{\varphi})\right]$$

(f) Once more, let $d := \deg[m]$. We then note:

$$\widehat{\varphi} \circ \varphi = [m] = \widehat{[m]} = \widehat{\widehat{\varphi} \circ \varphi} = \widehat{\varphi} \circ \widehat{\widehat{\varphi}}$$

□

16.4 The structure of the torsion subgroup

Theorem 16.4. *Let $m \in \mathbb{Z}$ and suppose $(m, \mathit{char}\ K) = 1$, if char $K \neq 0$. Then $[m]_E$ is a separable endomorphism.*

Proof. Consider the finite field extension:

$$\begin{array}{c} F := K(E) \\ \Big| \\ m^2 \\ \Big| \\ G := [m]_E^*\big(K(E)\big) \end{array}$$

Assume that $\alpha \in F$ is inseparable. Hence $f := \mathrm{mipo}_G(\alpha) \in G\big[t^p\big]$, where $p := \mathrm{char}(K)$. As $np := \deg(f)$ has to divide $\big[F : G\big] = m^2$, we get $p|m$. Contradiction. □

Corollary 16.5. *Suppose again $(m, \mathit{char}(K)) = 1$. Then*

$$E_m = \mathit{ker}\big([m]_E\big) \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Proof. As $[m]$ is separable, we have $\big|\ker[m]\big| = \big|[m]^{-1}(0)\big| \overset{(R4)}{=} \deg_s[m] = \deg[m] = m^2$. Similarly, we have $\big|E_d\big| = d^2$ for all $d|m$. So E_m is abelian, of exponent $\leq m$ and has order m^2. The structure theorem now tells us that $E_m \simeq \bigoplus_i \mathbb{Z}_{p_i^{n_i}}$. We may just look at the part with $p_i = p$, i.e. we assume $E_m \simeq \bigoplus_i \mathbb{Z}_{p^{n_i}}$ and $m = p^r$. We certainly have $n_i \leq r$, as E_m has exponent m. If $n_i < r$ for some i, then $(\alpha)^{p^{r-1}} = 0$ for at least $\big(p^{r-1} \cdot p^r\big)$ elements $\alpha \in E_m$, i.e. $\big|E_{p^{r-1}}\big| \geq p^{r-1}p^r > (p^{r-1})^2$. This contradicts our observation made above. So we have in fact $n_i = r$, which means $E_m \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. □

Lecture 17

Hasse's Theorem

David Geraghty
07 / 03 / 2005

Recall from earlier lectures:

1. If E_1 and E_2 are elliptic curves over a field k we defined the abelian group
$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } \phi : E_1 \to E_2\}$$
2. We defined a function
$$\begin{array}{rccl} \deg: & \mathrm{Hom}(E_1,E_2) & \longrightarrow & \mathbb{Z} \\ & \phi & \longmapsto & \begin{cases} [k(E_1) : \phi^* k(E_2)] & \text{if } \phi \neq 0; \\ 0 & \text{if } \phi = 0. \end{cases} \end{array}$$
Note that $\deg(\phi) > 0$ if $\phi \neq 0$.

Definition 17.1. *Let A be an abelian group. A function $q : A \to \mathbb{R}$ is a **positive definite quadratic form** on A if:*

1. $q(-a) = q(a)\ \forall a \in A$
2. *The map $A \times A \to \mathbb{R}$; $(a, b) \mapsto q(a + b) - q(a) - q(b)$ is bilinear*
3. $q(a) > 0$ *if* $a \neq 0$.

Lemma 17.2. *The function $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive definite quadratic form.*

Proof. We have to show that $\deg$ satisfies the conditions of the previous definition:

1. Observe that $-\phi = [-1]_{E_2} \circ \phi$. Taking degrees we get $\deg(-\phi) = \deg([-1]_{E_2}) \deg(\phi) = \deg(\phi)$.
2. Let $\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$. We need to show that $\langle \cdot, \cdot \rangle$ is bilinear. Recalling properties of the dual isogeny from the last lecture we have
$$\begin{aligned} [\langle \phi, \psi \rangle]_{E_1} &= [\deg(\phi + \psi)]_{E_1} - [\deg(\phi)]_{E_1} - [\deg(\psi)]_{E_1} \\ &= \widehat{(\phi + \psi)} \circ (\phi + \psi) - \widehat{\phi} \circ \phi - \widehat{\psi} \circ \psi \\ &= (\widehat{\phi} + \widehat{\psi}) \circ (\phi + \psi) - \widehat{\phi} \circ \phi - \widehat{\psi} \circ \psi \\ &= \widehat{\phi} \circ \psi + \widehat{\psi} \circ \phi \end{aligned}$$

which is certainly bilinear in ϕ and ψ. Hence for all $\phi_1, \phi_2 \in \mathrm{Hom}(E_1, E_2)$, we have

$$[\langle \phi_1 + \phi_2, \psi \rangle]_{E_1} = [\langle \phi_1, \psi \rangle]_{E_1} + [\langle \phi_2, \psi \rangle]_{E_1} = [\langle \phi_1, \psi \rangle + \langle \phi_2, \psi \rangle]_{E_1}$$

Recalling that $\mathbb{Z} \hookrightarrow \mathrm{End}(E_1)$, we deduce that

$$\langle \phi_1 + \phi_2, \psi \rangle = \langle \phi_1, \psi \rangle + \langle \phi_2, \psi \rangle.$$

Similarly we have linearity in the second variable.

3. We noted earlier that $\deg(\phi) > 0$ when $\phi \neq 0$.

□

We now prove a version of the Cauchy-Schwarz inequality which we will need to prove Hasse's theorem.

Lemma 17.3. *Let A be an abelian group and $q : A \to \mathbb{Z}$ a positive definite quadratic form. Then*

$$|q(\psi - \phi) - q(\psi) - q(\phi)| \leq 2\sqrt{q(\phi)q(\psi)}$$

$\forall \psi, \phi \in A$.

Proof. By Definition 17.1, the map $\langle \psi, \phi \rangle = q(\psi + \phi) - q(\psi) - q(\phi)$ is bilinear. It follows that $q(0) = 0$ and $q(m\phi) = m^2 q(\phi)$ for all $m \in \mathbb{Z}$ and $\phi \in A$.

Now, take any $\phi, \psi \in A$. If $\psi = 0$, then the result is clear, so assume $\psi \neq 0$. For any $m, n \in \mathbb{Z}$, we have

$$\begin{aligned} q(m\psi - n\phi) &= \langle m\psi, -n\phi \rangle + q(m\psi) + q(n\phi) \\ &= -mn\langle \psi, \phi \rangle + m^2 q(\psi) + n^2 q(\phi). \end{aligned}$$

Since q takes values in $\mathbb{Z}$, by assumption, we can set $m = \langle \psi, \phi \rangle$ and $n = 2q(\psi)$ to get

$$q(m\psi - n\phi) = -q(\phi)\langle \psi, \phi \rangle^2 + 4q(\psi)^2 q(\phi).$$

Now the left hand side of this equation is non-negative and therefore

$$q(\psi)[4q(\psi)q(\phi) - \langle \psi, \phi \rangle^2] \geq 0.$$

But $q(\psi) > 0$ since $\psi \neq 0$, so the result follows. □

Let E be an elliptic curve over the finite field $\mathbb{F}_q$ where $q = p^r$, for some prime p. Observe that for any polynomial $f(x, y) \in \mathbb{F}_q[x, y]$, we have $f(x, y)^q = f(x^q, y^q)$. Choose a generalized Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^4 + a_4 x + a_6$$

for E, with each $a_i \in \mathbb{F}_q$. We define the (q-th power) **Frobenius morphism**

$$\begin{aligned} \phi : \quad E(\bar{\mathbb{F}}_q) &\longrightarrow E(\bar{\mathbb{F}}_q) \\ (x, y) &\longmapsto (x^q, y^q). \end{aligned}$$

Lemma 17.4. *Let E be an elliptic curve over $\mathbb{F}_q$ and let ϕ be the q-th power Frobenius morphism. Then*

1. $\deg \phi = q$
2. *For any $m, n \in \mathbb{Z}$, $[m]_E + [n]_E \circ \phi$ is separable if and only if $p \not| m$.*

Proof. Omitted - see Silverman pp. 30 and pp. 83 □

Theorem 17.5. (Hasse) *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then*

$$| \#E(\mathbb{F}_q) - q - 1 | \leq 2\sqrt{q}.$$

Proof. Choose a generalized Weierstrass equation for E and let $\phi : E \to E$ be the q-th power Frobenius morphism, as defined above. Let $P \in E(\bar{\mathbb{F}}_q)$. The coordinates of P lie in some finite extension L of $\mathbb{F}_q$. We know that the extension $L/\mathbb{F}_q$ is Galois, with Galois group generated by the Frobenius automorphism $(x \mapsto x^q)$. Hence

$$P \in E(\mathbb{F}_q) \iff \phi(P) = P.$$

Therefore, we have

$$E(\mathbb{F}_q) = \mathrm{Ker}(1 - \phi : E(\bar{\mathbb{F}}_q) \to E(\bar{\mathbb{F}}_q)).$$

By Lemma 17.4, $1 - \phi$ is separable and hence

$$\deg(1 - \phi) = \#\,\mathrm{Ker}(1 - \phi) = \#E(\mathbb{F}_q).$$

Now, taking $A = \mathrm{End}(E)$ and $\psi = 1$ in Lemma 17.3, we get

$$| \deg(1 - \phi) - 1 - \deg(\phi) | \leq 2\sqrt{\deg \phi}.$$

The result follows. □

Example. *Let $K = \mathbb{F}_q$ be a finite field with $q = p^r$ elements. Let $f(x) \in K[x]$ be a cubic polynomial which has distinct roots in $\bar{K}$. We show that the values of f (evaluated at elements of K) tend to be distributed equally amongst squares and non squares: Define*

$$\begin{array}{rccl} \chi: & K^* & \longrightarrow & \{\pm 1\} \\ & t & \longmapsto & \begin{cases} 1 & \text{if } t \in (K^*)^2; \\ -1 & \text{otherwise.} \end{cases} \end{array}$$

We set $\chi(0) = 0$. Since f has distinct roots, we can define an elliptic curve by the equation

$$E: \quad y^2 = f(x).$$

What is the size of $E(K)$? Well, for each point $x \in K$ there are $1 + \chi(f(x))$ solutions of the equation $y^2 = f(x)$. Remembering the point at infinity, we see that

$$\#E(K) = 1 + \sum_{x \in K} (1 + \chi(f(x))) = 1 + q + \sum_{x \in K} \chi(f(x)).$$

Applying Hasse's theorem, we get

$$\left| \sum_{x \in K} \chi(f(x)) \right| \leq 2\sqrt{q}.$$

Lecture 18

Introduction to Galois cohomology

Will Shapiro
09 / 03 / 2005

It would be impossible to improve on John Tate's notes at http://modular.ucsd.edu/Tables/Notes/tate-pcmi.html.

Lecture 19

Cohomology and Mordell-Weil

Sarah Zerbes
11 / 03 / 2005

Let $K/\mathbb{Q}$ be a finite extension, E, E' elliptic curves over K. Let $\phi : E \to E'$ be an isogeny over K.

Theorem 19.1.

$$\frac{E'(K)}{\phi(E(K))} \text{ is finite.}$$

Observation:

$$0 \longrightarrow E(\bar{K})[\phi] \longrightarrow E(\bar{K}) \longrightarrow E'(\bar{K}) \longrightarrow 0$$

is an exact sequence of G_K-modules (where $G_K = \mathrm{Gal}(\bar{K}/K)$).
So we can take the long exact sequence on cohomology:

$$0 \longrightarrow E(K)[\phi] \longrightarrow E(K) \longrightarrow E'(K)$$

$$\xrightarrow{\delta} H^1(G_K, E[\phi]) \longrightarrow H^1(G_K, E) \longrightarrow H^1(G_K, E')$$

The map δ is defined like so: given $P \in E'(K)$, take $Q \in E(\bar{K})$ such that $\phi(Q) = P$. Then, define

$$\delta(P) : \sigma \longmapsto \sigma(Q) - Q$$

So we have a short exact sequence:

$$0 \longrightarrow \tfrac{E'(K)}{\phi(E(K))} \longrightarrow H^1(G_K, E[\phi]) \longrightarrow H^1(G_K, E)[\phi] \longrightarrow 0$$

We can study this prime by prime. Let M_K be the complete set of all places of K. For $v \in M_K$, write $G_v = \mathrm{Gal}(\bar{K}_v/K_v)$. Then we have the exact sequence:

$$0 \longrightarrow \tfrac{E'(K_v)}{\phi(E(K_v))} \longrightarrow H^1(G_v, E[\phi]) \longrightarrow H^1(G_v, E)[\phi] \longrightarrow 0$$

Choose an embedding $\bar{K} \hookrightarrow \bar{K}_v$, which induces an injective homomorphism $G_v \hookrightarrow G_K$.

We have restriction maps $H^1(G_K, E[\phi]) \longrightarrow H^1(G_v, E[\phi])$, and these give us the following diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E'(K)}{\phi(E(K))} & \longrightarrow & H^1(G_K, E[\phi]) & \longrightarrow & H^1(G_K, E)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \frac{E'(K_v)}{\phi(E(K_v))} & \longrightarrow & H^1(G_v, E[\phi]) & \longrightarrow & H^1(G_v, E)[\phi] & \longrightarrow & 0 \end{array}$$

So we also have a diagram (with exact rows):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E'(K)}{\phi(E(K))} & \longrightarrow & H^1(G_K, E[\phi]) & \longrightarrow & H^1(G_K, E)[\phi] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_{v \in M_K} \frac{E'(K_v)}{\phi(E(K_v))} & \longrightarrow & \prod_{v \in M_K} H^1(G_v, E[\phi]) & \longrightarrow & \prod_{v \in M_K} H^1(G_v, E)[\phi] & \longrightarrow & 0 \end{array}$$

Definition 19.2. *The **Selmer group** is defined:*

$$\mathrm{Sel}^{(\phi)}(E/K) = \ker\left(H^1(G_K, E[\phi]) \longrightarrow \prod_{v \in M_K} H^1(G_v, E)[\phi] \right)$$

*The **Tate-Shafarevich group** is defined:*

$$Ш^{(\phi)}(E/K) = \ker\left(H^1(G_K, E)[\phi] \longrightarrow \prod_{v \in M_K} H^1(G_v, E)[\phi] \right)$$

Remarks:
(i) These definitions are independent of the choice of embeddings $\bar{K} \hookrightarrow \bar{K_v}$.
(ii) We have an embedding:

$$\frac{E'(K)}{\phi(E(K))} \hookrightarrow \mathrm{Sel}^{(\phi)}(E/K)$$

Proposition 19.3. *We have an exact sequence:*

$$0 \longrightarrow \frac{E'(K)}{\phi(E(K))} \longrightarrow \mathrm{Sel}^{(\phi)}(E/K) \longrightarrow Ш^{(\phi)}(E/K) \longrightarrow 0$$

So, to show $\frac{E'(K)}{\phi(E(K))}$ is finite, it suffices to show that $\mathrm{Sel}^{(\phi)}(E/K)$ is finite.

Theorem 19.4. $\mathrm{Sel}^{(\phi)}(E/K)$ *is finite.*

Idea: $\mathrm{Sel}^{(\phi)}(E/K) \subset H^1(G_K, E[\phi])$
We'll show that every cohomology class is trivial on a large subgroup of G_K, then "replace" G_K by a more manageable quotient.

Let v be a finite prime of K. Let $I_v \subset G_v$ be the inertia group of v (that is, I_v consists of all the elements that act trivially on the residue field).

Definition 19.5. *Consider a cohomology class $\zeta \in H^1(G_v, M)$, where M is a finite G_K-module.*
*We say ζ is **unramified** if its restriction to I_v is trivial; that is, it has trivial image under the restriction map $H^1(G_v, M) \longrightarrow H^1(I_v, M)$*

Definition 19.6. *Now let $\zeta \in H^1(G_K, M)$, and let v be a finite place of K.*
*We say ζ is **unramified at** v if its image (under restriction) in $H^1(G_v, M)$ is unramified.*

Now, let $m = \deg(\phi)$. Define a finite set of primes $S \subset M_K$ like so:

$$S = \{v : v \text{ divides } m\} \cup \{v : E \text{ has bad reduction at } v\} \cup \{ \text{ all infinite primes}\}$$

Lemma 19.7. *If $\zeta \in \mathrm{Sel}^{(\phi)}(E/K)$, then ζ is unramified at v for all primes $v \notin S$.*

Proof. Take $v \notin S$. Look at image of ζ in $H^1(G_v, E[\phi])$. Consider the following exact sequence:

$$E(K_v) \longrightarrow E'(K_v) \xrightarrow{\delta} H^1(G_v, E[\phi]) \xrightarrow{f} H^1(G_v, E)[\phi]$$

Since ζ is in the Selmer group, $f(\zeta) = 0$ so we have some point $P \in E'(K_v)$ such that $\delta(P) = \zeta$.
So we have $Q \in E(\bar{K}_v)$ such that $\phi(Q) = P$ and $\zeta(\sigma) = \sigma(Q) - Q$ for all $\sigma \in G_v$.

Note: that $\phi(\sigma(Q) - Q) = 0$ for all σ.
To see this, $\phi(\sigma(Q) - Q) = \sigma(\phi(Q)) - \phi(Q) = \sigma(P) - P$. But $P \in E'(K_v)$ so $\sigma \in \mathrm{Gal}(\bar{K}_v/K_v)$ must fix P. So, $\phi(\sigma(Q) - Q) = 0$.

In particular, $\zeta(\sigma) = \sigma(Q) - Q$ for all $\sigma \in I_v$.
Consider reduction modulo v:

$$\begin{aligned}(\sigma(Q) - Q)^{\sim} &= \sigma(\widetilde{Q}) - \widetilde{Q} \\ &= \widetilde{Q} - \widetilde{Q} \text{ since } \sigma \in I_v \text{ acts trivially on the residue field} \\ &= 0\end{aligned}$$

So (since $v \notin S$, and $\phi(\sigma Q - Q) = 0$ so $\sigma Q - Q$ is an m-torsion point) $\sigma(Q) - Q = 0$; that is, ζ is trivial in $H^1(I_v, E[\phi])$. □

Lecture 20

Completion of the proof of Mordell-Weil

Sarah Zerbes
14 / 03 / 2005

Lemma 20.1. *$T \subset M_K$ a finite subset, M a finite G_K-module. Let*

$$H^1(G_K, M, T) = \{\zeta \in H^1(G_K, M) : \zeta \text{ is unramified outside } T\}$$

*Then $H^1(G_K, M, T)$ is **finite**.*

Proof. G_K acts continuously on the finite module M; hence there exists an open normal subgroup $H \trianglelefteq G_K$ acting trivially on M. We have an exact sequence:

$$0 \longrightarrow H^1(\tfrac{G_K}{H}, M) \longrightarrow H^1(G_K, M) \longrightarrow H^1(H, M)$$

Since $\frac{G_K}{H}$ is finite, WLOG we may assume G_K acts trivially on M;
so $H^1(G_K, M) = \mathrm{Hom}(G_K, M)$.

Now, if $\zeta \in \mathrm{Hom}(G_K, M)$ then ζ factors through an extension L/K, unramified outside T. Let $k \in \mathbb{N}$ be the exponent of M (so $kx = 0$ for all $x \in M$).
In fact ζ must factor through the maximal abelian extension F/K of exponent k which is unramified outside T. By Hermite's theorem, F/K is finite. □

Now, combining Lemmas 19.7 and 20.1, and using the fact that $E(\bar{K})[\phi]$ is finite (by the Finiteness Theorem), we deduce $\mathrm{Sel}^{(\phi)}(E/K)$ is finite, and the result we originally wanted follows.

Lecture 21

Sarah vs. Zacky

Vladimir Dokchitser
16 / 03 / 2005

In this lecture, we want to explain why Sarah's cohomological approach to proving the Mordell-Weil theorem for a general number field K agrees with what we did (in a more low-tech way) over $\mathbb{Q}$ in Zacky's lectures.

Once again, let E be an elliptic curve given by the GWE:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Let's briefly remind ourselves of some things we did earlier on. If E is defined over $\mathbb{Q}$ and E has a point of order 2, we can change co-ordinates (as we did before) to get E in the form:

$$E : y^2 = x^3 + ax^2 + bx$$

We have the dual curve:

$$E' : y^2 = x^3 + a'x^2 + b'x$$

(with $a' = -2a$, $b' = a^2 - 4b$.)
We also have the map $\phi : E \longrightarrow E'$ where

$$\phi(u, v) = (\frac{v^2}{u^2}, \frac{v(b - u^2)}{u^2})$$

There is a similar map $\phi' : E' \longrightarrow E$ such that $\phi \circ \phi' = [2]_{E'}$ and $\phi' \circ \phi = [2]_E$.

Zacky's Method In Zacky's lectures we found $\left|\frac{E}{\phi'(E')}\right|$ and $\left|\frac{E'}{\phi(E)}\right|$. We proved a formula for the rank of the curve:

$$2^{g_E} = \frac{1}{4}\left|\frac{E}{\phi'(E')}\right|\left|\frac{E'}{\phi(E)}\right|$$

We also had the map:

$$\alpha' : E \longrightarrow \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}$$

with $\alpha(x,y) = x$ unless $(x,y) = \mathcal{O}$ or $(0,0)$. This map had the property $\ker(\alpha') = \phi(E)$, so α induces an embedding

$$\frac{E'}{\phi(E)} \hookrightarrow \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}$$

Sarah's Method Consider the isogeny $\phi : E \longrightarrow E'$ above. We have an exact sequence of $G_\mathbb{Q}$-modules:

$$0 \longrightarrow E(\bar{\mathbb{Q}})[\phi] \longrightarrow E(\bar{\mathbb{Q}}) \xrightarrow{\phi} E'(\bar{\mathbb{Q}}) \longrightarrow 0$$

So we can take the long exact sequence on cohomology:

$$0 \longrightarrow E(\mathbb{Q})[\phi] \longrightarrow E(\mathbb{Q}) \longrightarrow E'(\mathbb{Q}) \xrightarrow{\delta} H^1(G_\mathbb{Q}, E[\phi]) \longrightarrow \ldots$$

This gives us an exact sequence:

$$0 \longrightarrow \tfrac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \xrightarrow{\delta} H^1(G_\mathbb{Q}, E[\phi]) \longrightarrow H^1(G_\mathbb{Q}, E)[\phi] \longrightarrow 0$$

We know that $E[\phi] = \{\mathcal{O}, (0,0)\} \cong C_2$, and $G_\mathbb{Q}$ acts **trivially** on it. Therefore

$$H^1(G_\mathbb{Q}, E[\phi]) = \mathrm{Hom}(G_\mathbb{Q}, C_2)$$

If we pick $\xi \in \mathrm{Hom}(G_\mathbb{Q}, C_2)$ with $\xi \neq 0$, then $\ker \xi \lhd G_\mathbb{Q}$ of index 2.
Let L be the fixed field of $\ker \xi$; then $L/\mathbb{Q}$ is a quadratic extension. Therefore ξ is determined by the quadratic field $L = \mathbb{Q}(\sqrt{n})$.

Note: $\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$ if and only if $\frac{n}{m} \in \mathbb{Q}^{\times 2}$; which is to say, ξ determines an element of $\frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}$.

So we can rewrite our short exact sequence as:

$$0 \longrightarrow \tfrac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \longrightarrow \tfrac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}} \longrightarrow H^1(G_\mathbb{Q}, E)[\phi] \longrightarrow 0$$

Recall Zacky's α' map:

$$\alpha' : E' \longrightarrow \frac{\mathbb{Q}^\times}{\mathbb{Q}^{\times 2}}$$

$$(u,v) \longmapsto u \mod \mathbb{Q}^{\times 2}$$

(unless $u = 0$ or ∞.)

We want to compare α' and δ. Recall how δ was defined: take some $Q \in E(\bar{\mathbb{Q}})$ such that $\phi(Q) = P$. Then

$$\delta(P) : \sigma \longmapsto Q - \sigma(Q) \text{ for all } \sigma \in G_\mathbb{Q}$$

So, what is the kernel of $\delta(P) \in \mathrm{Hom}(G_\mathbb{Q}, C_2)$?

$$\delta(P)(\sigma) = \mathcal{O} \Leftrightarrow \sigma(Q) = Q$$

$$\Leftrightarrow P \text{ has a } \phi\text{-preimage fixed by } \sigma$$

Recall: $P \in \phi(E(\mathbb{Q})) \Leftrightarrow P = (u, v)$ with $u \in \mathbb{Q}^{\times 2}$ (for details see the end of lecture 6.)
In fact, it can be shown that $P \in \phi(E(K)) \Leftrightarrow u \in K^{\times 2}$ for a general number field K; although we won't do that here.

Hence if we set $L = \mathbb{Q}(Q)$ (the field of definition of the point Q) then we have

$$\delta(P)(\sigma) = \mathcal{O} \Leftrightarrow \sigma \in G_L$$

Note: $L = \mathbb{Q}(\sqrt{u})$ where $P = (u, v)$. In the language we were using before, if $\xi = \delta(P)$ then ξ determines the quadratic field $L = \mathbb{Q}(\sqrt{u})$.

So, under the isomorphism

$$\mathrm{Hom}(G_{\mathbb{Q}}, C_2) \xrightarrow{\sim} \frac{\mathbb{Q}^{\times}}{\mathbb{Q}^{\times 2}}$$

δ becomes the map

$$(u, v) \longmapsto u \mod \mathbb{Q}^{\times 2}$$

so δ has become Zacky's α' under this isomorphism!

So, let's compare the images of the maps α' and δ.

Zacky: $\mathrm{Im}(\alpha') \subset \langle -1, p_1, p_2, ..., p_n \rangle$ where the p_i are the primes dividing b'.

Sarah: $\mathrm{Im}(\delta)$ consists of cocycles unramified outside ∞, 2 and the primes $\{p : p | b(a^2 - 4b)\}$
Recall that $\xi \in \mathrm{Hom}(G_{\mathbb{Q}_p}, E[\phi])$ is unramified if its restriction to the inertia group I_p is trivial.
Therefore, if ξ corresponds to $\mathbb{Q}(\sqrt{n})$, then $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$ is unramified at p; so (for $p > 2$) p does not divide n. Now we know that α and δ are the same map, we recover the fact that

$$\mathrm{Im}(\alpha') \subset \langle -1, 2, p_1, p_2, ..., p_n \rangle$$

where the p_i are the primes dividing $b(a^2 - 4b)$.
Therefore, $\mathrm{Im}(\alpha')$ is finite, so $\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}$is finite. This proves the Weak Mordell-Weil Theorem.

The Selmer Group: Take $\xi \in \mathrm{Hom}(G_{\mathbb{Q}}, E[\phi])$. Let ξ correspond to $\mathbb{Q}(\sqrt{n})/\mathbb{Q}$.

$$\mathrm{Res}^{G_{\mathbb{Q}}}_{G_{\mathbb{Q}_p}}(\xi) \in \mathrm{Hom}(G_{\mathbb{Q}_p}, E[\phi])$$

If $\xi \in \mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$, then Res($\xi$) comes from $\frac{E'(\mathbb{Q}_p)}{\phi E(\mathbb{Q}_p)}$. That is, there exists a point $P \in E'(\mathbb{Q}_p)$ which maps to Res(ξ) under δ. So there is a point $P = (u, v) \in E'(\mathbb{Q}_p)$ such that $u \equiv n \mod \mathbb{Q}^{\times 2}$ (for every p). So, to identify $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$ for concrete curves E, take all possible $n \in \langle -1, 2, p_1, p_2, ..., p_m \rangle$ (as in Sarah's theorem.) For each n, we check: for all primes p, does there exist $P = (u, v) \in E'(\mathbb{Q}_p)$ such that $u \equiv n \mod \mathbb{Q}^{\times 2}$ (and similarly over $\mathbb{R} = \mathbb{Q}_\infty$.)
(**Remark:** It is sufficient to check such a P exists for $p = \infty, 2, p_1, ..., p_m$.)

However, to identify $\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))}$, we need to take all n and check for $P = (u, v) \in E(\mathbb{Q})$ with $u \equiv n \mod \mathbb{Q}^{\times 2}$.

The Villain of the Piece: Recall the the Tate-Shafarevich group $Ш^{(\phi)}(E/\mathbb{Q})$. The problem is that $Ш^{(\phi)}(E/\mathbb{Q})$ may not be zero. In this case, $\xi \in \mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$ does **not** imply that ξ comes from $E'(\mathbb{Q})$. Let

$$Ш(E/\mathbb{Q}) = \ker\left(H^1(G_{\mathbb{Q}}, E) \longrightarrow \prod_{p,\infty} H^1(G_{\mathbb{Q}_p}, E)\right)$$

Conjecture: $Ш(E/\mathbb{Q})$ is **finite**. (When it is finite, a theorem of Cassels tells us $|Ш(E/\mathbb{Q})|$ is a square.)