Notes for “Elliptic Curves” by Vladimir Dokchitser

Calum Crossley

LSGNT 2023-2024

Preparatory information:

- Books: Silverman’s “The Arithmetic of Elliptic Curves”
- Prerequisites: basics of Galois theory, basics of number fields, basics of algebraic curves, complex analysis, and p-adic numbers
- Exercise sheets: 1 per lecture, 2 out of 5 exercises for assessment (marked with a “+”)
- Lectures: 10 of them

Scribe’s note: Exercises marked with a “!” here were marked with a skull and crossbones on the sheets. I have not included solutions to them since I cannot solve them.

Tentative lecture topics:

1) The group law
2) Elliptic curves over $\mathbb{C}$
3) Heights
4) The Mordell–Weil theorem
5) Elliptic curves over $\mathbb{Q}_p$
6) Formal groups
7) Explicit 2-descent
8) Tate modules
9) L-functions and BSD
10) Selmer groups

Pre-waffle. This is a number theory course, so we care about solving Diophantine equations. For example, what are the rational solutions of $x^2 + y^2 = 1$?

$$x = \frac{2t}{t^2+1}, \quad y = \frac{t^2-1}{t^2+1}, \quad t \in \mathbb{Q}.$$

The general case is impossibly hard; it is formally undecidable. We will focus on curves, such as one equation with two variables. Life is strongly affected by the geometry over $\mathbb{C}$, where the curve is a closed orientable surface in projective space.

- Genus 0: The Riemann sphere; $\mathbb{P}^1$. The number theory is easy; either there are no $\mathbb{Q}$-solutions or infinitely many nicely parametrized, and we can decide which (Hasse principle).
- Genus 1 (this course): The torus. There can be no $\mathbb{Q}$-solutions, or finitely many, or infinitely many. No proven algorithm exists for deciding which in general, although there are algorithms conditional on the Tate–Shafarevich conjecture or the BSD conjecture.
- Genus ≥ 2: There are finitely many $\mathbb{Q}$-solutions by a theorem of Faltings.

Remark. By Siegel’s theorem there are only finitely many $\mathbb{Z}$-solutions for $g \geq 1$.

1 Group Law

Definition. An *elliptic curve* over a field K is a projective non-singular curve E of genus 1 over K, together with a given K-rational point $\mathcal{O}$.

Example. Take $E : y^2 = x^3 - x$, that is $Y^2Z = X^3 - XZ^2$, with $\mathcal{O} = [0 : 1 : 0]$ the point at infinity.

Definition. A *(generalized) Weierstrass equation* over K is an equation of the form

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

with $a_i \in K$. For ease of notation we identify this with the affine equation

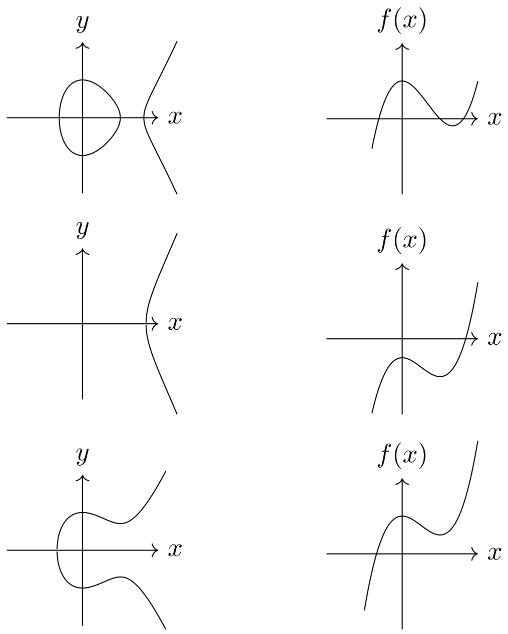
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Remark. At infinity we have the point $[0 : 1 : 0]$ and no others. This is the standard choice for $\mathcal{O}$. If E is non-singular, the genus is 1.

Notation. We write

$$\begin{aligned} E(K) &= \{\text{solutions } [X : Y : Z] \text{ to the equation over } K\} \\ &= \{\mathcal{O}\} \cup \{\text{solutions } (x, y) \text{ to the equation over } K\}. \end{aligned}$$

Example. If $E : y^2 = f(x)$ with $f(x)$ a monic cubic, then $E(\mathbb{R})$ looks as follows:



Theorem 1 (see Silverman, Chapter III)**.** *Let $\mathcal{E}$ be an elliptic curve over K. Then there exists an isomorphism (of projective varieties) from $\mathcal{E}$ to the projective curve defined by*

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

for some $a_i \in K$, mapping the given K-rational point to the point at infinity.

Remark. To keep track of the indices for the Weierstrass equation, give x weight 2, y weight 3, and a_i weight i. The terms all have weight 6.

Example. Take $\mathcal{E} : y^2 = x^4 - 1$ with point $P = (1, 0)$.

- Let $x_2 = x - 1$, giving $y^2 = x_2(x_2 + 2)(x_2^2 + 2x_2 + 2)$. (Move P to the origin.)
- Let $x_3 = 1/x_2$, giving $(x_3^2y)^2 = (1 + 2x_3)(1 + 2x_3 + 2x_3^2)$. (Move P to infinity.)
- Let $y_2 = yx_3^2$, giving $y_2^2 = 4x_3^3 + 6x_3^2 + 4x_3 + 1$. (Make monic in y.)

- Let $y_3 = y_2/2$, giving $y_3^2 = x_3^3 + \frac{3}{2}x_3^2 + x_3 + \frac{1}{4}$. (Make monic in x.)

Note here we need $\operatorname{char} K \neq 2$. In fact this is a sloppy example, since the naive projectivization of the equation is singular. Instead one should use the equation $t^2 = 1 - s^4$ at infinity, where $s = 1/x$, $t = y/x^2$.

Proposition 2 (see Silverman, Chapter III)**.**

(i) One can further simplify the Weierstrass equation to

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

when $\operatorname{char} K \neq 2$*, and to*

$$E : y^2 = x^3 + Ax + B$$

when $\operatorname{char} K \neq 2, 3$.

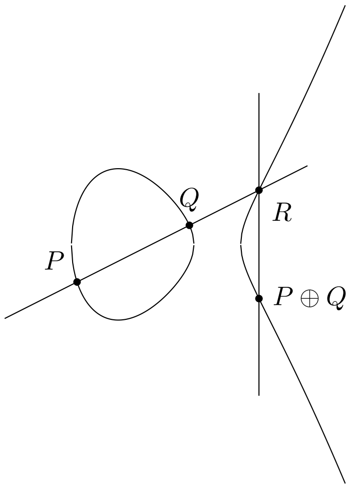
(ii) Two curves given by generalized Weierstrass equations E and E' are isomorphic over K iff they are related by a change of variables of the form

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

for some $u, r, s, t \in K$ with $u \neq 0$.

(iii) If $\operatorname{char} K \neq 2$*, and $E : y^2 = x^3 + ax^2 + bx + c$, then E is non-singular iff the RHS cubic has no repeated roots, i.e. iff its discriminant is non-zero.*

Definition. Suppose E/K is an elliptic curve given by a Weierstrass equation. Let $P, Q \in E(K)$. Define their *sum* $P \oplus Q$ (or just $P + Q$) by the following process:



The line through P and Q, or the tangent if $P = Q$, meets E at exactly one other point R when counting with multiplicity. Repeat the process with $\mathcal{O}$ and R, i.e. reflect R across $y = 0$, to obtain $P \oplus Q$.

Remark. If $P, Q \in E(K)$ then $P \oplus Q \in E(K)$. (If two roots of a cubic are rational then the third is too.) This gives a process to construct new rational points from old ones.

Theorem 3. *The operation $\oplus$ makes $E(K)$ an abelian group with identity $\mathcal{O}$.*

Proof. See Silverman, Chapter III. See next section for the characteristic 0 case. □

Remark. (i) If $P = (x_1, y_1)$, then $\ominus P = (x_1, -y_1 - a_1x - a_3)$ for a generalized Weierstrass equation.

(ii) If F/K is a field extension, then $E(K) \subseteq E(F)$ is a subgroup.

(iii) For $E : y^2 = (x - a)(x - b)(x - c)$, the points where $y = 0$ are precisely the points of order 2.

Example. The equation $y^2 = (x - 1)(x - 2)(x - 3) \bmod p$, where $p \neq 2$ is prime, has total number of solutions $N \equiv 3 \bmod 4$. Indeed $E(\mathbb{F}_p)$ has a subgroup isomorphic to $C_2 \times C_2$ given by the points of order 2 and the identity, so $4 \mid \#E(\mathbb{F}_p)$, and removing the point at infinity gives $N = \#E(\mathbb{F}_p) - 1$.

Theorem 4 (Mordell 1922)**.** *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})$ is a finitely generated abelian group.*

Proof. See section 4. $\square$

Remark. So $E(\mathbb{Q}) \simeq \Delta \times \mathbb{Z}^r$ for some $r \geq 0$ and finite group Δ.

Definition. With $E(\mathbb{Q}) \simeq \Delta \times \mathbb{Z}^r$ as above r is the *rank* of $E/\mathbb{Q}$, and Δ the torsion subgroup of $E(\mathbb{Q})$.

Remark. The result also holds over number fields, and for all abelian varieties (Mordell–Weil theorem).

Remark. To describe $E(\mathbb{Q})$, one is happy with having generators for the group; finite data from which the points can be enumerated computationally. One cannot parametrize $E(\mathbb{Q})$ like the conics: there are no non-constant $P(t), Q(t) \in \mathbb{Q}(t)$ satisfying the equation of an elliptic curve. (Otherwise we get a rational map $\mathbb{P}^1_{\mathbb{C}} \to E(\mathbb{C})$ contradicting the Riemann–Hurwitz formula.)

Example.

- $E : y^2 - y = x^3 - x$ has $E(\mathbb{Q}) = \{\mathcal{O}, (0,0), (0,1), (1,0), (1,1)\} \simeq C_5$.
- $E : y^2 + y = x^3 - x$ has $E(\mathbb{Q}) \simeq \mathbb{Z}$ generated by $(0,0)$.
- $E : y^2 + y = x^3 + x - 2x$ has $E(\mathbb{Q}) \simeq \mathbb{Z}^2$ generated by $(0,0)$ and $(1,0)$.
- $E : y^2 = x^3 - 2x$ has $E(\mathbb{Q}) \simeq C_2 \times \mathbb{Z}$ generated by $(0,0)$ and $(-1,1)$ respectively.
- $E : y^2 = x^3 + 877x$ has $E(\mathbb{Q}) \simeq C_2 \times \mathbb{Z}$ generated by $(0,0)$ and (*a horrid mess*) respectively.

Exercise Sheet 1

+1. Let E be the elliptic curve given by
$$y^2 - y = x^3 - x^2.$$
Verify that the point $P = (0,0)$ has order 5.

Solution. The tangent at P is $y = 0$, which intersects E when $x^3 - x^2 = 0$. The third point is then $(1,0)$, and the line through $(1,0)$ and $\mathcal{O}$ intersects E again at $(1,1)$. Hence $2 \cdot P = (1,1)$.

The tangent at $(1,1)$ is $y = x$, which intersects E when $x^2 - x = x^3 - x^2$. The third point is then $(0,0)$, and the line through $(0,0)$ and $\mathcal{O}$ intersects E again at $(0,1)$. Hence $4 \cdot P = (0,1)$.

The line through P and $(0,1)$ is $x = 0$, which meets E at the point $\mathcal{O}$ at infinity. Hence $5 \cdot P = \mathcal{O}$, so P has order 5. $\square$

+2. Let $E/\mathbb{Q}$ be an elliptic curve that has a rational point of order 3. Show that E is isomorphic to one of the form
$$y^2 = x^3 + (ax - b)^2.$$
(*Hint: you may find it helpful to show that a point P has order 3 if and only if the tangent line to E through P intersects E at P with multiplicity 3.*)

Solution. We have $3 \cdot P = \mathcal{O}$ iff the tangent line at P intersects E at P only. By Proposition 1(i), we may assume E has an equation of the form $y^2 = x^3 + px^2 + qx + r$, and by translation we may assume the rational point P of order 3 is of the form $(0, \beta)$. If $\beta = 0$ then $r = 0$ and $q \neq 0$ by non-singularity, so the tangent line at P is the y-axis, whose intersections with E are given by the cubic equation $x^3 + px^2 + qx = 0$. This has at least two distinct roots, since $q \neq 0$, contradicting the fact that P is the only intersection of the tangent line with E. Hence $\beta \neq 0$, so the tangent line at P is
$$y = \beta + \frac{q}{2\beta}x,$$
which intersects E when
$$\begin{aligned} &\big(\beta + \frac{q}{2\beta}x\big)^2 = x^3 + px^2 + qx + r \\ \iff\ & x^3 + \big(p - \frac{q^2}{4\beta^2}\big)x^2 + r - \beta^2 = 0. \end{aligned}$$

Then since $3 \cdot P = \mathcal{O}$ this cubic has only the one root at $x = 0$, meaning

$$p - \frac{q^2}{4\beta^2} = r - \beta^2 = 0,$$

so

$$\begin{aligned} E : y^2 &= x^3 + \frac{q^2}{4\beta^2}x^2 + qx + \beta^2 \\ &= x^3 + \big(\frac{q}{2\beta}x + \beta\big)^2, \end{aligned}$$

which is of the desired form with $a = \frac{q}{2\beta}$ and $b = -\beta$. □

3. Determine the group $E(\mathbb{F}_3)$ for the elliptic curves

$$E : y^2 = x^3 - x \qquad \text{and} \qquad E : y^2 = x^3 + x.$$

Solution. For $E : y^2 = x^3 - x$ the polynomial $x^3 - x$ vanishes on $\mathbb{F}_3$, so the points (apart from $\mathcal{O}$) are $\{(x, 0) : x \in \mathbb{F}_3\}$. All have order 2 since $y = 0$, so $E(\mathbb{F}_3) \simeq C_2 \times C_2$.

For $E : y^2 = x^3 + x$ the points (apart from $\mathcal{O}$) are $\{(0, 0), (2, 1), (2, 2)\}$. Since $(2, 1)$ and $(2, 2)$ do not have order 2, having $y \neq 0$, we have $E(\mathbb{F}_3) \simeq C_4$. □

4. Let E and E' be two elliptic curves over a field K given by Weierstrass equations. Show that if the elliptic curves E and E' are isomorphic, then so are the groups $E(K)$ and $E'(K)$.

Solution. By Proposition 1(ii) we may assume E and E' are related by a linear change of coordinates. Now a K-linear change of coordinates preserves K-rational points, lines, incidence, and tangency, and therefore preserves the definition of the group law on $E(K)$. Hence it gives a group isomorphism $E(K) \simeq E'(K)$. □

!5. Prove that for every positive integer $N \equiv 5 \bmod 8$, the elliptic curve

$$y^2 = x^3 - N^2 x$$

has a rational point with a non-zero y-coordinate.

2 Elliptic Curves / $\mathbb{C}$

Recall that for an elliptic curve E we defined an operation on rational points geometrically via intersections of lines with E. Now an elliptic curve $E/\mathbb{C}$ is supposed to be a torus (a genus 1 Riemann surface), and the standard construction of a complex torus as $\mathbb{C}/\Lambda$ for a lattice Λ has an obvious group structure as a quotient of $(\mathbb{C}, +)$. How does this relate to the group structure given by line intersections?

Proposition 5 (Recall from complex analysis). *A function $f : \mathbb{C} \to \mathbb{C}$ is meromorphic iff at every $a \in \mathbb{C}$ it has a Laurent series expression*

$$f(z) = \sum_{n=n_0}^{\infty} c_n (z - a)^n$$

where $n_0 \in \mathbb{Z}$ and $c_{n_0} \neq 0$ unless $f(z) \equiv 0$. We write

$$\operatorname{ord}_a f = n_0 \quad \textit{and} \quad \operatorname{res}_a f = c_{-1}.$$

Definition. A *lattice* $\Lambda \subseteq \mathbb{C}$ is a discrete rank 2 subgroup of $(\mathbb{C}, +)$. Say

$$\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2.$$

The parallelogram spanned by ω_1 and ω_2 is the *fundamental parallelogram*, denoted Π.

Idea: Curves are essentially degree 1 transcendental extensions of $\mathbb{C}$, and the Riemann surface $\mathbb{C}/\Lambda$ has a field of meromorphic functions, so we check if that field has transcendence degree 1 over $\mathbb{C}$.

Definition. An *elliptic function* (w.r.t. Λ) is a meromorphic function f on $\mathbb{C}$ such that $f(z+w) = f(z)$ for all $w \in \Lambda$. In other words, a doubly-periodic meromorphic function.

Remark. These are precisely the meromorphic functions on the Riemann surface $X = \mathbb{C}/\Lambda$. They form a field, since we allow poles, denoted $\mathbb{C}(X)$.

Lemma 6. *Suppose f is a non-zero elliptic function.*

(i) If f is analytic, then f is constant.

(ii) We have $\operatorname{ord}_a f \neq 0$ at only finitely many $a \in \mathbb{C}/\Lambda$.

(iii) $\sum_{a\in\mathbb{C}/\Lambda} \operatorname{res}_a f = 0$.

(iv) $\sum_{a\in\mathbb{C}/\Lambda} \operatorname{ord}_a f = 0$.

(v) $\sum_{a\in\mathbb{C}/\Lambda} \operatorname{ord}_a f \cdot a \in \Lambda$.

Proof. (i) If f is analytic then f is continuous, and hence bounded on Π since Π is compact. By periodicity f is bounded on $\mathbb{C}$, and hence constant by Liouville's theorem.

(ii) Otherwise, we have an accumulation point in Π either of zeros or of poles. In the former case $f = 0$ by the identity theorem, and in the latter case the limit point is an essential singularity. (One can also reduce to only one of these cases by considering $1/f$.)

(iii) After translating Π by some amount we can assume no zeros or poles like on $\partial\Pi$, since there are only finitely many. Then

$$\sum_{a\in\mathbb{C}/\Lambda} \operatorname{res}_a f = \frac{1}{2\pi i}\oint_{\partial\Pi} f(z)dz$$

by the residue theorem. The integral splits up into four parts

$$\oint_{\partial\Pi} = \left[\int_0^{\omega_1} + \int_{\omega_1+\omega_2}^{\omega_2}\right] + \left[\int_{\omega_2}^{0} + \int_{\omega_1}^{\omega_1+\omega_2}\right],$$

but since the integrand is doubly periodic we have

$$\int_0^{\omega_1} = -\int_{\omega_1+\omega_2}^{\omega_2} \quad \text{and} \quad \int_{\omega_2}^{0} = -\int_{\omega_1}^{\omega_1+\omega_2},$$

so the result is zero.

(iv) Apply (iii) to $f'(z)/f(z)$, whose residues are the orders of $f(z)$ by local Taylor expansion.

(v) Exercise. (Use $zf'(z)/f(z)$.)

□

We are prompted to ask, are there any non-constant elliptic functions? From above they must have at least two poles, or a double pole. The answer is yes, via (almost) the most obvious construction.

Definition. The *Weierstrass $\wp$-function* (w.r.t. Λ) is given by

$$\wp(z) = \wp_\Lambda(z) = \frac{1}{z^2} + \sum_{w\in\Lambda\setminus\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right).$$

Exercise. The sum $\sum_{w\in\Lambda\setminus\{0\}} \frac{1}{|w|^\alpha}$ converges iff $\alpha > 2$.

Proposition 7. *The expression for $\wp(z)$ converges locally uniformly to an elliptic function analytic on $\mathbb{C}\setminus\Lambda$ with doubles poles on Λ.*

Proof. If $2|z| < |w|$, then

$$\left|\frac{1}{(z-w)^2} - \frac{1}{w^2}\right| = \left|\frac{z(2w-z)}{w^2(z-w)^2}\right| \leq \frac{\frac{5}{2}|zw|}{\frac{1}{4}|w|^4} = 10\frac{|z|}{|w|^3}.$$

Hence

$$\sum_{|w|>2|z|} \left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| \le 10|z| \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{|w|^3},$$

which is a finite constant multiple of $|z|$ by the exercise above. Therefore the series converges locally uniformly absolutely on $\mathbb{C}\setminus\Lambda$, and the limit is an analytic function on $\mathbb{C}\setminus\Lambda$. Clearly it has double poles on Λ. To see that $\wp$ is elliptic, note that

$$\wp'(z) = -2\sum_{w\in\Lambda} \frac{1}{(z-w)^3}$$

which is clearly elliptic, so $\wp(z+w)-\wp(z) = C(w)$ is a constant depending on $w\in\Lambda$. But we can see that $\wp(z)=\wp(-z)$ by definition, so $\wp(-w/2)=\wp(w/2)=\wp(-w/2+w)$, so $C(w)=0$. $\square$

Lemma 8.

(i) $\wp(z)$ *is even.*

(ii) $\wp'(z)$ *is odd.*

(iii) $\wp(z)-\wp(\alpha)$ *has a double pole at* $0+\Lambda$*, simple zeros at* $\pm\alpha+\Lambda$ *(or a double zero if* $2\alpha\in\Lambda$*), and no other zeros or poles.*

Proof. (i) was noted above. (ii) follows immediately. For (iii) the statement about poles is clear, and the statement about zeros follows by counting using Lemma 6(iv). $\square$

Theorem 9. *Let* $\Lambda\subseteq\mathbb{C}$ *be a lattice, and set* $X=\mathbb{C}/\Lambda$*.*

(i) $\mathbb{C}(X)=\mathbb{C}(\wp(z),\wp'(z))$.

(ii) Every even elliptic function lies in $\mathbb{C}(\wp(z))$.

Proof. For (ii), suppose an even elliptic function $f(z)$ has zeros/poles away from Λ at $\pm z_i\notin\Lambda$, with $\operatorname{ord}_{\pm z_i} f = n_i$. (If $2z_i\in\Lambda$ take $n_i=\frac{1}{2}\operatorname{ord}_{z_i} f$.) Consider

$$\tilde f(z) = \prod_i (\wp(z)-\wp(z_i))^{n_i} \in \mathbb{C}(\wp(z)).$$

Then $f(z)/\tilde f(z)$ has no zeros/poles except possibly on Λ by Lemma 8(iii). By Lemma 6(iv) then $f(z)/\tilde f(z)$ has no zeros/poles at all, and hence is constant. Therefore $f(z)\in\mathbb{C}(\wp(z))$. For (i), write an arbitrary elliptic function $f(z)$ as a sum

$$f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2}$$

of an even and an odd elliptic function. Since an odd function is an even multiple of the odd function $\wp'(z)$, we are done by (ii). In fact we see that $\mathbb{C}(\wp(z),\wp'(z))$ is a quadratic extension of $\mathbb{C}(\wp(z))$. $\square$

Definition. We define

$$G_{2k} = G_{2k}(\Lambda) = \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{w^{2k}} \in \mathbb{C}$$

for $k\ge 2$. This is known as the *Eisenstein series* of weight $2k$.

Remark. This is a two-dimensional version of the special values $\zeta(2k)$ for $k\ge 1$.

Lemma 10. *The Taylor series expansion around* $z=0$ *of* $\wp(z)$ *is*

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

Proof. We have

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{1}{w^2}\cdot\frac{1}{\left(1-\frac{z}{w}\right)^2 - 1} = \frac{1}{w^2}\sum_{k=1}^{\infty} \frac{2k+1}{w^{2k}} z^{2k}.$$

Summing over w gives the result. $\square$

Lemma 11. *We have the equation*

$$\frac{1}{4}\wp'(z)^2 = \wp(z)^3 - 15G_4\wp(z) - 35G_6.$$

Proof. From the Taylor expansions

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + 3G_4z^2 + 5G_6z^4 + \cdots \\
\wp(z)^3 &= \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + \cdots \\
\frac{1}{4}\wp'(z)^2 &= \frac{1}{z^6} - \frac{6G_4}{z^2} - 20G_6 + \cdots
\end{aligned}$$

we see that the difference between the two sides of the equation is analytic and vanishes at the origin, whence it is identically zero. □

Theorem 12. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice. Then*

$$E_\Lambda : y^2 = x^3 - 15G_4x - 35G_6$$

defines an elliptic curve over $\mathbb{C}$, i.e. it is non-singular, and

$$\varphi(z) = (\wp(z), \frac{1}{2}\wp'(z)) \qquad \wp(0) = \mathcal{O}$$

is an isomorphism of groups $\mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$.

Proof.

- φ is well-defined by Lemma 11 and periodicity of $\wp$.
- φ is bijective: if $(x_0, y_0) \in E_\Lambda(\mathbb{C})$, then $\wp(z) - x_0$ has one double pole, and therefore two zeros $\pm\alpha$, giving
  $$\{\varphi(\alpha), \varphi(-\alpha)\} = \{(x_0, y_0), (x_0, -y_0)\}.$$
  Hence φ is a bijection.
- E_Λ is non-singular: as $\wp'(z)$ is odd, it vanishes at the three points τ of order 2 in $\mathbb{C}/\Lambda$, and hence the roots of the cubic in x are the images $\wp(\omega_1/2)$, $\wp(\omega_2/2)$, $\wp((\omega_1+\omega_2)/2)$ of these points. These roots are distinct, since $\wp(z) - \wp(\tau)$ has a double root at τ and hence no other zeros.
- φ is a group homomorphism:
  - $\varphi(0) = \mathcal{O}$.
  - $\varphi(-\alpha)$ and $\varphi(\alpha)$ lie on a vertical line since $\wp(z)$ is even.
  - Suppose $P_1 \oplus P_2 = \ominus P_3$, with $\{P_i\}$ lying on the line
    $$\lambda y + \mu x + \nu = 0.$$
    Writing $P_i = \varphi(\alpha_i)$, the elliptic function $\frac{\lambda}{2}\wp'(z) + \mu\wp(z) + \nu$ vanishes at each α_i, and has a triple pole on Λ. By Lemma 6(v) we therefore have $\alpha_1 + \alpha_2 + \alpha_3 = 0$.

□

Remark. The result shows that $(E_\Lambda(\mathbb{C}), \oplus)$ is indeed a group.

Theorem 13 (Uniformization Theorem)**.** *Every elliptic curve over $\mathbb{C}$ is isomorphic to E_Λ for some Λ.*

Proof. Beyond the scope of the course. □

Corollary 14. *Let K be a number field, and E/K an elliptic curve. Then $E(K)[n] \leq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.*

Here $A[n] = \{a \in A : na = 0\}$ denotes the n-torsion subgroup of an abelian group A.

Proof. By the uniformization theorem we have $E(K) \leq E(\mathbb{C}) \simeq E_\Lambda(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ for some Λ. But by inspection $(\mathbb{C}/\Lambda)[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. □

Corollary 15. *Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over a field of characteristic 0. Then $(E(K), \oplus)$ is a group.*

Note that K may have cardinality too large to embed into $\mathbb{C}$.

Proof. This is an example of the "Lefschetz principle". All group axioms apart from associativity are easy. Suppose $P_i = (x_i, y_i) \in E(K)$ for $i = 1, 2, 3$. Define the field $F = \mathbb{Q}(a_1, a_2, a_3, a_4, a_6, x_1, y_1, x_2, y_2, x_3, y_3)$, which embeds into $\mathbb{C}$ as a finitely generated $\mathbb{Q}$-extension. We may then view E over $\mathbb{C}$ via this embedding, and $P_i \in E(F) \leq E(\mathbb{C})$ where $(P_1 \oplus P_2) \oplus P_3 = P_1 \oplus (P_2 \oplus P_3)$ by the previous result. □

Exercise Sheet 2

+1. Let $E/\mathbb{C}$ be an elliptic curve given by

$$y^2 = x^3 + Ax + B,$$

and let $m \geq 1$ be an integer. Use the uniformization theorem to show that there are rational functions f, g such that for every $P = (x_1, y_1) \in E(\mathbb{C})$, the point mP is given by $(f(x_1), y_1 g(x_1))$.

Solution. By the uniformization theorem $E \simeq E_\Lambda$ for some Λ, and by Proposition 2(ii) there is an isomorphism given by a linear change of coordinates of the form

$$x = u^2 x' + r, \quad y = u^3 y' + u^2 s x' + t.$$

Since E_Λ has no xy and no y term we have $s = t = 0$, and so this change of coordinates preserves functions of the desired form $(f(x), yg(x))$. Hence we may assume $E = E_\Lambda$, where there is the group isomorphism $\mathbb{C}/\Lambda \to E_\Lambda(\mathbb{C})$ given by $z + \Lambda \mapsto (\wp(z), \frac{1}{2}\wp'(z))$. Then if $(x_1, y_1) = (\wp(z), \frac{1}{2}\wp'(z))$, the coordinates of mP are $(\wp(mz), \frac{1}{2}\wp'(mz))$, and it suffices to note that $\wp(mz)$ and $\wp'(mz)/\wp'(z)$ are even elliptic functions, hence given by rational functions f, g of $\wp(z)$. $\square$

+2. Let Λ be a lattice in $\mathbb{C}$ and f an elliptic function with respect to Λ. Prove that $\sum_{z \in \mathbb{C}/\Lambda}(z \cdot \operatorname{ord}_z f)$ is an element of Λ. (*Hint: Integrate* $\frac{zf'(z)}{z}$ *over the boundary of the fundamental parallelogram and don't be afraid of logs.*)

Solution. Assuming f is non-zero it has finitely many zeros/poles, so we may translate it so that none lie on the boundary of the fundamental parallelogram Π. Then by the residue theorem

$$\frac{1}{2\pi i}\oint_{\partial\Pi} \frac{zf'(z)}{f(z)}dz = \sum_{a \in \Pi} \operatorname{res}_a \frac{zf'(z)}{f(z)} = \sum_{a \in \Pi}\left(a \cdot \operatorname{res}_a \frac{f'(z)}{f(z)}\right) = \sum_{a \in \Pi}(a \cdot \operatorname{ord}_a f).$$

Now if Λ is generated by ω_1, ω_2, then

$$\begin{aligned}\oint_{\partial\Pi} \frac{zf'(z)}{f(z)}dz &= \int_0^{\omega_1}\left[\frac{zf'(z)}{f(z)} - \frac{(z+\omega_2)f'(z+\omega_2)}{f(z+\omega_2)}\right]dz \\ &\quad + \int_0^{\omega_2}\left[\frac{(z+\omega_1)f'(z+\omega_1)}{f(z+\omega_1)} - \frac{zf'(z)}{f(z)}\right]dz \\ &= -\omega_2\int_0^{\omega_1}\frac{f'(z)}{f(z)}dz + \omega_1\int_0^{\omega_2}\frac{f'(z)}{f(z)}dz.\end{aligned}$$

But the integral

$$\int_0^{\omega_i}\frac{f'(z)}{f(z)}dz = \int_0^{\omega_i} d\log f(z)$$

is the increment of the analytic continuation of the logarithm along $f([0, \omega_i])$; a loop based at $f(\omega_i) = f(0)$. This is an integer multiple of $2\pi i$, so $\frac{1}{2\pi i}\oint_{\partial\Pi}\frac{zf'(z)}{f(z)}dz \in \mathbb{Z}\omega_2 + \mathbb{Z}\omega_1 = \Lambda$. $\square$

3. Let E/K be an elliptic curve over a field of characteristic zero. Prove that

$$E(\bar{K})[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Solution. By a change of coordinates we may assume $E : y^2 = x^3 + Ax + B$ for some $A, B \in K$. The map $P \mapsto nP$ on $E(L)$ for any L/K is given by $(x, y) \mapsto (p(x, y), q(x, y))$ for some $p, q \in K(x, y)$. Let $F/\mathbb{Q}$ be the extension generated by A, B, and the coefficients of p and q. Then F embeds into $\mathbb{C}$, and we may view E/F. From exercise 1 we have that $p(x, y)$ and $q(x, y)/y$ lie in $F(x, y) \cap \mathbb{C}(x) = F(x)$; say $p(x, y) = P_1(x)/P_2(x)$ and $q(x, y) = yQ_1(x)/Q_2(x)$ where $P_i, Q_i \in F[x]$. Then

$$E(\bar{K})[n] = \{(x, y) \in E(\bar{K}) : Q_2(x) = 0, y = 1/(Q_1(x)P_2(x))\} \cup \{\mathcal{O}\}$$

is finite since $Q_2(x)$ has finitely many roots, so we may assume F also contains the coordinates of all the points in $E(\bar{K})[n]$, meaning $E(\bar{F})[n] = E(\bar{K})[n]$. Now

$$E(\mathbb{C})[n] = \{(x, y) \in E(\mathbb{C}) : Q_2(x) = 0, y = 1/(Q_1(x)P_2(x))\} \cup \{\mathcal{O}\}$$

consists of points whose coordinates are algebraic over F, so since $\bar{F}$ embeds into $\mathbb{C}$ we must have $E(\bar{F})[n] \simeq E(\mathbb{C})[n]$. Hence

$$E(\bar{K})[n] = E(\bar{F})[n] \simeq E(\mathbb{C})[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

by the uniformization theorem. $\square$

4. Let E be an elliptic curve over $\mathbb{F}_p$ given by a Weierstrass equation. Prove that the operation $\oplus$ is associative. (*Hint: Write E as the reduction mod p of a suitable elliptic curve with coefficients in $\mathbb{Z}_p$. You'll need Hensel's Lemma to lift points from $\mathbb{F}_p$ to $\mathbb{Z}_p$.*)

Solution. Firstly, note that the associativity equation $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R$ for an elliptic curve is easily seen to be true in the following cases:

- If $P = \mathcal{O}$, $Q = \mathcal{O}$, or $R = \mathcal{O}$.
- If $P \oplus (Q \oplus R) = \mathcal{O}$ or $(P \oplus Q) \oplus R = \mathcal{O}$, since these both happen iff P, Q, R are collinear.
- If $P \oplus Q = \mathcal{O}$ or $Q \oplus R = \mathcal{O}$, since $(-P) \oplus (P \oplus Q) = Q$: the points $P, Q, -(P \oplus Q)$ are the intersections of a line with E, so the reflections $-P, -Q, P \oplus Q$ are also. (For a Weierstrass equation negation $(x, y) \mapsto (x, -y - a_1x - a_3)$ is linear and so sends lines to lines.)

Now suppose

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

is an equation over $\mathbb{Z}_p$ reducing to E modulo p which defines an elliptic curve $\tilde{E}/\mathbb{Q}_p$. One exists by completing the square and applying Proposition 2(iii); the discriminant cannot vanish for the infinitely many possible lifts of the coefficients. Since $\mathbb{Q}_p$ embeds into $\mathbb{C}$, we see that $\oplus$ is associative on $\tilde{E}(\mathbb{Q}_p)$ by the uniformization theorem.

If $P \in \tilde{E}(\mathbb{Z}_p)$, write $\bar{P} \in E(\mathbb{F}_p)$ for the reduction modulo p. Since E is non-singular, for every point in $E(\mathbb{F}_p)$ one coordinate when fixed leaves the other as a simple root of the defining equation. By Hensel's lemma simple roots can be lifted to $\mathbb{Z}_p$, so all points of $E(\mathbb{F}_p)$ are of the form $\bar{P}$.

Claim: If $P, Q \in \tilde{E}(\mathbb{Z}_p)$ with $\bar{P} \oplus \bar{Q} \neq \mathcal{O}$, then $P \oplus Q \in \tilde{E}(\mathbb{Z}_p)$ and $\overline{P \oplus Q} = \bar{P} \oplus \bar{Q}$.

Since we dealt with the case of vanishing sums earlier, this proves associativity on $E(\mathbb{F}_p)$:

$$\bar{P} \oplus (\bar{Q} \oplus \bar{R}) = \bar{P} \oplus \overline{Q \oplus R} = \overline{P \oplus Q \oplus R} = \overline{P \oplus Q} \oplus \bar{R} = (\bar{P} \oplus \bar{Q}) \oplus \bar{R}.$$

Proof of claim: Suppose $P = (x_1, y_1)$, $Q = (x_2, y_2)$, and $P \oplus Q = (x_3, y_3)$. Write $s = \frac{y_2 - y_1}{x_2 - x_1} \in \mathbb{Z}_p$, where $x_2 - x_1$ is invertible in $\mathbb{Z}_p$ since $\bar{P} \oplus \bar{Q} \neq \mathcal{O}$. We have a monic cubic

$$(y_1 + s(x - x_1))^2 + (a_1x + a_3)(y_1 + s(x - x_1)) = x^3 + a_2x^2 + a_4x + a_6$$

in x over $\mathbb{Z}_p$, whose roots in $\mathbb{Q}_p$ are x_1, x_2, x_3, and whose roots upon reduction to $\mathbb{F}_p$ are the x-coordinates of $\bar{P}, \bar{Q}, \bar{P} \oplus \bar{Q}$. Factoring out $(x - x_1)(x - x_2)$ we see that $x_3 \in \mathbb{Z}_p$, since the equation is monic, and reducing to $\mathbb{F}_p$ we see that x_3 lifts the x-coordinate of $\bar{P} \oplus \bar{Q}$. Similarly, factoring out the root $y_1 + s(x_1 - x_3)$ of the monic quadratic

$$y^2 + a_1x_3y + a_3y = x_3^3 + a_2x_3^2 + a_4x_3 + a_6$$

in y over $\mathbb{Z}_p$, we see that $y_3 \in \mathbb{Z}_p$ lifts the y-coordinate of $\bar{P} \oplus \bar{Q}$. $\square$

!5. Fix an elliptic curve $E/\mathbb{Q}$ given by $y^2 = x^3 + Ax + B$ and consider the family of its "quadratic twists",

$$d \cdot y^2 = x^3 + Ax + B,$$

where d runs over all square-free integers (ordered by absolute value). Show that 50% of the elliptic curves in this family have an infinite number of rational points.

3 Heights

Definition. For $\alpha = p/q \in \mathbb{Q}$ with p and q coprime, define the *height* of α

$$H(\alpha) = H_{\mathbb{Q}}(\alpha) = \max\{|p|, |q|\},$$

and the *logarithmic height* of α

$$h(\alpha) = \log H(\alpha).$$

Notation. For a rational function $f(x) = P(x)/Q(x) \in K(x)$ over a field K where $P(x), Q(x) \in K[x]$ have no common factor, we define the degree of f to be $\max\{\deg P, \deg Q\}$.

Proposition 16.

(i) $h(\alpha) \geq 0$ *for all* $\alpha \in \mathbb{Q}$.

(ii) $h(\alpha) = 0$ *iff* $\alpha \in \{0, 1, -1\}$.

(iii) $h(\alpha^d) = d \cdot h(\alpha)$ *for each* $d \geq 1$.

(iv) If $f(x) = (a_n x^n + \cdots + a_0)/(b_m x^m + \cdots + b_0) \in \mathbb{Q}(x)$ *has degree* d*, then* $h(f(\alpha)) = d \cdot h(\alpha) + O(1)$*, i.e. there is a constant* c *such that*

$$d \cdot h(\alpha) - c \leq h(f(\alpha)) \leq d \cdot h(\alpha) + c$$

for all $\alpha \in \mathbb{Q}$.

(v) The set $\{\alpha \in \mathbb{Q} : h(\alpha) < c\}$ *is finite for each* $c > 0$.

Proof. All except (iv) are clear. For (iv), we may assume without loss of generality that $n \geq m$, otherwise considering $1/f(x)$, and that $a_i, b_j \in \mathbb{Z}$. Write

$$f(S/T) = \frac{a_n S^n + \cdots + a_0 T^n}{(b_m S^m + \cdots + b_0 T^m) T^{n-m}} = \frac{A(S,T)}{B(S,T)},$$

with $A(S,1)$ and $B(S,1)$ coprime in $\mathbb{Q}[S]$. Then for $\alpha = p/q$, we have

$$|a_n p^n + \cdots + a_0 q^n| \leq (n+1) \max\{|a_i|\} \max\{|p|, |q|\}^n$$

and

$$|(b_m p^m + \cdots + b_0 q^m) q^{n-m}| \leq (m+1) \max\{|b_j|\} \max\{|p|, |q|\}^n,$$

so $H(f(\alpha)) \leq c_1 H(\alpha)^n$ where $c_1 = (n+1)\max(\{|a_i|\} \cup \{|b_j|\})$. On the other hand, since $A(S,1)$ and $B(S,1)$ are coprime in $\mathbb{Q}[S]$ we have some $\phi(S), \psi(S) \in \mathbb{Z}[S]$ with

$$A(S,1)\phi(S) + B(S,1)\psi(S) = d_1 \in \mathbb{Z}_{>0}.$$

By homogenizing terms, we get some $\tilde{\phi}(S,T), \tilde{\psi}(S,T) \in \mathbb{Z}[S,T]$ homogeneous of degree $N - n$ with

$$A(S,T)\tilde{\phi}(S,T) + B(S,T)\tilde{\psi}(S,T) = d_1 T^N$$

for a sufficiently large $N > n$. We also have that $A(1,T)$ and $B(1,T)$ are coprime in $\mathbb{Q}[T]$, and so for N large enough we also get $\tilde{\phi}'(S,T), \tilde{\psi}'(S,T) \in \mathbb{Z}[S,T]$ homogeneous of degree $N - n$ with

$$A(S,T)\tilde{\phi}'(S,T) + B(S,T)\tilde{\psi}'(S,T) = d_2 S^N,$$

where $d_2 \in \mathbb{Z}_{>0}$. Now $\gcd\{A(p,q), B(p,q)\}$ divides $d_1 p^N$ and $d_2 q^N$, and hence also $d_1 d_2$ since p and q are coprime. Then we have

$$H(f(\alpha)) \geq \frac{1}{d_1 d_2} \max\{|A(p,q)|, |B(p,q)|\},$$

and

$$\begin{aligned} d_1 |p|^N &\leq |A(p,q)||\tilde{\phi}(p,q)| + |B(p,q)||\tilde{\psi}(p,q)| \\ &\leq 2g_1 \max\{|A(p,q)|, |B(p,q)|\} \max\{|p|, |q|\}^{N-n} \end{aligned}$$

where g_1 is the maximal size of the coefficients in $\tilde{\phi}(S,T)$ and $\tilde{\psi}(S,T)$ multiplied by the number of monomials in both. Similarly

$$d_2 |q|^N \leq 2g_2 \max\{|A(p,q)|, |B(p,q)|\} \max\{|p|, |q|\}^{N-n}$$

for some constant g_2, and hence $H(f(\alpha)) \geq c_2 H(\alpha)^n$ where $c_2 = \frac{1}{2\max\{g_1 d_2, g_2 d_1\}}$. $\square$

Definition. Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$, and suppose $P = (x_0, y_0) \in E(\mathbb{Q})$. The *naive height* of P is $h_E(P) = h_{\mathbb{Q}}(x_0)$. (If $P = \mathcal{O}$ then $h_E(P) = 0$.)

Remark. For all $c > 0$, the set $\{P \in E(\mathbb{Q}) : h_E(P) < c)\}$ is finite by Proposition 16(v).

Lemma 17. *For $m \geq 1$ we have*

$$h_E(mP) = m^2 h_E(P) + O(1),$$

i.e. there is a constant c such that

$$m^2 h_E(P) - c \leq h_E(mP) \leq m^2 h_E(P) + c$$

for all $P \in E(\mathbb{Q})$.

Proof. This follows from Proposition 16, and the following lemma. □

Lemma 18. *For each $m \geq 1$ there is an $f(x) \in \mathbb{Q}(x)$ of degree m^2 such that if $P = (x_0, y_0) \in E(\mathbb{Q})$ then $mP = (f(x_0), \cdots)$.*

Proof. Applying the group law m times gives $\mathcal{X}_m(x,y), \mathcal{Y}_m(x,y) \in \mathbb{Q}(x,y)$ such that for $P = (x_0, y_0)$ we have $mP = (\mathcal{X}_m(x_0,y_0), \mathcal{Y}_m(x_0,y_0))$. Now since $y^2 = x^3 + Ax + B$ on E, and $1, y$ is a basis for $\mathbb{Q}(x,y)$ over $\mathbb{Q}(x,y^2)$, we can assume

$$\mathcal{X}_m(x,y) = g_1(x) + y g_2(x)$$

for some $g_1(x), g_2(x) \in \mathbb{Q}(x)$. By the uniformization theorem we have $E_{\mathbb{C}} \simeq E_\Lambda$ for some Λ, and by Proposition 2(ii) this isomorphism is given by a linear change of variables which due to the form of our equations preserves the given condition on $\mathcal{X}_m$ and $\mathcal{Y}_m$. Hence we may assume $E = E_\Lambda$, where we have

$$P = (x_0, y_0) = (\wp(z), \frac{1}{2}\wp'(z))$$

and

$$mP = (\mathcal{X}_m(x_0,y_0), \mathcal{Y}_m(x_0,y_0)) = (\wp(mz), \frac{1}{2}\wp'(mz))$$

according to the isomorphism with $\mathbb{C}/\Lambda$. Then $\wp(mz) = g_1(\wp(z)) + \frac{1}{2}\wp'(z) g_2(\wp(z))$, and since $\wp(mz)$ is even we must have $g_2(x) = 0$. Writing

$$g_1(\wp(z)) = \frac{\prod_i (\wp(z) - \alpha_i)}{\prod_j (\wp(z) - \beta_j)}$$

we see that $g_1(\wp(z))$ has $2 \deg g_1$ poles; each factor in the denominator has two zeros by Lemma 8, and excess of factors in the numerator contributes multiples of the double pole of $\wp(z)$. As $\wp(mz)$ has m^2 double poles, we must have $\deg g_1 = m^2$. □

Theorem 19 (Parallelogram Law)**.** *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$. Then for $P, Q \in E(\mathbb{Q})$ we have*

$$h(P \oplus Q) + h(P \ominus Q) = 2h(P) + 2h(Q) + O(1).$$

Proof. By applying the transformation $P = P' \oplus Q'$, $Q = P' \ominus Q'$ it suffices to prove the claim with $\leq$ in place of $=$. The proof is omitted. □

Theorem 20. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$. There is a unique function $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$, called the canonical height, such that:*

(i) $\hat{h}(P) = h(P) + O(1)$, *and*

(ii) $\hat{h}(mP) = m^2 \hat{h}(P)$ *for each* $P \in E(\mathbb{Q})$.

Moreover, it satisfies:

(iv) For each $c > 0$ the set $\{P \in E(\mathbb{Q}) : \hat{h}(P) < c\}$ is finite.

(v) The parallelogram law for $\hat{h}$ is satisfied exactly.

(vi) We have $\hat{h}(P) \geq 0$, with equality iff P has finite order.

(vii) The height pairing $\langle P, Q \rangle = \hat{h}(P \oplus Q) - \hat{h}(P) - \hat{h}(Q)$ is bilinear.

Proof. Suppose $\hat{h}$ and $\hat{h}'$ satisfy (i) and (ii). If $\hat{h}(P) \neq \hat{h}'(P)$ for some $P \in E(\mathbb{Q})$, then by (ii) with $m = 2$ we have

$$\hat{h}(2^n P) - \hat{h}'(2^n P) = 4^n \hat{h}(P) - \hat{h}'(P).$$

This is unbounded as n varies, contradicting the fact that $\hat{h}(P) - \hat{h}'(P) = O(1)$ from (i). To prove existence, define $\hat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h(2^n P)$. By the parallelogram law $h(2^n P) = 4^n h(P) + O(1)$, which shows that the limit converges and $\hat{h}(P) = h(P) + O(1)$. By construction (ii) holds for $m = 2$. Now for a given $k \geq 1$, define

$$\hat{h}'(P) = \frac{1}{k^2} \hat{h}(kP).$$

This satisfies (i), and (ii) with $m = 2$. Since the proof of uniqueness only used the $m = 2$ case of (ii) we have $\hat{h}' = \hat{h}$, proving (ii) for $\hat{h}$ with $m = k$. As k was arbitrary this proves (ii). The properties (iv) and (v) are clear from (i) and the corresponding facts about the naive height, while (vii) is a consequence of the parallelogram law. For (vi) the inequality is clear, and if $\hat{h}(P) = 0$ then $h(mP)$ is bounded as m varies by (i) and (ii), so $\{mP : m \geq 1\}$ is a finite set. $\square$

Corollary 21. *Elliptic curves over $\mathbb{Q}$ have only finitely many points of finite order.*

Lemma 22. *Let A be a countable abelian group with no elements of finite order, and $h : \mathcal{A} \to \mathbb{R}$ a positive-definite quadratic form such that*

$$\{p \in \mathcal{A} : h(p) < c\}$$

is finite for each $c > 0$. Then $\mathcal{A} \simeq \mathbb{Z}^{\oplus n}$ for some $n \in \mathbb{N}$ or $\mathcal{A} \simeq \mathbb{Z}^{\oplus \mathbb{N}}$.

Theorem 23. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q}) \simeq \Delta \times \mathbb{Z}^n$ or $\Delta \times \mathbb{Z}^{\mathbb{N}}$ for some finite group Δ.*

Proof. If Δ is the torsion subgroup of $E(\mathbb{Q})$, then by Corollary 21 it is a finite group, and by Theorem 20 the canonical height is a positive-definite quadratic form on $E(\mathbb{Q})/\Delta$, so we can apply Lemma 22. $\square$

Lemma 24.

(i) $P \in E(\mathbb{Q})$ has infinite order iff $\hat{h}(P) \neq 0$.

(ii) $P_1, \ldots, P_n \in E(\mathbb{Q})$ are linearly independent iff $\det(\langle P_i, P_j \rangle) \neq 0$.

Proof. This follows from Theorem 21. $\square$

Exercises

+1. Let $E/\mathbb{Q}$ be an elliptic curve given by $E : y^2 = x^3 + Ax + B$, and let $P \in E(\mathbb{Q})$. For $n \geq 1$ write $nP = (x_n, y_n)$. Use the canonical height to prove that

$$h_{\mathbb{Q}}(x_n) = n^2 a + O(1),$$

where the constant $a \in \mathbb{R}$ and the error term $O(1)$ may depend on E and P, but not on n.

Solution. We have

$$h_{\mathbb{Q}}(x_n) = \hat{h}(nP) + O(1) = n^2 \hat{h}(P) + O(1),$$

where the error term $O(1)$ doesn't depend on the point nP, so $a = \hat{h}(P)$ suffices. $\square$

+2. Let $E/\mathbb{Q}$ be the elliptic curve given by $y^2 = (x+1)(x+4)(x-5)$. Assuming that its group of rational points is isomorphic to $C_2 \times C_2 \times \mathbb{Z}$, prove that it is generated by $(-1, 0)$, $(5, 0)$ and $Q = (-3, 4)$. You may assume that for this curve

$$-5.60 \leq h(P) - \hat{h}(P) \leq 1.58$$

for all $P \in E(\mathbb{Q})$, and may find it helpful to know that $10Q$ has x-coordinate

$$\frac{661822357518174342999917659646891158606732140305553705}{311668667097257198712027230911109622652235276597856l6}.$$

(*Hint: Find an upper bound on $h(R)$ for the generator R of the copy of $\mathbb{Z}$ in $E(\mathbb{Q})$.*)

Solution. The two given points of order 2 must generate $C_2 \times C_2$. Let R denote a generator for the copy of $\mathbb{Z}$ in $E(\mathbb{Q})$, and suppose $Q = P \oplus nR$ where P is torsion and $n \in \mathbb{Z}$. If $|n| = 1$ we are done, so assume $|n| \geq 2$. We have $\hat{h}(Q) = \hat{h}(nR) = n^2\hat{h}(R)$ since the bilinear height pairing satisfies $2\langle P, Q\rangle = \langle 2P, Q\rangle = 0$. Counting digits in the above fraction gives $h(10Q) \leq 54\log 10$, so

$$\begin{aligned} h(R) \leq 1.58 + \hat{h}(R) &= 1.58 + \frac{\hat{h}(10Q)}{100n^2} \\ &\leq 1.58 + \frac{\hat{h}(10Q)}{400} \\ &\leq 1.58 + \frac{h(10Q) + 5.60}{400} \\ &\leq 1.58 + \frac{54\log 10 + 5.60}{400}. \end{aligned}$$

Then $H(R) \leq \exp(1.58 + \frac{54\log 10+5.60}{400}) \leq 6.72$, i.e. $H(R) \leq 6$. Since rational points of E have either $-4 \leq x \leq -1$ or $x \geq 5$, the possibilities for the x-coordinate of R are:

x	$(x+1)(x+4)(x-5)$	$\exists y$
$+5/1$	0	yes
$+6/1$	70	no
$-1/1$	0	yes
$-2/1$	14	no
$-3/1$	16	yes
$-3/2$	$65/8$	no
$-4/1$	0	yes
$-4/3$	$152/27$	no
$-5/2$	$135/8$	no
$-5/3$	$280/27$	no
$-5/4$	$275/64$	no
$-6/5$	$434/125$	no

The only non-torsion points from this list are $\pm Q$, contradicting $|n| \geq 2$ as required. $\square$

3. Prove that the two definitions of height on $\mathbb{Q}$ agree, i.e. that for $x = \frac{n}{m}$ with $n, m \in \mathbb{Z} \setminus \{0\}$ coprime,

$$\max(|n|, |m|) = \max(1, |x|) \cdot \prod_p \max(1, |x|_p) \qquad \text{where } |p^r \tfrac{a}{b}|_p = p^{-r} \text{ for } p \nmid a, b.$$

4. (i) Show that the number of rational points on an elliptic curve $E : y^2 = x^3 + Ax + B$ of height up to X is asymptotically $C \cdot X^{r/2}$, where r is the rank of $E/\mathbb{Q}$ and $C \in \mathbb{R}$ is some constant.

   (ii) Show that $C = |E(\mathbb{Q})_{\text{tors}}| \cdot \frac{\pi^{r/2}}{\Gamma(\frac{r}{2}+1)} \cdot \frac{1}{\sqrt{\operatorname{Reg}(E/\mathbb{Q})}}$, where $E(\mathbb{Q})_{\text{tors}}$ is the torsion subgroup of points of finite order of $E(\mathbb{Q})$ and $\operatorname{Reg}(E/\mathbb{Q})$ is the *regulator* of $E/\mathbb{Q}$, defined as

$$\operatorname{Reg}(E/\mathbb{Q}) = \det \begin{pmatrix} \langle P_1, P_1\rangle & \langle P_1, P_2\rangle & \cdots & \langle P_1, P_r\rangle \\ \vdots & & & \vdots \\ \langle P_r, P_1\rangle & \langle P_r, P_2\rangle & \cdots & \langle P_r, P_r\rangle \end{pmatrix}$$

   for any basis $P_1, \ldots, P_r$ of $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ and where $\langle , \rangle$ is the height pairing.
   (*The volume of an n-sphere of radius R is $\frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}R^n$.*)

!5. Either

   (i) Show that there are elliptic curves over $\mathbb{Q}$ with arbitrarily large rank, or

   (ii) Show that ranks of elliptic curves over $\mathbb{Q}$ are bounded.

4 Mordell–Weil Theorem

Notation. Let E/K be an elliptic curve, and F/K a field extension. For $P = (x_0, y_0) \in E(F)$ write

$$K(P) = K(x_0, y_0).$$

If F/K is Galois, write

$$\sigma(P) = (\sigma(x_0), \sigma(y_0))$$

for $\sigma \in \mathrm{Gal}(F/K)$. Note that $\sigma(P) \in E(F)$ since it satisfies the same equation with coefficients in K, and if $P, Q \in E(F)$ then

$$\sigma(P \oplus Q) = \sigma(P) \oplus \sigma(Q)$$

since σ sends lines to lines.

Lemma 25. *Let E/K be an elliptic curve with $K \subseteq \mathbb{C}$. Let $P \in E(K)$ and $n \in \mathbb{N}$.*

(i) There are n^2 points $Q \in E(\mathbb{C})$ with $nQ = P$.

(ii) $K(Q)$ is algebraic over K.

(iii) If $E(K)[n] = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ then

- *$K(Q_1) = K(Q_2)$ for $nQ_1 = nQ_2 = P$.*
- *$K(Q)/K$ is Galois.*
- *$\mathrm{Gal}(K(Q)/K) \leq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

Proof. Without loss of generality $E : y^2 = x^3 + Ax + B$ since $\mathrm{char}\, K = 0$.

(i) True by the uniformization theorem.

(ii) Recall from Lemma 18 that if $P = (x_0, y_0)$ then $nP = (f(x_0), \cdots)$ for some $f(x) \in K(x)$. Since $f(x_0) \in K$ we get that x_0 is algebraic over K, and since $y_0^2 = x_0^3 + Ax_0 + B$ we get that y_0 is algebraic over K.

(iii)
- We have
$$n(Q_1 \ominus Q_2) = nQ_1 \ominus nQ_2 = P \ominus P = \mathcal{O},$$
so $Q_1 = Q_2 \oplus T$ with $T \in E(\mathbb{C})[n]$. By assumption $E(K)[n] = E(\mathbb{C})[n]$, so $T \in E(K)[n]$, and hence $K(Q_1) = K(Q_2 \oplus T) \subseteq K(Q_2)$.
- If F/K is the Galois closure of $K(Q)$ and $\sigma \in \mathrm{Gal}(F/K)$, then
$$n \cdot \sigma(Q) = \sigma(nQ) = \sigma(P) = P,$$
so
$$\sigma(K(Q)) = K(\sigma(Q)) = K(Q).$$
As this holds for all $\sigma \in \mathrm{Gal}(F/K)$ we get that $F = K(Q)$ is Galois over K.
- Set $\sigma(Q) = Q \oplus T_\sigma$, so $T_\sigma \in E(K)[n]$. The map
$$\begin{aligned} \mathrm{Gal}(K(Q)/K) &\to E(K)[n] \\ \sigma &\mapsto T_\sigma \end{aligned}$$
is an injective group homomorphism:
  - Homomorphism: We have $T_{\sigma\tau} = T_\sigma \oplus T_\tau$ by applying $\tau \in \mathrm{Gal}(F/K)$ to $\sigma(Q) = Q \oplus T_\sigma$.
  - Injective: If $\sigma(Q) = Q$ then σ fixes $K(Q)$, and hence $\sigma = \mathrm{id}$.

$\square$

The strategy for proving the Mordell–Weil theorem is as follows:

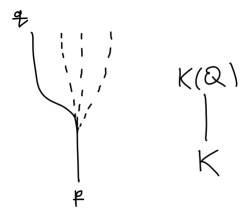
- Enlarge K so that $E(K)[2] = C_2 \times C_2$, i.e. $E : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$.
- Note that $\mathrm{Gal}(K(\frac{1}{2}P)/K) \leq C_2 \times C_2$, where $K(\frac{1}{2}P)$ means $K(Q)$ for Q satisfying $2Q = P$.

- Note that $K(\frac{1}{2}P)/K$ can only ramify at certain primes independent of the point P. (The primes dividing the discriminant of the curve.)
- Note that there are only finitely many such field extensions.
- Note that "Different points P give different fields $K(\frac{1}{2}P)/K$", or more correctly we have a finite-to-one map
$$E(K)/2E(K) \to \{\text{fields } K(\tfrac{1}{2}P)\}$$
- Deduce that $E(K)/2E(K)$ is finite.
- Using heights we know that $E(K) \cong \Delta \times \mathbb{Z}^n$ where Δ is a finite group and n is possibly infinite. But since $E(K)/2E(K)$ is finite we must have that n is finite (as otherwise $(\mathbb{Z}/2\mathbb{Z})^n$ is not finite.)

Notation. Let $K/\mathbb{Q}$ be a number field (or a local field), and let $\mathfrak{p}$ be a prime of K with residue field $\mathbb{F}_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$. For $P = (x_0 : \cdots : x_n) \in \mathbb{P}^n(K)$, find an $\alpha \in K$ such that $\alpha x_i \in \mathcal{O}_K$ for all i, and $\mathfrak{p} \nmid \alpha x_j$ for some j. Define the *reduction mod* $\mathfrak{p}$ of P to be
$$\overline{P} = (\overline{\alpha x_0} : \cdots : \overline{\alpha x_n}) \in \mathbb{P}^n(\mathbb{F}_\mathfrak{p}).$$
Note that this is well-defined; different α result in scalar multiples. If E/K is an elliptic curve given by
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{$*$}$$
with $a_i \in \mathcal{O}_K$ (or at least $\operatorname{ord}_\mathfrak{p} a_i \geq 0$), then reduction mod $\mathfrak{p}$ gives a map
$$\begin{aligned} E(K) &\to \overline{E}(\mathbb{F}_\mathfrak{p}) \\ (x_0, y_0) &\mapsto \begin{cases} (\overline{x_0}, \overline{y_0}) & \text{if } \mathfrak{p} \nmid \frac{1}{x_0}, \frac{1}{y_0} \\ \mathcal{O} & \text{otherwise,} \end{cases} \end{aligned}$$
where $\overline{E}$ is the (possibly singular) curve obtained by reducing $(*)$ mod $\mathfrak{p}$. If $\overline{E}$ is non-singular then this is a group homomorphism (reduction mod $\mathfrak{p}$ preserves lines).

Lemma 26. *Let K be a number field, and consider an elliptic curve*
$$E : y^2 = f(x) = (x-\alpha)(x-\beta)(x-\gamma)$$
with $\alpha, \beta, \gamma \in \mathcal{O}_K$ distinct. If $Q \in E(\overline{K})$ with $2Q \in E(K)$ then $K(Q)/K$ can only ramify at primes dividing
$$2\operatorname{Disc}(f(x)) = 2(\alpha-\beta)^2(\beta-\gamma)^2(\alpha-\gamma)^2.$$

Proof. Let $\mathfrak{p}$ be a prime of K with $\mathfrak{p} \nmid 2(\alpha-\beta)(\beta-\gamma)(\alpha-\gamma)$. Then $\overline{E}$ is an elliptic curve over $\mathbb{F}_\mathfrak{p}$, and
$$\overline{E}(\mathbb{F}_\mathfrak{p})[2] = \{\mathcal{O}, (\overline{\alpha}, 0), (\overline{\beta}, 0), (\overline{\gamma}, 0)\}.$$
Let $\mathfrak{q}$ be a prime of $K(Q)$ lying over $\mathfrak{p}$.



Recall the ramification index is given by $e_{\mathfrak{q}/\mathfrak{p}} = |I_{\mathfrak{q}/\mathfrak{p}}|$, where
$$I_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in \operatorname{Gal}(K(Q)/K) : \sigma(\mathfrak{q}) = \mathfrak{q} \text{ and } \sigma(t) = t \bmod \mathfrak{q} \text{ for all } t \in \mathcal{O}_{K(Q)}\}$$
is the inertia group. Hence it suffices to show that $\sigma(Q) = Q$ for all $\sigma \in I_{\mathfrak{q}/\mathfrak{p}}$, as then σ fixes $K(Q)$ so $\sigma = \text{id}$, meaning $I_{\mathfrak{q}/\mathfrak{p}}$ has order 1. Now for $\sigma \in I_{\mathfrak{q}/\mathfrak{p}}$, if $Q = (x_0, y_0)$ then
$$\sigma(x_0) = x_0 \bmod \mathfrak{p}, \quad \sigma(y_0) = y_0 \bmod \mathfrak{q}$$
so $\overline{\sigma(Q)} = \overline{Q}$, and $2\sigma(Q) = \sigma(2Q) = 2Q$, and hence $\sigma(Q) = Q \oplus T$ for some $T \in E(K)[2]$. Then $\overline{\sigma(Q)} = \overline{Q}$ implies $\overline{T} = \mathcal{O}$, and from the explicit list of points in $E(K)[2]$ we must have $T = \mathcal{O}$. Hence $\sigma(Q) = Q$ as required. $\square$

Lemma 27. *Let K be a number field.*

(i) If $a \in \mathcal{O}_K \setminus \{0\}$, and $(a) = \prod_i \mathfrak{p}_i^{n_i}$ for distinct primes $\mathfrak{p}_i$, then $K(\sqrt{a})/K$ ramifies at the $\mathfrak{p}_i$ where n_i is odd.

(ii) If S is a finite set of primes of K, then there are only finitely many quadratic extensions that ramify only at primes in S.

Proof. Exercise. $\square$

Lemma 28. *Let E/K be an elliptic curve over a number field with $E(K)[2] = C_2 \times C_2$. The map*

$$\begin{aligned} E(K)/2E(K) &\to \{F/K : \mathrm{Gal}(F/K) \leq C_2 \times C_2\} \\ P &\mapsto K(Q) \text{ where } Q \in E(\overline{K}) \text{ with } 2Q = P \end{aligned}$$

is well-defined, and finite-to-one.

Proof. Firstly, we check well-definedness:

- The Galois group satisfies the right condition by Lemma 25(iii).
- If $P = 2Q = 2Q'$ then $K(Q) = K(Q')$ by Lemma 25(iii).
- If $P' = P \oplus 2R$, and $2Q = P$, then $2Q' = P'$ for $Q' = Q \oplus R$, and $K(Q') \subseteq K(Q)$. We get equality by symmetry.

Suppose $P_1, \ldots, P_{17} \in E(K)$ have $P_i = 2Q_i$, where $Q_i \in E(\overline{K})$, and suppose all $K(Q_i)$ are equal to one field F. Write $\mathrm{Gal}(F/K) = \langle \sigma_1, \sigma_2 \rangle \leq C_2 \times C_2$, where possibly $\sigma_i = 1$. Then $\sigma_i(Q_j) = Q_j \oplus T$ with $T \in E(K)[2]$, and since $\#E(K)[2]^2 = 4^2 < 17$ we must have two points that have the same T for each σ_i; without loss of generality

$$\begin{aligned} \sigma_1(Q_1) &= Q_1 \oplus T & \sigma_1(Q_2) &= Q_2 \oplus T \\ \sigma_2(Q_1) &= Q_1 \oplus T' & \sigma_2(Q_2) &= Q_2 \oplus T' \end{aligned}$$

for some $T, T' \in E(K)[2]$. Then

$$\sigma_1(Q_1 \ominus Q_2) = Q_1 \ominus Q_2 = \sigma_2(Q_1 \ominus Q_2),$$

so $R = Q_1 \ominus Q_2 \in E(K)$. Hence $P_1 \ominus P_2 = 2R \in 2E(K)$, so the map is at most 16-to-1. $\square$

Theorem 29 (Weak Mordell–Weil Theorem)**.** *Let E/K be an elliptic curve over a number field, with $E(K)[2] = C_2 \times C_2$. Then $E(K)/2E(K)$ is finite.*

Proof. Without loss of generality $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ with $\alpha, \beta, \gamma \in \mathcal{O}_K$ distinct. By the previous lemma we have a finite-to-one map

$$E(K)/2E(K) \to \{F/K : \mathrm{Gal}(F/K) \leq C_2 \times C_2\}.$$

Now such F/K must be of the form $K(\sqrt{a}, \sqrt{b})$ for some $a, b \in K$, and must only ramify at finitely many $\mathfrak{p}$ (those satisfying $\mathfrak{p} \mid 2(\alpha-\beta)(\beta-\gamma)(\alpha-\gamma)$). There are only finitely many fields $K(\sqrt{a})$, $K(\sqrt{b})$ satisfying this ramification property by Lemma 27, and hence only finitely many such $K(\sqrt{a}, \sqrt{b})$. Therefore the codomain of the map is finite, so the domain is finite. $\square$

Remark 30. By some algebra one can check that $E(K)/2E(K)$ is finite even if $E(K)[2] \neq C_2 \times C_2$. (Apply the previous theorem over a splitting field of the cubic, and chase some diagrams.)

Theorem 31 (Mordell–Weil Theorem)**.** *Let E/K be an elliptic curve over a number field. Then $E(K)$ is finitely generated.*

Proof. Let $F = K(\alpha, \beta, \gamma)$, where $E : y^2 = f(x) = (x-\alpha)(x-\beta)(x-\gamma)$. Then by Theorem 23 (over number fields) we have

$$E(F) \cong \Delta \times \mathbb{Z}^n$$

where Δ is a finite group and n is possibly infinite. Then by Theorem 29 we have that $E(F)/2E(F)$ is finite, so n must be finite. Since $E(K) \leq E(F)$, and $E(F)$ is finitely generated, it follows that $E(K)$ is finitely generated. (Once can avoid using heights over number fields when $K = \mathbb{Q}$ by Remark 30.) $\square$

Example. Consider $E : y^2 = x^3 - x$ over $\mathbb{Q}$. Now

$$E(\mathbb{Q})[2] = \{\mathcal{O}, (0,0), (1,0), (-1,0)\} = C_2 \times C_2,$$

so $E(\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}^r$ for some n, m even and $r \geq 0$. Our proof of Theorem 29 gives a bound on r as follows: For $P \in E(\mathbb{Q})$, we have $\mathbb{Q}(\frac{1}{2}P) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ for some a, b, which only ramifies at $p \mid 2\,\mathrm{Disc}(x^3 - x) = -8$, i.e. at $p = 2$. Then 2 is the only prime factor of a and b, so $\mathbb{Q}(\frac{1}{2}P) \subseteq \mathbb{Q}(\sqrt{2}, i)$. By an argument as in Lemma 28, or see Exercise 3, we have an injective group homomorphism

$$\begin{aligned} E(\mathbb{Q})/2E(\mathbb{Q}) &\to \mathrm{Hom}(\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}), E(\mathbb{Q})[2]) \\ P &\mapsto (\sigma \mapsto \sigma(\tfrac{1}{2}P) \ominus \tfrac{1}{2}P). \end{aligned}$$

Now the Galois group of $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ is $C_2 \times C_2$, and $E(\mathbb{Q})[2] = C_2 \times C_2$, so we get

$$E(\mathbb{Q})/2E(\mathbb{Q}) \leq C_2 \times C_2 \times C_2 \times C_2,$$

and hence $\mathrm{rk}(E/\mathbb{Q}) = r \leq 2$. (In fact $r = 0$, which we will be able to prove later.)

Exercises

+1. Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ given by

$$E: \quad y^2 = (x - \alpha)(x - \beta)(x - \gamma) \qquad\qquad \alpha, \beta, \gamma \in \mathbb{Z}.$$

Find a crude[1] but completely explicit bound on the rank of $E/\mathbb{Q}$ in terms of α, β, γ.

Solution. For $P \in E(\mathbb{Q})/2E(\mathbb{Q})$ we have $\mathbb{Q}(\frac{1}{2}P) = \mathbb{Q}(\sqrt{a}, \sqrt{b})$ with $a, b \in \mathbb{Z}$ square-free and only divisible by the prime factors $p_1, \ldots, p_N$ of $2(\alpha - \beta)(\beta - \gamma)(\alpha - \gamma)$. This is then a subfield of $F = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_N}, i)$, and as in Exercise 3 we have an injective group homomorphism

$$\begin{aligned} E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Hom}(\mathrm{Gal}(F/\mathbb{Q}), E(\mathbb{Q})[2]) &\cong \mathrm{Hom}(\overbrace{C_2 \times \cdots \times C_2}^{N+1 \text{ times}}, C_2 \times C_2) \\ &\cong \overbrace{C_2 \times \cdots \times C_2}^{2N+2 \text{ times}}, \end{aligned}$$

implying that the rank of $E/\mathbb{Q}$ is at most $2N$. Now $\log p > 1$ for primes $p > 2$, so taking the logarithm of a prime factorization we see that

$$N \leq 1 + \log\bigl(|\alpha - \beta||\beta - \gamma||\alpha - \gamma|\bigr).$$

Hence

$$\mathrm{rk}(E/\mathbb{Q}) \leq 2 + 2\log\bigl(|\alpha - \beta||\beta - \gamma||\alpha - \gamma|\bigr).$$

□

+2. Suppose A is an abelian group with $A/2A$ finite that admits a function $h : A \to \mathbb{R}_{\geq 0}$ satisfying

- For every $C \in \mathbb{R}$ there are only finitely many $x \in A$ with $h(x) < C$, and
- $h(x+y) + h(x-y) = 2h(x) + 2h(y) + O(1)$, where the implied constant is independent of $x, y \in A$.

By expressing $x \in A$ as $x = a_1 + 2a_2 + \cdots + 2^n a_n + 2^{n+1} y$, where a_i are fixed representatives for $A/2A$, prove that A must be finitely generated. (This gives an elementary proof that Weak Mordell–Weil plus naive heights implies Mordell–Weil.)

Solution. Let $C > 0$ be such that $|h(x + y) + h(x - y) - 2h(x) - 2h(y)| \leq C$ for all $x, y \in A$. Fix a complete set $S \subseteq A$ of representatives for the elements of $A/2A$. Given $x \in A$, we have some $a_0 \in S$ with $x + a_0 = 2y$ for some $y \in A$, and continuing inductively we get $a_0, a_1, \ldots \in S$ sastifying $x + a_0 + 2a_1 + \cdots + 2^n a_n = 2^{n+1} y$ for some $y \in A$ for each n. Now

$$\begin{aligned} h(2^{n+1}y) = h(2^n y + 2^n y) &\geq 4h(2^n y) - h(0) - C \\ &\geq 4^{n+1} h(y) - (1 + 4 + 4^2 + \cdots + 4^n)(h(0) + C) \\ &\geq 4^{n+1}(h(y) - h(0) - C), \end{aligned}$$

[1] ideally logarithmic

and

$$\begin{aligned} h(2^{n+1}y) = h(2^n y + 2^n y) &\leq 4h(2^n y) - h(0) + C \\ &\leq 4^{n+1}h(y) + (1 + 4 + 4^2 + \cdots + 4^n)(C - h(0)) \\ &\leq 4^{n+1}(h(y) - h(0) + C), \end{aligned}$$

so we get that

$$\left| h(y) - \frac{h(2^{n+1}y)}{4^{n+1}} - h(0) \right| \leq C.$$

Then

$$\begin{aligned} h(2^{n+1}y) &= h(x + a_0 + 2a_1 + \cdots + 2^n a_n) \\ &\leq 2h(2^n a_n) + 2h(x + a_0 + 2a_1 + \cdots + 2^{n-1}a_{n-1}) + C \\ &\leq 2h(2^n a_n) + 2^2 h(2^{n-1}a_{n-1}) + \cdots + 2^{n+1}h(a_0) + 2^{n+1}h(x) + (1 + 2 + 2^2 + \cdots + 2^n)C \\ &\leq 2 \cdot 4^n \big(h(a_n) + C - h(0)\big) \\ &\qquad + 2^2 \cdot 4^{n-1}\big(h(a_{n-1}) + C - h(0)\big) \\ &\qquad + \cdots \\ &\qquad + 2^n \cdot 4^1 \big(h(a_1) + C - h(0)\big) + 2^{n+1}h(a_0) + 2^{n+1}h(x) + 2^{n+1}C \\ &\leq 2^{2n+1} \cdot \max_{a \in S}\big(h(a) + C - h(0)\big) + 2^{n+1}(h(x) + C), \end{aligned}$$

noting that $h(a_0) \leq h(a_0) + C - h(0)$ since $|2h(0) - 4h(0)| \leq C$ implies $h(0) \leq \frac{C}{2}$. Hence

$$\begin{aligned} h(y) &\leq 4^{-n-1}h(2^{n+1}y) + h(0) + C \\ &\leq 2^{-1} \cdot \max_{a \in S}\big(h(a) + C - h(0)\big) + 2^{-n-1}(h(x) + C), \end{aligned}$$

so for n large enough we have

$$h(y) \leq 2^{-1} \cdot \max_{a \in S}\big(h(a) + C - h(0)\big) + 1.$$

Now the set $T \subseteq A$ of y satisfying this inequality is finite, and since f is a linear combination of $a_0, a_1, \ldots \in S$ and $y \in T$, we see that the finite set $S \cup T$ generates A. □

3. Let E/K be an elliptic curve over a number field, such that $E(K)[2] \cong C_2 \times C_2$. Fix representatives $P_1, \ldots, P_k$ for $E(K)/2E(K)$, and let $Q_i \in E(\bar{K})$ satisfy $2Q_i = P_i$. Show that the number field $F = K(Q_1, \ldots, Q_k)$ generated by the x- and y-coordinates of the Q_i has Galois group of the form $G = \mathrm{Gal}(F/K) \cong C_2 \times \cdots \times C_2$.

   Verify that for a fixed P_i, the map $f_{P_i} : \sigma \mapsto \sigma(Q_i) \ominus Q_i$ is a homomorphism from G to $E(K)[2]$. Show furthermore that the association $P_i \mapsto f_{P_i}$ is an injective homomorphism from $E(K)/2E(K)$ to $\mathrm{Hom}(G, E(K)[2])$.

   Deduce that the rank of E/K is at most $2n - 2$, where $G \cong C_2 \times \cdots \times C_2$ (n times).

Solution. For the Galois group, by Lemma 25 we have

$$\mathrm{Gal}(K(Q_i)/K) \leq C_2 \times C_2,$$

so $K(Q_i) = K(\sqrt{a}, \sqrt{b})$ for some $a, b \in K$. Therefore F is given by adjoining at most $2k$ square roots to K, and hence G is isomorphic to a product of at most $2k$ copies of C_2. Now the maps f_{P_i} are independent of the choice of Q_i, since if $2Q_i' = P_i$ then $Q_i \ominus Q_i' \in E(F)[2]$, and $E(F)[2] = E(K)[2]$ since $E(K)[2] \cong C_2 \times C_2$, so $Q_i \ominus Q_i' \in E(K)$. Hence for $\sigma \in G$ we have

$$\sigma(Q_i \ominus Q_i') \ominus (Q_i \ominus Q_i') = (Q_i \ominus Q_i') \ominus (Q_i \ominus Q_i') = 0,$$

so $\sigma(Q_i) \ominus Q_i = \sigma(Q_i') \ominus Q_i'$. Also $2f_{P_i}(\sigma) = \sigma(P_i) \ominus P_i = 0$, and

$$\begin{aligned} f_{P_i}(\sigma\tau) &= \sigma\tau(Q_i) \ominus Q_i \\ &= (\sigma\tau(Q_i) \ominus \tau(Q_i)) \oplus (\tau(Q_i) \ominus Q_i) \\ &= f_{\tau(P_i)}(\sigma) \oplus f_{P_i}(\tau) \\ &= f_{P_i}(\sigma) \oplus f_{P_i}(\tau), \end{aligned}$$

so $f_{P_i}(\sigma) \in E(F)[2] = E(K)[2]$ and f_{P_i} is a homomorphism $G \to E(K)[2]$. Moreover

$$\begin{aligned} f_{P_i \oplus P_j}(\sigma) &= \sigma(Q_i \oplus Q_j) \ominus Q_i \ominus Q_j \\ &= \sigma(Q_i) \oplus \sigma(Q_j) \ominus Q_i \ominus Q_j \\ &= f_{P_i}(\sigma) \oplus f_{P_j}(\sigma), \end{aligned}$$

so this gives a homomorphism $E(K)/2E(K) \to \mathrm{Hom}(G, E(K)[2])$. If $f_{P_i} = 0$ then $\sigma(Q_i) = Q_i$ for all $\sigma \in G$, and hence $Q_i \in E(K)$, so $P_i \in 2E(K)$. Therefore this homomorphism is injective.

Now by the Mordell–Weil Theorem we have $E(K) \cong \Delta \times \mathbb{Z}^r$ for some finite group Δ, where r is the rank. Then

$$E(K)/2E(K) \cong E(K)[2] \times C_2^r \cong C_2^{r+2},$$

and from above this is a subgroup of

$$\mathrm{Hom}(G, E(K)[2]) = \mathrm{Hom}(C_2^n, C_2 \times C_2) = C_2^{2n}.$$

Hence $r + 2 \leq 2n$, i.e. $r \leq 2n - 2$. $\square$

4. Let E/K be an elliptic curve over a number field given by $y^2 = x^3 + ax^2 + bx + c$. For $d \in K^\times$, the *quadratic twist of E by d* is the elliptic curve given by

$$E_d : \quad d \cdot y^2 = x^3 + ax^2 + bx + c.$$

Prove that E and E_d are isomorphic over $K(\sqrt{d})$ and that (for $\sqrt{d} \notin K$)

$$\mathrm{rk}\, E/K(\sqrt{d}) = \mathrm{rk}\, E/K + \mathrm{rk}\, E_d/K.$$

!5. Prove that $y^2 + y = x^3 + x^2 + x$ has an infinite number of solutions over every cubic field of the form $\mathbb{Q}(\sqrt[3]{m})$ for $m \in \mathbb{Z}$.

5 Reduction mod p and Torsion

Definition. For E/K given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (*)$$

the *discriminant* of E is

$$\Delta_E = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6,\ b_8 = b_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

Remark. If $E : y^2 = f(x)$, i.e. $a_1 = 0 = a_3$, then $\Delta_E = 16\,\mathrm{Disc}(f)$. If $E : y^2 = x^3 + Ax + B$ then $\Delta_E = -16(4A^3 + 27B^2)$.

Proposition 32. *(i) E is non-singular iff $\Delta_E \neq 0$.*

(ii) If E, E' are isomorphic, related by a change of coordinates of the form

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

then $\Delta_{E'} = u^{12}\Delta_E$.

Proof. (i) See Silverman, Ch III, Prop 1.4.

(ii) Computation.

$\square$

Definition. Let K be a number field (or a non-Archimedean local field), and $\mathfrak{p}$ a prime of K. Let E/K be given by $(*)$. The equation is *integral* at $\mathfrak{p}$ if $\mathrm{ord}_\mathfrak{p}(a_i) \geq 0$ for all i. It is *minimal* at $\mathfrak{p}$ (or a minimal model for E at $\mathfrak{p}$) if it is integral with $\mathrm{ord}_\mathfrak{p}\Delta_E$ minimal among integral Weierstrass equations in the isomorphism class of E. The *reduced curve* at $\mathfrak{p}$ is then

$$\tilde{E}/\mathbb{F}_\mathfrak{p} : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

for any minimal model, where $\mathbb{F}_\mathfrak{p}$ is the residue field at $\mathfrak{p}$ and $\bar{a}_i$ denotes the reduction of a_i mod $\mathfrak{p}$.

Remark. The minimal model is unique up to transformations of the form

$$y' = u^3 y + sx_t,\, x' = u^2 x + r$$

where $\mathrm{ord}_{\mathfrak{p}}$ of u, s, t, r is ≥ 0 to preserve integrality and $\mathrm{ord}_{\mathfrak{p}}(u) = 0$ to preserve minimality by Proposition 32. This reduces to an isomorphism of reduced curves, so $\tilde{E}/\mathbb{F}_{\mathfrak{p}}$ is well-defined up to isomorphism.

Definition. E/K has *good reduction* at $\mathfrak{p}$ if $\tilde{E}/\mathbb{F}_{\mathfrak{p}}$ is non-singular, and *bad reduction* otherwise. We write

$$\tilde{E}_{\mathrm{ns}}(\mathbb{F}_{\mathfrak{p}}) \coloneqq \tilde{E}(\mathbb{F}_{\mathfrak{p}}) \setminus \{\text{the singular point if it exists}\}.$$

Proposition 33. *(i) E has good reduction at $\mathfrak{p}$ iff $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) = 0$ for a minimal model.*

(ii) If E is integral at $\mathfrak{p}$ and $\mathrm{ord}_{\mathfrak{p}}(\Delta_E) < 12$ then E is a minimal model.

(iii) $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_{\mathfrak{p}})$ is an abelian group with identity $\mathcal{O}$ and $P \oplus Q \oplus R = \mathcal{O}$ iff P, Q, R are collinear.

Proof. (i) Good reduction is equivalent to $\Delta_{\tilde{E}} \neq 0$ by Proposition 32(i), which is equivalent to $\Delta_E \neq 0$ mod $\mathfrak{p}$ for a minimal model.

(ii) Follows from Proposition 32(ii).

(iii) See Silverman, Ch III, Prop 2.5. (It is clear if $\tilde{E}$ is non-singular.)

□

Remark. We have the following taxonomy of reduction types:

- Good reduction $\iff$ $\tilde{E}$ is non-singular.
- Split multiplicative reduction $\iff$ $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_{\mathfrak{p}}) \cong \mathbb{F}_{\mathfrak{p}}^{\times}$.
- Non-split multiplicative reduction $\iff$ $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_{\mathfrak{p}}) \cong \mathbb{F}_{q^2}^{\times}/\mathbb{F}_q^{\times} \cong C_{q+1}$ where $q = |\mathbb{F}_{\mathfrak{p}}|$.
- Additive reduction $\iff$ $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_{\mathfrak{p}}) \cong (\mathbb{F}_{\mathfrak{p}}, +)$.

The last three are classified as bad reduction, and the first three are classified as "semistable" reduction. When $\mathfrak{p} \nmid 2$ there is a minimal model of the form $E : y^2 = f(x)$, and then we have the following characterizations:

- Good reduction $\iff$ $f(x)$ has distinct roots mod $\mathfrak{p}$.
- Multiplicative reduction $\iff$ $f(x)$ has a double root mod $\mathfrak{p}$. Here $\tilde{E}$ can be written as $y^2 = x^2(x+\eta)$, and $\eta \in (\mathbb{F}_{\mathfrak{p}}^{\times})^2 \iff$ the reduction is split multiplicative. (This is equivalent to the slopes of the two tangent lines being defined over $\mathbb{F}_{\mathfrak{p}}$.) The isomorphism

$$\tilde{E}_{\mathrm{ns}}(\mathbb{F}_{\mathfrak{p}}) \cong \mathbb{F}_{\mathfrak{p}}^{\times} \quad \text{or} \quad \mathbb{F}_{q^2}^{\times}/\mathbb{F}_q^{\times}$$

  is given by $(x, y) \mapsto -y/x$.
- Additive reduction $\iff$ $f(x)$ has a triple root mod $\mathfrak{p}$. Here the isomorphism

$$\tilde{E}_{\mathrm{ns}}(\mathbb{F}_{\mathfrak{p}}) \cong (\mathbb{F}_{\mathfrak{p}}, +)$$

  is given by $(x, y) \mapsto -y/x$.

Example. $E : y^2 = x^3 - 3 \cdot 5^4 x - 3 \cdot 5^6$ has $\Delta_E = -2^4 \cdot 3^3 \cdot 5^{13}$, and is integral but not minimal at 5; we can take

$$x = 5^2 x',\, y = 5^3 y'$$

to get

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

which is integral, and has $\Delta_{E'} = -2^4 \cdot 3^3 \cdot 5$, so it is minimal by Proposition 33(ii). The reduced curve is then

$$\tilde{E} : y^2 = x^3 + 2x + 2 = (x-1)^2(x+2)/\mathbb{F}_5$$

which is isomorphic to $y^2 = x^2(x+3)$, and hence has multiplicative reduction which is non-split as $3 \notin (\mathbb{F}_5^{\times})^2$. The points are

$$\tilde{E}(\mathbb{F}_5) = \{\text{the singular point } (1,0)\} \cup \{(2, \pm 2), (3, 0), (4, \pm 2), \mathcal{O}\},$$

and we see $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_5) \cong C_6$.

Remark. We have $\mathbb{Q} \subseteq \mathbb{Q}_p$, so $E(\mathbb{Q}) \subseteq E(\mathbb{Q}_p)$. In this and the following section we will describe $E(\mathbb{Q}_p)$.

Definition. Let E/K be an elliptic curve over a non-Archimedean local field (e.g. $\mathbb{Q}_p$). Then

$$\begin{aligned} E_0(K) &:= \{P \in E(K) : P \text{ reduces to a point in } \tilde{E}_{\mathrm{ns}}(\mathbb{F}_\mathfrak{p})\} \\ E_1(K) &:= \{P \in E(K) : P \text{ reduces to } \mathcal{O} \in \tilde{E}_{\mathrm{ns}}(\mathbb{F}_\mathfrak{p})\}. \end{aligned}$$

Lemma 34. *(i) $E_1(K) \leq E_0(K) \leq E(K)$ are subgroups.*

(ii) The reduction mod $\mathfrak{p}$ map $P \mapsto \tilde{P}$ is a homomorphism $E_0(K) \to \tilde{E}_{\mathrm{ns}}(\mathbb{F}_\mathfrak{p})$.

Proof. The inclusions are clear, $E_0(K)$ is a subgroup since $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_\mathfrak{p})$ is a group and the reduction map respects the group structure by Proposition 33(iii). Then $E_1(K)$ is also a subgroup, being the kernel of the reduction map. □

Theorem 35. *Let E/K be an elliptic curve over a non-Archimedean local field. Let $n = \operatorname{ord}_\mathfrak{p} \Delta_{E'}$ for a minimal model E' of E. Then $E(K)/E_0(K)$ is finite, and*

(i) $E(K)/E_0(K) = 1$ if E/K has good reduction.

(ii) $E(K)/E_0(K) \cong \mathbb{Z}/n\mathbb{Z}$ if E/K has split multiplicative reduction.

(iii) We have

$$E(K)/E_0(K) \cong \begin{cases} 1 & n \text{ odd} \\ \mathbb{Z}/2\mathbb{Z} & n \text{ even.} \end{cases}$$

if E/K has non-split multiplicative reduction.

(iv) $|E(K)/E_0(K)| \leq 4$ if E/K has additive reduction.

Proof. (i) is clear. For the rest, see Silverman's "Advanced Topics...". □

Remark. The order $|E(K)/E_0(K)|$ is called the *local Tamagawa number*, usually written $c_\mathfrak{p}$ or $c(E/K)$. The group $E(K)/E_0(K)$ and its order $c_\mathfrak{p}$ are fully determined by "Tate's algorithm".

Theorem 36. *Let E/K be ane elliptic curve over a non-Archimedean local field, given by a minimal Weierstrass equation. The reduction mod $\mathfrak{p}$ map induces an isomorphism*

$$E_0(K)/E_1(K) \xrightarrow{\sim} \tilde{E}_{\mathrm{ns}}(\mathbb{F}_\mathfrak{p}).$$

Proof. By Lemma 34 this is a homomorphism, which is injective by the definition of $E_1(K)$, so it suffices to prove surjectivity. Write the equation for E as

$$E : g(x,y) = 0, \quad g(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,$$

with $a_i \in \mathcal{O}_K$. If $P_0 = (x_0, y_0) \in \tilde{E}_{\mathrm{ns}}(\mathbb{F}_\mathfrak{p})$, we have either $\frac{\partial g}{\partial x}|_{P_0} \neq 0$ or $\frac{\partial g}{\partial y}|_{P_0} \neq 0$. By symmetry, assume $\frac{\partial g}{\partial y}|_{P_0} \neq 0$, and pick some $x \in \mathcal{O}_K$ with $\bar{x} = x_0$. Then by Hensel's lemma, we can solve $g(x,y) = 0$ for y subject to $\bar{y} = y_0$. □

Theorem 37. *Let $E/\mathbb{Q}_p$ be an elliptic curve. Then $E_1(\mathbb{Q}_p)$ contains no non-trivial points of finite order, except possibly points of order 2 if $p = 2$.*

Proof. This will be proved in the next section. □

Corollary 38. *Let $E/\mathbb{Q}$ be an elliptic curve, with p a prime of good reduction. Then the reduction map*

$$E(\mathbb{Q})_{\mathrm{tors}} \to \tilde{E}(\mathbb{F}_p)$$

is injective, except possibly if $p = 2$ where it may have kernel contained in $E(\mathbb{Q})[2]$.

Proof. The kernel is $\big(E(\mathbb{Q}) \cap E_1(\mathbb{Q}_p)\big)_{\mathrm{tors}}$. Now apply Theorem 37. □

Corollary 39 (Nagell–Lutz Theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve given by*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}.$$

If $P = (x_0, y_0)$ is a non-trivial point of finite order, then *(i)* $x_0, y_0 \in \mathbb{Z}$*, and*

(ii) $y_0 = 0$ *or* y_0^2 *divides* $4A^3 + 27B^2$.

Proof. (i) If P has order 2 then $y_0 = 0$, and x_0 is a root of $x^3 + Ax + B$, and hence is an integer by the rational root theorem. Now suppose P has order greater than 2. Let p be a prime, with E' a minimal model at p, and let $P' = (x_1, y_1)$ be the corresponding point on E'. By Theorem 37 we have $P' \notin E_1(\mathbb{Q}_p)$, so P' does not reduce to $\mathcal{O}$, and hence $x_1, y_1 \in \mathbb{Z}_p$ are p-adic integers. The change of coordinates

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

with some algebra then gives that $x_0, y_0 \in \mathbb{Z}_p$. Since $x_0, y_0 \in \mathbb{Q}$ it follows that $x_0, y_0 \in \mathbb{Z}$.

(ii) If $y_0 \neq 0$ we may check that

$$y_0^2(4f(x_0)x_1 - g(x_0)) = 4A^3 + 27B^2,$$

where $f(x) = 3x^2 + 4A$, $g(x) = 3x^2 - 5Ax - 27B$, and x_1 is the x-coordinate of $2P$, which is an integer by (i).

$\square$

Remark. Corollaries 38 and 39 give practical ways to determine $E(\mathbb{Q})_{\text{tors}}$; either compute $\tilde{E}(\mathbb{F}_p)$ for a few primes to bound $E(\mathbb{Q})_{\text{tors}}$, or factorize $4A^3 + 27B^2$ for possible y_0 and solve for x_0.

Exercises

+1. Let $E/\mathbb{Q}$ be the elliptic curve given by $y^2 + y = x^3 - x^2$. Show that E has discriminant -11 and that it has good reduction at 2 and split multiplicative reduction at 11. Prove that $E(\mathbb{Q})_{\text{tors}} \cong C_5$.

(*Recall from Exercise Sheet 1 that* $(0, 0) \in E(\mathbb{Q})$ *has order 5.*)

Solution. Using the formula for the discriminant, we have $a_1 = a_4 = a_6 = 0$ and $a_3 = -a_2 = 1$, so

$$b_2 = 0 - 4, b_4 = 0 + 0, b_6 = 1 + 0, b_8 = 0 + 0 - 1 + 0,$$

giving $\Delta_E = -(-4)^2(-1) + 0 - 27 + 0 = -11$. This is odd, so E has good reduction at 2. At 11 we have

$$y^2 + y = (y + 2^{-1})^2 - 4^{-1} = (y + 6)^2 - 3,$$

so E is given by $(y - 5)^2 = x^3 - x^2 + 3 = (x - 8)^2(x - 7)$. This is singular at $(8, 5)$ from the double root of $(x - 8)^2(x - 7)$, with split multiplicative reduction since $(x - 7) - (x - 8) = 1 \in (\mathbb{F}_{11}^\times)^2$. Now $E(\mathbb{Q})[2] = \{\mathcal{O}\}$, since $E : (y + \frac{1}{2})^2 = x^3 - x^2 + \frac{1}{4}$ with the cubic in x having no rational root. Hence by Corollary 38 the reduction mod 2 map $E(\mathbb{Q})_{\text{tors}} \to \tilde{E}(\mathbb{F}_2)$ is injective. But

$$\begin{aligned}\tilde{E}(\mathbb{F}_2) &= \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{F}_2^2 : y^2 + y = x^3 + x^2\} \\ &= \{\mathcal{O}\} \cup \mathbb{F}_2^2\end{aligned}$$

has order 5, so we see that $E(\mathbb{Q})_{\text{tors}}$ is either trivial or C_5. Since $(0, 0) \in E(\mathbb{Q})$ is a point of order 5, we must have $E(\mathbb{Q})_{\text{tors}} \cong C_5$. $\square$

+2. Show that $y^2 + y = x^3 - x$ has infinitely many rational solutions.

Solution. We have good reduction at 2, where the derivative of $y^2 + y$ is a non-zero constant, and also at 3, where the derivative of $x^3 - x$ is a non-zero constant. Writing E for the given curve, we have

$$\begin{aligned}\tilde{E}(\mathbb{F}_2) &= \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{F}_2^2 : y^2 + y = x^3 + x\} \\ &= \{\mathcal{O}\} \cup \mathbb{F}_2^2\end{aligned}$$

since $y^2 + y = 0 = x^3 + x$ for $x, y \in \mathbb{F}_2$, so we get $\tilde{E}(\mathbb{F}_2) \cong C_5$. Also

$$\begin{aligned}\tilde{E}(\mathbb{F}_3) &= \{\mathcal{O}\} \cup \{(x, y) \in \mathbb{F}_3^2 : y(y + 1) = x^3 - x\} \\ &= \{\mathcal{O}\} \cup \big(\{0, -1\} \times \mathbb{F}_3\big)\end{aligned}$$

since $x^3 - x = 0$ for $x \in \mathbb{F}_3$, so we get $\tilde{E}(\mathbb{F}_3) \cong C_7$. Hence by Corollary 38 we have only 2-torsion; $E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}[2]$. But the points of order 2 are given by $y = -\frac{1}{2}$ and $x^3 - x - \frac{1}{4} = 0$, and this cubic in x has no rational roots. Therefore $E(\mathbb{Q})_{\text{tors}}$ is trivial, so the point $(0, -1) \in E(\mathbb{Q})$ is non-torsion, and hence $E(\mathbb{Q})$ is infinite. $\square$

3. Show that if E does not have multiplicative reduction at 2, 3 or 5, then $|E(\mathbb{Q})_{\mathrm{tors}}| \leq 6$.

4. Suppose the elliptic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, with $a_i \in \mathbb{Q}$ is integral at p. Check that a substitution of the form $x = u^2x' + r$, $y = u^3y' + su^2x' + t$, for $r, s, t \in \mathbb{Z}$ and $u \in \mathbb{Q}^\times$ with $\mathrm{ord}_p\, u = 0$, yields another equation E' that is integral at p and with $\mathrm{ord}_p\, \Delta_E = \mathrm{ord}_p\, \Delta_{E'}$.

   Show also that there must be a substitution of this form with $r, s, t \in \mathbb{Z}$ and u purely a power of p, that will make the equation minimal at p.

   Prove that every elliptic curve over $\mathbb{Q}$ has a model which is minimal at all primes simultaneously. (This is called a *global minimal model*. What goes wrong over larger number fields?)

!5. Prove that there is a constant $C \in \mathbb{R}$ such that for every elliptic curve $E/\mathbb{Q}$,

$$\Delta_E < C \cdot P_E^{13},$$

   where Δ_E is the minimal discriminant of E and P_E is the product of the primes at which E has bad reduction.

6 Formal Groups

Proposition 40. *Let $E/\mathbb{Q}_p$ be an elliptic curve given by a minimal Weierstrass equation*

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}_p.$$

Then

(i) The map $E_1(\mathbb{Q}_p) \to \mathbb{Z}_p$ given by $(x_0, y_0) \mapsto -x_0/y_0$ and $\mathcal{O} \mapsto 0$ is a bijection.

(ii) There are Laurent series $x(t), y(t) \in \frac{1}{t^3}\mathbb{Z}_p[\![t]\!]$ such that the inverse of the above map is $t \mapsto (x(t), y(t))$. These are given by

$$\begin{aligned} x(t) &= \frac{1}{t^2} - \frac{a_1}{t} - a_2 - a_3t - (a_4 + a_1a_3)t^2 + \cdots \\ y(t) &= -\frac{1}{t^3} + \frac{a_1}{t^2} + \frac{a_2}{t} + a_3 + (a_4 + a_1a_3)t + \cdots . \end{aligned}$$

Proof. Set $w = -1/y$ and $t = -x/y$ to get a chart for E near $\mathcal{O}$ with the following equation:

$$w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3. \tag{$\dagger$}$$

In these coordinates $\mathcal{O}$ is $(0, 0)$ and $E_1(\mathbb{Q}_p)$ is precisely the set of points with $w, t \in p\mathbb{Z}_p$.

(i) For each $t \in p\mathbb{Z}_p$, the equation ($\dagger$) has a unique solution $w(t) \in p\mathbb{Z}_p$ by Hensel's lemma:

$$\left.\frac{\partial}{\partial w}\right|_{(0,0)} = 1 \neq 0 \quad \text{in } \mathbb{F}_p \qquad \Longrightarrow \exists! \text{ lift of } 0 \in \mathbb{F}_p \text{ to } w \equiv 0 \bmod p \text{ for any } t \equiv 0 \bmod p.$$

So $E_1(\mathbb{Q}_p) \to p\mathbb{Z}_p; (x_0, y_0) \mapsto (t, w) \mapsto t$ is a bijection.

(ii) Solving ($\dagger$) for $w(t) \in \mathbb{Z}_p[\![t]\!]$ expicitly (again Hensel's lemma) gives

$$w(t) = t^3 + a_1t^4 + (a_1^2 + a_2)t^5 + (a_1^3 + 2a_1a_2 + a_3)t^6 + \cdots$$

Note that this converges for $t \in p\mathbb{Z}_p$ as all the coefficients are integral, so this gives the value of $w(t)$ for $t \in p\mathbb{Z}_p$. Hence

$$\begin{aligned} x(t) = t/w(t) &= \frac{1}{t^2} - \frac{a_1}{t} - a_2 - a_3t - (a_4 + a_1a_3)t^2 + \cdots \\ y(t) = -1/w(t) &= -\frac{1}{t^3} + \frac{a_1}{t^2} + \frac{a_2}{t} + a_3 + (a_4 + a_1a_3)t + \cdots . \end{aligned}$$

$\square$

Proposition 41. *Let $E/\mathbb{Q}_p$ be an elliptic curve given by a minimal Weierstrass equation.*

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}_p.$$

Then

(i) *There is a unique power series*

$$\mathcal{F}_E(t_1, t_2) = t_1 + t_2 - a_1t_1t_2 - a_2(t_1^2t_2 + t_1t_2^2) + \cdots \in \mathbb{Z}[a_1, \ldots, a_6][\![t_1, t_2]\!]$$

such that for $t_3 = \mathcal{F}_E(t_1, t_2)$, we have

$$(x(t_1), y(t_1)) \oplus (x(t_2), y(t_2)) = (x(t_3), y(t_3))$$

in $E(K)$ for $K = \mathbb{Q}(a_1, \ldots, a_6)(\!(t_1, t_2)\!)$.

(ii) *There is a unique power series $\iota_E(t) \in \mathbb{Z}[a_1, \ldots, a_6][\![t]\!]$ such that*

$$\ominus(x(t), y(t)) = (x(\iota_E(t)), y(\iota_E(t))).$$

(iii) *These describe the elliptic curve's addition law on $p\mathbb{Z}_p$:*

$$\begin{tikzcd}
(P,Q) \arrow[r, mapsto] & P \oplus Q \\
E_1(\mathbb{Q}_p) \times E_1(\mathbb{Q}_p) \arrow[r] \arrow[d, "t=-x/y"'] & E_1(\mathbb{Q}_p) \arrow[d] \\
p\mathbb{Z}_p \times p\mathbb{Z}_p \arrow[r] & p\mathbb{Z}_p \\
(t_1,t_2) \arrow[r, mapsto] & \mathcal{F}_E(t_1,t_2)
\end{tikzcd}
\qquad
\begin{tikzcd}
P \arrow[r, mapsto] & \ominus P \\
E_1(\mathbb{Q}_p) \arrow[r] \arrow[d, "t=-x/y"'] & E_1(\mathbb{Q}_p) \arrow[d] \\
p\mathbb{Z}_p \arrow[r] & p\mathbb{Z}_p \\
t \arrow[r, mapsto] & \iota_E(t)
\end{tikzcd}$$

Proof. Let $(x(t), y(t)) \in E(K)$.

(ii) We have

$$\iota_E(t) = \frac{-x(t)}{-y(t) - a_1x(t) - a_3} \cdot \frac{t^3}{t^3} = \frac{t - a_1t^2 + \cdots}{1 + a_1t + \cdots} \in \mathbb{Z}[a_1, \ldots, a_6][\![t]\!].$$

(i) Let $P_1 = (x(t_1), y(t_1)), P_2 = (x(t_2), y(t_2)) \in E(K)$. The x- and y- coordinates of $P_1 \oplus P_2$ are rational functions in $x(t_i)$ and $y(t_i)$, hence lie in K, say

$$P \oplus Q = (x_3(t_1, t_2), y_3(t_1, t_2)) \in E(K).$$

Then

$$\mathcal{F}_E(t_1, t_2) = -x_3(t_1, t_2)/y_3(t_1, t_2) \in K$$

suffices. By an explicit computation we have $\mathcal{F}_E \in \mathbb{Z}[a_1, \ldots, a_6][\![t_1, t_2]\!]$ with the given leading terms.

(iii) This holds by construction, noting that the expressions converge for $t_1, t_2 \in p\mathbb{Z}_p$.

□

Definition. A (one-parameter, commutative) *formal group* over a ring R is a power series $\mathcal{F} \in R[\![X, Y]\!]$, such that

(i) $\mathcal{F}(X, Y) \in X + Y + (X, Y)^2$,

(ii) $\mathcal{F}(X, \mathcal{F}(Y, Z)) = \mathcal{F}(\mathcal{F}(X, Y), Z)$ (associativity),

(iii) $\mathcal{F}(X, Y) = \mathcal{F}(Y, X)$ (commutativity),

(iv) $\mathcal{F}(X, 0) = X$, $\mathcal{F}(0, Y) = Y$ (identity), and

(v) There exists a unique $i(T) \in R[\![T]\!]$ such that $\mathcal{F}(T, i(T)) = 0 = \mathcal{F}(i(T), T)$ (inverses).

Notation. We write $X \oplus_{\mathcal{F}} Y$ for $\mathcal{F}(X, Y)$. For $R = \mathbb{Z}_p$, we write $\mathcal{F}(p\mathbb{Z}_p)$ for the group $(p\mathbb{Z}_p, \oplus_{\mathcal{F}})$. Note that we have convergence of $\mathcal{F}(X, Y)$ to an element of $p\mathbb{Z}_p$ for $X, Y \in p\mathbb{Z}_p$.

Examples.

- $\hat{\mathbb{G}}_a(X, Y) = X + Y$, $\hat{\mathbb{G}}_a(p\mathbb{Z}_p) = (p\mathbb{Z}_p, +)$.
- $\hat{\mathbb{G}}_m(X, Y) = (1 + X)(1 + Y) - 1 = X + Y + XY$, $\hat{\mathbb{G}}_m(p\mathbb{Z}_p) \cong (1 + p\mathbb{Z}_p, \times)$.

Corollary 42. *$\mathcal{F}_E$ is a formal group over any ring $R \supseteq \mathbb{Z}[a_1, \ldots, a_6]$.*

Theorem 43. *Let $E/\mathbb{Q}_p$ be an elliptic curve given by a minimal Weierstrass equation. Then*

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

where $\hat{E} = \mathcal{F}_E$ is the formal group associated to E.

Proof. This follows from Corollary 42, Proposition 40, and Proposition 41. □

Lemma 44. *Let $\mathcal{F}$ be a formal group over R, and let $[n]$ denote the multiplication by n map, i.e.*

$$[n](T) = \underbrace{T \oplus_{\mathcal{F}} \cdots \oplus_{\mathcal{F}} T}_{n \text{ times}}.$$

Then $[n](T) = nT + (T^2) \in R[\![T]\!]$.

Proof. The case $n = 1$ is clear, and the rest follows by induction and part (i) of the definition. □

Lemma 45. *Suppose $f(T) = aT + O(T^2) \in R[\![T]\!]$ with $a \in R^\times$. Then there is a power series $g(T) \in R[\![T]\!]$ of the form $g(T) = a^{-1}T + O(T^2)$ such that $f(g(T)) = T = g(f(T))$.*

Proof. Write $f(T) = aT + a_2T^2 + a_3T^3 + \cdots$. Construct $g(T) = b_1T + b_2T^2 + \cdots$ as follows. Let $g_1(T) = b_1T$ where $b_1 = a^{-1} \in R$, so $f(g_1(T)) = T + c_2T^2 + \cdots$. Suppose we have $g_n(T) = b_1T + \cdots + b_nT^n$ such that $f(g_n(T)) = T + c_{n+1}T^{n+1} + \cdots$. Then let $g_{n+1}(T) = g_n(T) - \frac{c_{n+1}}{a}T^{n+1}$, i.e. $b_{n+1} = -\frac{c_{n+1}}{a}$. We get

$$\begin{aligned}
f(g_{n+1}(T)) &= f(g_n(T) - \frac{c_{n+1}}{a}T^{n+1}) \\
&= a(g_n(T) - \frac{c_{n+1}}{a}T^{n+1}) + a_2(\cdots)^2 + \cdots \\
&= f(g_n(T)) - c_{n+1}T^{n+1} + O(T^{n+2}) \\
&= T + O(T^{n+2}).
\end{aligned}$$

Thus $f(g(T)) = T$. Similarly we can construct $h(T) \in R[\![T]\!]$ such that $g(h(T)) = T$, and $h(T) = f(T)$ by a simple argument about monoids. □

Corollary 46. *Let $E/\mathbb{Q}_p$ be an elliptic curve. Then for $p \nmid n$, multiplication by n is an isomorphism*

$$E_1(\mathbb{Q}_p) \to E_1(\mathbb{Q}_p).$$

In particular $E_1(\mathbb{Q}_p)[n] = \{\mathcal{O}\}$.

Proof. Theorem 43 implies $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p)$ for a minimal model. As $n \in \mathbb{Z}_p^\times$ we get that $[n] : \hat{E}(p\mathbb{Z}_p) \to \hat{E}(p\mathbb{Z}_p)$ is both surjective and injective by Lemma 45. □

Remark. This works equally well over non-Archimedean local fields when n is coprime to the residue characteristic.

Theorem 47. *Let $E/\mathbb{Q}_p$ be an elliptic curve given by a minimal Weierstrass equation*

$$E : y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in \mathbb{Z}_p.$$

(i) If $p \neq 2$, then $E_1(\mathbb{Q}_p)$ has no elements of order p.

(ii) If $p = 2$ and $a_1 \equiv 0 \bmod 2$, then $E_1(\mathbb{Q}_p)$ has no elements of order 2.

(iii) If $p = 2$, then $E_1(\mathbb{Q}_p)$ has no elements of order 4.

Proof. (i) and (ii): Set $x = x'$, $y = y' - \frac{a_1}{2}x$. This gives another minimal model with no xy term, so we may assume $a_1 = 0$. Then

$$\mathcal{F}_E(t_1, t_2) = t_1 + t_2 - \cancelto{0}{a_1 t_1 t_2} + \cdots,$$

so by induction on n we get

$$[n](T) = nT + O(T^3).$$

If $\alpha \in p\mathbb{Z}_p \setminus \{0\}$ with $\operatorname{ord}_p(\alpha) = k$, then

$$[p](\alpha) = p\alpha + O(p^{3k}),$$

and $\operatorname{ord}_p(p\alpha) = k + 1 < 3k$, so $[p](\alpha) \neq 0$. Hence multiplication by p has trivial kernel on $\hat{E}(p\mathbb{Z}_p)$ and hence also on $E_1(\mathbb{Q}_p)$ by Theorem 43.
(iii) Exercise (hint: $2 + 2 = 4$). □

Corollary 48 (Theorem 37)**.** *If $E/\mathbb{Q}_p$ is an elliptic curve, then $E_1(\mathbb{Q}_p)$ has no points of finite order, except possibly those of order 2 when $p = 2$.*

Exercises

+1. Without moaning, honestly compute the first two leading terms of $x(t), y(t), w(t)$ and $\mathcal{F}_E(t_1, t_2)$.

Solution. Taking $w = -1/y$, $t = -x/y$ we have the equation

$$w = t^3 + a_1 tw + a_2 t^2 w + a_3 w^2 + a_4 t w^2 + a_6 w^3$$

which we want to solve for $w(t)$. Letting $w(t) = At^3 + Bt^4 + Ct^5 + O(t^6)$ we expand:

$$At^3 + Bt^4 + Ct^5 = t^3 + a_1 A t^4 + (a_1 B + a_2 A)t^5 + O(t^6),$$

so $A = 1$, $B = a_1$, $C = a_1^2 + a_2$, i.e. $w(t) = t^3 + a_1 t^4 + (a_1^2 + a_2)t^5 + O(t^6)$. Hence

$$y(t) = -1/w(t) = -\frac{1}{t^3} \cdot \frac{1}{1 + a_1 t + (a_1^2 + a_2)t^2 + O(t^3)} = -\frac{1}{t^3} + \frac{a_1}{t^2} + \frac{a_2}{t} + O(1),$$

and $x(t) = -ty(t) = \frac{1}{t^2} - \frac{a_1}{t} - a_2 + O(t)$. Note that the change of coordinates $(t, w) = (-x/y, -1/y)$ comes from a projective transformation, so we can compute the group law using lines in the (t, w)-plane. For formal variables t_1, t_2 with $w_i = w(t_i)$, the line through (t_i, w_i) has slope

$$d = \frac{w(t_2) - w(t_1)}{t_2 - t_1} = (t_1^2 + t_1 t_2 + t_2^2) + a_1(t_1^3 + t_1^2 t_2 + t_1 t_2^2 + t_2^3) + O(t_1, t_2)^4.$$

The two leading terms of the cubic giving the intersection of the line with the curve are

$$(1 + a_2 d + a_4 d^2 + a_6 d^3)t^3 + (a_2 w_1 + (a_1 - a_2 t_1 + 2w_1)d + (a_3 - 2t_1 + 3w_1)d^2 - 3t_1 d^3)t^2,$$

so the roots t_1, t_2, t_3 satisfy

$$-(t_1 + t_2 + t_3) = \frac{a_2 w_1 + (a_1 - a_2 t_1 + 2w_1)d + (a_3 - 2t_1 + 3w_1)d^2 - 3t_1 d^3}{1 + a_2 d + a_4 d^2 + a_6 d^3}.$$

Hence

$$-t_3 = t_1 + t_2 + a_1 d + O(t_1, t_2)^3 = t_1 + t_2 + a_1(t_1^2 + t_1 t_2 + t_2^2) + O(t_1, t_2)^3,$$

and the t coordinate $\mathcal{F}_E(t_1, t_2)$ of the sum of the points is given by the inverse $\iota_E(t_3)$, where

$$\iota_E(t) = \frac{x(t)}{y(t) + a_1 x(t) + a_3} = \frac{t - a_1 t^2 + O(t^3)}{-1 + 2a_1 t + O(t^2)} = -t - a_1 t^2 + O(t^3),$$

so

$$\begin{aligned}\mathcal{F}_E(t_1, t_2) &= t_1 + t_2 + a_1(t_1^2 + t_1 t_2 + t_2^2) - a_1(t_1 + t_2)^2 + O(t_1, t_2)^3 \\ &= t_1 + t_2 - a_1 t_1 t_2 + O(t_1, t_2)^3.\end{aligned}$$

(Here I wrote $O(t_1, t_2)^3$ to denote an element of the ideal $(t_1, t_2)^3 \subseteq \mathbb{Q}(a_1, \ldots, a_6)[\![t_1, t_2]\!]$ and similar.) □

+2. Let $E/\mathbb{Q}_2$ be an elliptic curve. Use the expression for the formal group law to show that $E_1(\mathbb{Q}_2)$ has no elements of order 4.

Solution. For $t \in 2\mathbb{Z}_2 \setminus \{0\}$ we have

$$[2](t) = \mathcal{F}_E(t,t) = 2t - a_1 t^2 + O(t^3) \in 2^2\mathbb{Z}_2,$$

so $[2](t) = 2^2 u$ for some $u \in \mathbb{Z}_2$. If $\operatorname{ord}_2(u) = k < \infty$ then

$$[4](t) = [2]([2](t)) = [2](4u) = 2^3 u - 2^4 a_1 u^2 + O((4u)^3) \equiv 2^3 u \bmod 2^{2k+4},$$

and hence $[4](t) = 0$ iff $u = 0$ iff $[2](t) = 0$ since $k + 3 < 2k + 4$. Hence $\hat{E}(2\mathbb{Z}_2) \cong E_1(\mathbb{Q}_2)$ has no elements of order 4. □

3. Let p be an odd prime and $E/\mathbb{Q}_p$ an elliptic curve given by a minimal Weierstrass equation. Show that the x-coordinate of any point in $E_1(\mathbb{Q}_p)$ is a perfect square.

4. Let μ be the Haar measure on $E(\mathbb{Q}_p)$ that, under the isomorphism $E_1(\mathbb{Q}_p) \cong p\mathbb{Z}_p$, maps to the usual Haar measure on $p\mathbb{Z}_p$ (i.e. the one that's inherited from $(\mathbb{Z}_p, +)$ and gives $\mathbb{Z}_p$ measure 1). Show that

$$\int_{E(\mathbb{Q}_p)} d\mu = c_p \cdot \frac{\#\tilde{E}(\mathbb{F}_p)}{p}.$$

!5. Let $E/\mathbb{Q}$ be an elliptic curve. Show that the product over all primes $\prod_p \frac{\#\tilde{E}(\mathbb{F}_p)}{p}$ converges if and only if $E(\mathbb{Q})$ is finite.

7 Descent

Lemma 49. *Let E/K be an elliptic curve with (for simplicity) $K \subseteq \mathbb{C}$, given by*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) \quad \alpha, \beta, \gamma \in K.$$

For $P \in E(K)$ write $\frac{1}{2}P \in E(\bar{K})$ for some point with $\frac{1}{2}P \oplus \frac{1}{2}P = P$.

(i) $K(\frac{1}{2}P)/K$ is Galois with $\mathrm{Gal}(K(\frac{1}{2}P)/K) \leq C_2 \times C_2$.

(ii) The map

$$\phi_P : \mathrm{Gal}(\bar{K}/K) \to E(K)[2]; \quad \phi_P(g) = g(\tfrac{1}{2}P) \ominus \tfrac{1}{2}P$$

is a well-defined homomorphism with kernel $\mathrm{Gal}(\bar{K}/K(\frac{1}{2}P))$.

(iii) The map

$$\phi : E(K)/2E(K) \to \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\bar{K}/K), E(K)[2]); \quad P \mapsto \phi_P$$

is a well-defined injective homomorphism.

Remark. A homomorphism $\phi : \mathrm{Gal}(\bar{K}/K) \to G$ for a finite group G is continuous if it comes from a finite Galois extension, i.e. there is F/K finite and Galois with $\tilde{\phi} : \mathrm{Gal}(F/K) \to G$ such that ϕ is the composition $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(F/K) \to G$. We say ϕ factors through F/K.

Proof. (i) By Lemma 25, since $E(K)[2] = \{\mathcal{O}, (0,\alpha), (0,\beta), (0,\gamma)\}$.

(ii) See the proof of Lemma 25(iii).

(iii) See Sheet 4, Exercise 3. Note that ϕ_P is continuous by (ii).

□

Remark. This is a refinement of our 16-to-1 map $P \mapsto K(\frac{1}{2}P)$; $P \mapsto \phi_P$ is now injective, respects addition, and recovers $K(\frac{1}{2}P)$ as the fixed field of $\ker \phi_P$.

Lemma 50. *Let E/K be an elliptic curve with $K \subseteq \mathbb{C}$, given by*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) \quad \alpha, \beta, \gamma \in K.$$

(i) We have a map

$$\eta : \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\bar{K}/K), E(K)[2]) \to \frac{K^\times}{K^{\times 2}} \times \frac{K^\times}{K^{\times 2}} \times \frac{K^\times}{K^{\times 2}}; \quad \psi \mapsto (\psi_\alpha, \psi_\beta, \psi_\gamma)$$

where $\psi(g) \in \{\mathcal{O}, (\alpha, 0)\}$ iff $g \in \mathrm{Gal}(\bar{K}/K(\sqrt{\psi_\alpha}))$, and similar for β, γ. Then η is an injective homomorphism; an isomorphism onto the subgroup of triples a, b, c with $abc \in K^{\times 2}$.

$$\begin{tikzcd}[arrows=dash]
 & K(\frac{1}{2}P) \arrow[dl] \arrow[d] \arrow[dr] & \\
K(\sqrt{\psi_\alpha}) \arrow[dr] & K(\sqrt{\psi_\beta}) \arrow[d] & K(\sqrt{\psi_\gamma}) \arrow[dl] \\
 & K &
\end{tikzcd}$$

(ii) If $P = (x_0, y_0) \in E(K)$ then $\eta(\phi_P) = (x_0 - \alpha, x_0 - \beta, x_0 - \gamma)$ unless $x_0 = \alpha$, in which case the first entry is $(x_0 - \beta)(x_0 - \gamma)$, and similar for β, γ.

Remark. . (i) simply records the subfields of $K(\frac{1}{2}P)$ associating each quadratic to a specific 2-torsion point. (ii) says that these quadratics are just $K(\sqrt{x_0 - \alpha})$, $K(\sqrt{x_0 - \beta})$, $K(\sqrt{x_0 - \gamma})$. Keeping this extra structure preserves the group structure on $E(K)$.

Proof. (i) $\mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(\bar{K}/K), C_2) \simeq K^\times/K^{\times 2}$ via $\psi \mapsto d$ for $\ker\psi = \mathrm{Gal}(\bar{K}/K(\sqrt{d}))$. This is a homomorphism since if $\ker\psi_i = \mathrm{Gal}(\bar{K}/K(\sqrt{d_i}))$ for $i = 1, 2$ then $\ker(\psi_1\psi_2) = \mathrm{Gal}(\bar{K}/K(\sqrt{d_1}\sqrt{d_2}))$. Now apply to $E(K)[2] \cong C_2 \times C_2$ to get $K^\times/K^{\times 2} \times K^\times/K^{\times 2} \times K^\times/K^{\times 2}$. Recording the third homomorphism gives the required map η.

(ii) (Sketch) If $E : y^2 = x^3 + Ax^2 + Bx$, then for $Q = (x_0, y_0)$ we have

$$2Q = \left(\left(\frac{x_0 - B}{2y_0} \right)^2, \dots \right).$$

Hence if $2Q = P = (x_1, y_1)$ then $K(\frac{1}{2}P)$ contains $\sqrt{x_1}$, so if $E : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$ with $P = (x_2, y_2)$ then

$$K(\tfrac{1}{2}P) \supseteq K(\sqrt{x_2 - \alpha}), K(\sqrt{x_2 - \beta}), K(\sqrt{x_2 - \gamma}).$$

Using α, β, γ as variables, and that $\mathrm{Gal}(K(\frac{1}{2}P)/K) \leq C_2 \times C_2$, we can deduce that

$$K(\tfrac{1}{2}P) = K(\sqrt{x_2 - \alpha}, \sqrt{x_2 - \beta}, \sqrt{x_2 - \gamma})$$

and no larger. Keep track of the Galois action to identify subfields for the final result.

□

Example. Consider $E : y^2 = x(x - 1)(x + 1)$. Recall for $P \in E(\mathbb{Q})$ that $\mathbb{Q}(\frac{1}{2}P)/\mathbb{Q}$ only ramifies at $p = 2$, so $\mathbb{Q}(\frac{1}{2}P) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Now $P = (x_0, y_0) \mapsto (x_0, x_0 - 1, x_0 + 1) \in (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^3$ is a homomorphism giving the quadratic subfields of $\mathbb{Q}(\frac{1}{2}P)$. Hence $x_0, x_0 - 1, x_0 + 1$ are given up to squares by elements of $\{\pm 1, \pm 2\}$. We go through the possibilities:

x_0	$x_0 - 1$	$x_0 + 1$	$\in$ image?
$+1$	$+1$	$+1$	yes; 1)
$+1$	-1	-1	no; 2)
$+1$	$+2$	$+2$	yes; 1)
$+1$	-1	-1	no; 2)
-1	$+1$	-1	no; 2)
-1	-2	$+2$	yes; 1)
-1	$+2$	-2	no; 2)
-1	-1	$+1$	yes; 1)
$+2$	$+1$	$+2$	no; 3)
$+2$	-2	-1	no; 2)
$+2$	$+2$	$+1$	no; 4)
$+2$	-1	-2	no; 2)
-2	$+1$	-2	no; 2)
-2	-1	$+2$	no; 4)
-2	$+2$	-1	no; 2)
-2	-2	$+1$	no; 4)

1) We have the 2-torsion points $(0,0),(1,0),(-1,0),\mathcal{O}\in E(\mathbb{Q})$.

2) We must have $x_0+1>0$, and $x_0(x_0-1)>0$.

3) We prove directly that the triple $(2,1,2)$ cannot occur. If $x_0=2a^2$, $x_0-1=b^2$ and $x_0+1=2c^2$ with $a,b,c\in\mathbb{Q}^\times$, take a denominator $z\in\mathbb{Z}$ such that $az\in\mathbb{Z}$ and $(az,z)=1$. Then $2(az)^2-z^2=(bz)^2$ and $2(az)^2+z^2=2(cz)^2$, so $A=az, B=bz, C=cz$ are integers satisfying $2A^2-z^2=B^2$, $2A^2+z^2=2C^2$, and $(A,z)=1$.

   - If A is even then z is odd, so $B^2\equiv -1 \bmod 8$, which is impossible.
   - If A is odd, then $A^2\equiv 1 \bmod 8$. If z is also odd then $2C^2\equiv 3 \bmod 8$, which is impossible, and if z is even then $B^2\equiv 2$ or $6 \bmod 8$, which is also impossible.

4) As the map is a homomorphism, the image is a subgroup.

Hence $\#E(\mathbb{Q})/2E(\mathbb{Q})=4$ so $\operatorname{rk} E=0$.

Theorem 51 (Complete 2-descent)**.** *Let K be a field of characteristic 0, and E/K an elliptic curve given by*

$$E: y^2=(x-\alpha)(x-\beta)(x-\gamma),\quad \alpha,\beta,\gamma\in K.$$

(i) The map $P\mapsto(x_0-\alpha,x_0-\beta,x_0-\gamma)$, replacing terms with the product of the other two if they vanish, and letting $\mathcal{O}\mapsto(1,1,1)$, is an injective homomorphism $E(K)/2E(K)\to(K^\times/K^{\times 2})^3$.

(ii) The triples (a,b,c) that lie in the image satisfy $abc\in K^{\times 2}$. Either they are in the image of $E(K)[2]$, or

$$cz_3^2-\alpha+\gamma=az_1^2,\quad cz_3^2-\beta+\gamma=bz_2^2$$

is soluble with $z_i\in K^\times$, in which case $P=(az_1^2+\alpha,\sqrt{abc}z_1z_2z_3)$ maps to (a,b,c).

(iii) If K is a number field, and (a,b,c) is in the image, then $K(\sqrt{a},\sqrt{b},\sqrt{c})/K$ only ramifies at primes dividing $2(\alpha-\beta)(\beta-\gamma)(\alpha-\gamma)$. If $K=\mathbb{Q}$, then taking $a,b,c\in\mathbb{Z}$ square-free we get that a,b,c only have prime factors $p\mid 2(\alpha-\beta)(\beta-\gamma)(\alpha-\gamma)$, assuming $\alpha,\beta,\gamma\in\mathbb{Z}$.

Proof. (i) Lemma 50.

(ii) Solve $x_0-\alpha=az_1^2$, $x_0-\beta=bz_2^2$, $x_0-\gamma=cz_3^2$.

(iii) Lemma 26.

□

Proposition 52. *Suppose $E/\mathbb{Q}_p$ is an elliptic curve, given by*

$$E: y^2=(x-\alpha)(x-\beta)(x-\gamma),\quad \alpha,\beta,\gamma\in\mathbb{Z}_p.$$

(i) If $p\neq 2$ then $\#E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)=4$.

(ii) If $p\nmid 2\Delta_E$ then $\mathbb{Q}_p(\frac{1}{2}P)/\mathbb{Q}_p$ is unramified for $P\in E(\mathbb{Q}_p)$.

(iii) If $p\nmid 2\Delta_E$ then (a,b,c) lies in the image of $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ iff $\operatorname{ord}_p(a),\operatorname{ord}_p(b),\operatorname{ord}_p(c)$ are all even and $abc\in\mathbb{Q}_p^{\times 2}$.

Remark. (iii) says that only p dividing $2\Delta_E$ give interesting constraints on the triples (a,b,c).

Proof. (i) Consider

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E_1(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) & \longrightarrow & 0\\
 & & \downarrow{\scriptstyle\times 2} & & \downarrow{\scriptstyle\times 2} & & \downarrow{\scriptstyle\times 2} & & \\
0 & \longrightarrow & E_1(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{Q}_p) & \longrightarrow & E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p) & \longrightarrow & 0.
\end{array}$$

If K_1,K_2,K_3,C_1,C_2,C_3 are the kernels and cokernels, we have the snake lemma:

$$0\to K_1\to K_2\to K_3\to C_1\to C_2\to C_3\to 0.$$

By Corollary 46 the map $E_1(\mathbb{Q}_p)\xrightarrow{\times 2}E_1(\mathbb{Q}_p)$ is an isomorphism, so $K_1=C_1=0$. Therefore

$$\#E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)=\#C_2=\#C_3=\#K_3=\#K_2=\#E(\mathbb{Q}_p)[2]=4.$$

(ii) Lemma 26.

(iii) Exercise (use (i) and (ii)).

$\square$

Example. Consider $E : y^2 = x(x-5)(x+5)$, with $\Delta_E = -2^6 5^6$, and recall the map

$$\begin{aligned} E(\mathbb{Q})/2E(\mathbb{Q}) &\to (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})^3 \\ P = (x_0, y_0) &\mapsto (x_0, x_0 - 5, x_0 + 5). \end{aligned}$$

Possible triples (a, b, c) in the image have $a, b, c \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ and $abc = 1$ up to squares.

- Over $\mathbb{R}$: The image of $E(\mathbb{R})$ is $\{(+,+,+), (-,-,+)\}$.
- Over $\mathbb{Q}_5$: We have representatives for $\mathbb{Q}_5^\times/\mathbb{Q}_5^{\times 2}$ given by $1, 2, 5, 10$. Note that $-1 \in \mathbb{Q}_5^{\times 2}$. We know there are only 4 triples coming from $E(\mathbb{Q}_5)$ by Proposition 52(i). These must be $(1,1,1)$, $(1,5,5)$, $(5,2,10)$, $(5,10,2)$ from the 2-torsion points.

Combining this information we deduce that $P \in E(\mathbb{Q})$ can only have image in

$$\{(1,1,1), (-1,-1,1), (1,5,5), (-1,-5,5), (5,2,10), (-5,-2,10), (5,10,2), (-5,-10,2)\}.$$

Now $\mathcal{O} \mapsto (1,1,1)$, $(0,0) \mapsto (-1,-5,5)$, $(5,0) \mapsto (5,2,10)$, $(-5,0) \mapsto (-5,-10,2)$, and we have the point $P = (-4,6) \mapsto (-1,-1,1)$, so the image (which is a subgroup) must be the whole of this set. From this we deduce that $\operatorname{rk} E(\mathbb{Q}) = 1$.

Exercises

+1. Compute the rank of $E : y^2 = x(x+3)(x-6)$ over $\mathbb{Q}$. (*Hint:* $(-2, 4) \in E(\mathbb{Q})$.)

+2. Compute the rank of $E : y^2 = x^3 - 49x$ over $\mathbb{Q}$. (*Hint:* $(25, 120) \in E(\mathbb{Q})$.)

3. Let $E/\mathbb{Q}_2$ be an elliptic curve with $E(\mathbb{Q}_2)[2] = C_2 \times C_2$. Show that $|E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)| = 8$.

4. Let K be a field of characteristic 0 that contains the p^{th} roots of unity, for some prime p. Show that $\operatorname{Hom}_{\text{cts}}(\operatorname{Gal}(\bar{K}/K), \mathbb{Z}/p\mathbb{Z}) \cong K^\times/K^{\times p}$.

!5. Let $E/\mathbb{Q}$ be an elliptic curve given by $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ for some $\alpha, \beta, \gamma \in \mathbb{Z}$. Let S denote the group of those triples $(a,b,c) \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2} \times \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ with $abc \in \mathbb{Q}^{\times 2}$, which (when working modulo $\mathbb{R}^{\times 2}$ or $\mathbb{Q}_p^{\times 2}$) lie in the image of $E(\mathbb{R})/2E(\mathbb{R})$ and $E(\mathbb{Q}_p)/2E(\mathbb{Q}_p)$ for every prime p. Prove that $|S| = 2^{\operatorname{rk}(E/\mathbb{Q})+n}$ for some even integer n.