Homework for Elliptic Curves

Nicolas Keng

2025/10/22

1 Example Sheet 1

Exercise 1.1 Alter building Vadic priests in India knew by about 800BC how to construct rational right-angled trianges with areas 6,15,21 and 210. Repeat their discovery.

Proof. Note that $a^2 + b^2 = c^2$ corresponds to the Pythagorean array:

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

1. Take $m = 2$, $n = 1$, the triangle has sides $(3, 4, 5)$, and the area is 6;
2. Take $m = 4$, $n = 1$ and then reduce the area by half, the triangle has sides $\left(4, \frac{15}{2}, \frac{17}{2}\right)$, and the area is 15;
3. Take $m = 4$, $n = 3$ and then reduce the area by half, the triangle has sides $\left(\frac{7}{2}, 12, \frac{25}{2}\right)$, and the area is 21;
4. Take $m = 5$, $n = 2$, the side length of the triangle is $(20, 21, 29)$, and the area is 210.

□

Exercise 1.2 Find rational parametrisations for the plane conic $x^2 + xy + 3y^2 = 1$ and for the singular plane cubic $y^2 = x^2(x + 1)$.

Proof. For $x^2 + xy + 3y^2 = 1$, $(-1, 0)$ is a solution. Substitute $y = k(x + 1)$ into $x^2 + xy + 3y^2 = 1$, we have

$$(3k^2 + k + 1)x^2 + (6k^2 + k)x + (3k^2 - 1) = 0,$$

by Vieta's Theorem we know $x = -\dfrac{3k^2 - 1}{3k^2 + k + 1}$, thus $y = \dfrac{k(k + 2)}{3k^2 + k + 1}$.

For $y^2 = x^2(x + 1)$, $(0, 0)$ is a singularity. Reshaping the original equation yields $\left(\dfrac{y}{x}\right)^2 = x + 1$. Taking $t = \dfrac{y}{x}$, we obtain $t^2 = x + 1$, $x = t^2 - 1$. Substituting $y = tx$, we know $y = t(t^2 - 1)$. Therefore, the rational parametrization of the curve is

$$x = t^2 - 1, \quad y = t(t^2 - 1).$$

□

Exercise 1.3 Consider the curve $C_d = \{U^d + V^d = W^d\} \subset \mathbb{P}^2$ defined over $\mathbb{Q}$.

(i) Find the points of inflection on C_3, and then put this curve in Weierstrass form.

(ii) Let $x, y \in \mathbb{Q}(C_4)$ be given by $x = W^2/U^2$ and $y = V^2W/U^3$. Show that $y^2 = x^3 - x$, and hence find all the $\mathbb{Q}$-rational points on C_4.

Proof. (i) The inflection point makes the quadratic partial derivative of $F(U, V, W) = U^3 + V^3 - W^3$ be zero. Calculation yields $F_{UU} = 6U$, $F_{VV} = 6V$, $F_{WW} = -6W$. Thus, the inflection point should make $UVW = 0$.

1. If $U = 0$, then $V^3 = W^3 \Rightarrow V = \zeta_3 W$, with inflection points at $(0 : 1 : 1)$, $(0 : \zeta_3 : 1)$, $(0 : \zeta_3^2 : 1)$;
2. If $V = 0$, then $U^3 = W^3 \Rightarrow U = \zeta_3 W$, with inflection points at $(1 : 0 : 1)$, $(\zeta_3 : 0 : 1)$, $(\zeta_3^2 : 0 : 1)$;
3. If $W = 0$, then $V^3 + U^3 = 0 \to U = -\zeta_3 V$, with inflection points at $(1 : -1 : 0)$, $(1 : -\zeta_3 : 0)$, and $(1 : -\zeta_3^2 : 0)$.

By transforming $x = \dfrac{12W}{U+V}$, $y = \dfrac{36(U-V)}{U+V}$, the curve becomes the standard Weierstrass form

$$y^2 = x^3 - 432.$$

(ii) We use the infinite descent method to demonstrate that $x^4 + y^4 = (x^2)^2 + (y^2)^2 = z^2$ has no positive integer solutions. If not, we assume that (x, y, z) is the z smallest positive integer solution. This demonstrates that C_4 has positive integer solutions only when z is odd, and x and y are both odd and even. Let's assume x is even, y and z are odd. Using the Pythagorean construction, we have:

$$x^2 = 2mn,\ y^2 = m^2 - n^2,\ z = m^2 + n^2.$$

Note that $n^2 + y^2 = m^2$, which makes (n, y, m) form a new set of Pythagorean ratios. Verifying by mod4, we know that n is even and m is odd. Again using the Pythagorean construction, we have:

$$n = 2pq,\ y = p^2 - q^2,\ m = p^2 + q^2.$$

Note that m and n coprime, and p and q coprime. Therefore, we have p, q, and $m = p^2 + q^2$ coprime.

Substituting into the equation, we obtain $x^2 = 4pq(p^2 + q^2)$, which means that p, q, and m are all squares, i.e.$p = r^2$, $q = s^2$, $m = t^2$.

Substituting into $m = p^2 + q^2$, we find that $r^4 + s^4 = t^2$, and (r, s, t) also forms a set of positive integer solutions to the original equation. However, it is clear that $t < z$, which contradicts the assumption that (x, y, z) is the z smallest positive integer solution. This also shows that C_4 has no positive integer solutions. The only rational points for $y^2 = x^3 - x$ are $(0, 0)$, $(\pm 1, 0)$, and $\mathcal{O}$. Therefore, all the rational points on C_4 are

$$(1 : 0 : \pm 1), \quad (0 : 1 : \pm 1).$$

□

Exercise 1.4 Let K be an algebraically closed field with $\mathrm{char}(K) \neq 2$. Let C be the projective closure of the affine curve with equation $y^2 = f(x)$, where $f(x) \in K[x]$. Show that if $\deg(f) = 3$ then C is smooth if and only if f has distinct roots.

[Hint: It's probably simplest to work with the affine equation, and then check the point at infinity separately.] What happens if $\deg(f) > 3$?

Proof. We set $F(x, y) = y^2 - f(x)$, and the affine curve is $F(x, y) = 0$. The partial derivatives are $F_x = -f'(x)$, $F_y = 2y$. Solution

$$F(x, y) = 0, \quad F_x(x, y) = 0, \quad F_y(x, y) = 0$$

We obtain$y = 0$, $f(x) = 0$, $f'(x) = 0$. Thus, the singularity occurs at the point $(x, 0)$ where $f(x) = 0$ and $f'(x) = 0$, meaning that $f(x)$ has multiple roots. Conversely, if $f(x)$ has three distinct roots, then for any root x, $f'(x) \neq 0$, so the affine curve is smooth.

Now we can check the infinity point. Let $x = \dfrac{X}{Z}$, $y = \dfrac{Y}{Z}$, note that deg $f = 3$, then homogenization yields

$$\left(\frac{Y}{Z}\right)^2 = f\left(\frac{X}{Z}\right) = \frac{1}{Z^3} g(X, Z),$$

where $g(X, Z)$ is a homogeneous cubic polynomial. Thus, the projection curve is:

$$F(X, Y, Z) = ZY^2 - g(X, Z) = 0.$$

The point at infinity corresponds to $Z = 0$. Substituting this into $0 = g(X, 0) = aX^3$, we solve for the point at infinity as $(0 : 1 : 0)$. Computing the partial derivatives,

$$F_X = -g_X(X, Z), \; F_Y = 2YZ, \; F_Z = Y^2 - g_Z(X, Z),$$

At the point $(0 : 1 : 0)$, $F_X = 0$, $F_Y = 0$, $F_Z = 1 \neq 0$, the gradient is non-zero, so the point is smooth.

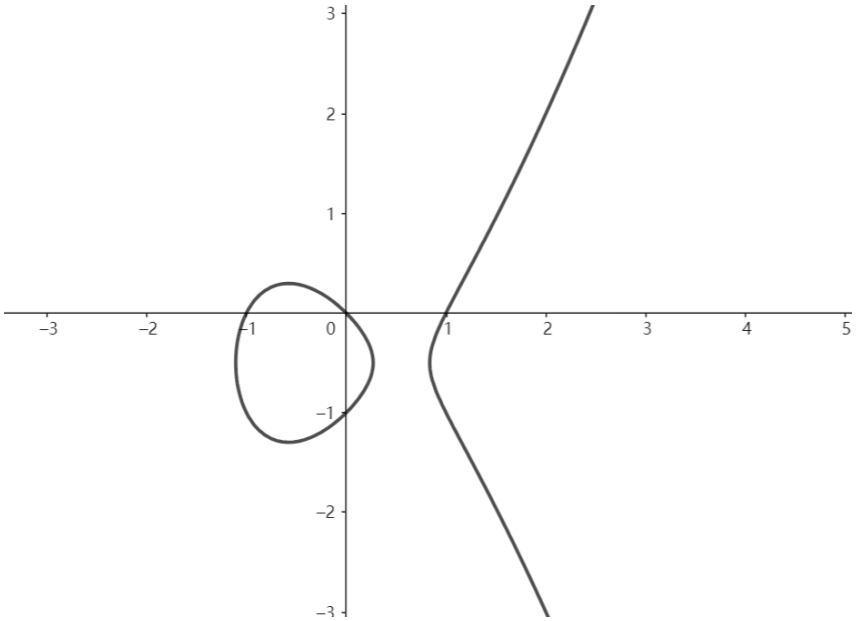
If $\deg(f) = d > 3$, the homogenized equation becomes

$$Y^2 Z^{d-2} = g(X, Z)$$

where $g(X, Z)$ is a homogeneous polynomial of degree d. In this case, the point at infinity may be a singular point. □

Exercise 1.5 Let E be the elliptic curve over $\mathbb{Q}$ defined by $y^2 + y = x^3 - x$. Draw a graph of its real points. Let $P = (0, 0)$. Compute nP for $n = 2, 3, 4, 5, 6, 7, 8$. What do you notice about the denominators? Can you prove anything in this direction?

Proof. We can draw the draph as follows. Note that the curve is symmetric about $y = -\dfrac{1}{2}$ and that the point $(0, 0)$ lies on the curve. Given a point $P = (0, 0)$, we differentiate the elliptic curve equation about x to obtain $y' = \dfrac{x^3 - x}{2y + 1}$. Therefore, the tangent line at P is $y = -x$, which intersects E at $(1, -1)$, and $2P = (1, 0)$.



For $Q = (x_0, y_0)$, calculate $P + Q$, the slope $k = \dfrac{y_0}{x_0}$, and $P + Q = (k^2 - x_0, x_0 k - k^3 - 1)$. Substituting nP into the equations, we calculate

$$2P = (1, 0),\ 3P = (-1, -1),\ 4P = (2, -3),\ 6P = (6, 14),$$

$$5P = \left(\frac{1}{4}, -\frac{5}{8}\right),\ 7P = \left(-\frac{5}{9}, \frac{8}{27}\right),\ 8P = \left(\frac{21}{25}, -\frac{69}{125}\right).$$

1. the denominator of $2P, 3P, 4P, 6P$ are all integers;
2. the denominator of $5P$ is both powers of 2;
3. the denominator of $7P$ is both powers of 3;
4. the denominator of $8P$ is both powers of 5.

This actually reflects the following fact: Taking the modulo p reduction of the elliptic curve, the order of $E(\mathbb{F}_p)$ annihilates P: modulo 2, the order is 5; modulo 3, the order is 7; and modulo 5, the order is 8. Since n is now divisible by the order of P modulo p, the point nP is at infinity modulo p, and thus the denominator is divisible by p.

We may can prove a general proposition: for a rational point P on an elliptic curve, the denominator of a point nP is divisible by a prime number p if and only if, under the modulo p reduction, the order of the point P is divisible by n. Specifically, if p is a good reduction, then the denominator of a point nP is divisible by p if and only if n is a multiple of the order of the point P modulo p. In this problem, $\Delta = 37$, so all prime numbers other than 37 can appear in the denominator of nP as powers. □

Exercise 1.6 Show that the congruent number elliptic curve $Dy^2 = x^3 - x$ has Weierstrass equation $y^2 = x^3 - D^2x$. Now use the group law to find two rational right-angled triangles of area 5.

Proof. Consider $Dy^2 = x^3 - x$, multiply both sides by D^3 and let $u = Dx$, $v = D^2y$, we have that

$$v^2 = u^3 - D^2u, \quad \text{i.e.} \quad y^2 = x^3 - D^2x.$$

Let $D = 5$, then the curve is $E_{25} : y^2 = x^3 - 25x$, the rational points on this curve correspond to rational right triangles with an area of 5. Noting that $(1, 1)$ is a solution for mod 5, analysis shows that $P = (-4, 6)$ is a solution to E_{25}. The calculated side lengths of the triangle are:

$$\left(\frac{3}{2}, \frac{20}{3}, \frac{41}{6}\right).$$

Using the group law, the multiple of $P = (-4, 6)$, $2P$ is calculated as we did before. The reuslt is $2P = \left(\frac{1681}{144}, -\frac{62279}{1728}\right)$. Similarly, the second triangle can be constructed as:

$$\left(\frac{1519}{492}, \frac{4920}{1519}, \frac{3344161}{747348}\right).$$

□

Exercise 1.7 Let E be an elliptic curve over $\mathbb{Q}$ with Weierstrass equation $y^2 = f(x)$.

(i) Put the curve $E_d : dy^2 = f(x)$ in Weierstrass form.

(ii) Show that if $j(E) \neq 0, 1728$ then every twist of E is isomorphic to E_d for some unique square-free integer d. [A twist of E is an elliptic curve E' defined over $\mathbb{Q}$ that is isomorphic to E over $\overline{\mathbb{Q}}$.]

Proof. (i) Let the Weierstrass equation for E be $y^2 = f(x) = x^3 + Ax + B$, and E_d be defined as $E_d : dy^2 = x^3 + Ax + B$. Let $u = dx$, $v = d^2y$. Substituting, we have

$$d\left(\frac{v}{d^2}\right)^2 = \left(\frac{u}{d}\right)^3 + A\left(\frac{u}{d}\right) + B \Rightarrow \frac{v^2}{d^3} = \frac{u^3}{d^3} + \frac{Au}{d} + B.$$

Multiplying both sides by d^3, we obtain the Weierstrass equation for E_d as

$$y^2 = x^3 + Ad^2x + Bd^3.$$

(ii) Let the Weierstrass equation and the j-invariant of E be

$$y^2 = x^3 + Ax + B, \quad j(E) = 1728 \cdot \frac{4A^3}{4A^3 + 27B^2},$$

(GTM106, PropX.5.4) If $j(E) \neq 0, 1728$, then the automorphism group of E is $\{\pm 1\}$, and all twists are quadratic twists. We know that quadratic twists are parameterized by $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, and can be uniquely represented by the square-free integer d as

$$E_d : y^2 = x^3 + Ad^2x + Bd^3.$$

□

Exercise 1.8 The elliptic curve E_λ over $\mathbb{C}$ with equation $y^2 = x\,(x-1)\,(x-\lambda)$ has j-invariant

$$j = \frac{2^8\left(\lambda^2-\lambda+1\right)^3}{\lambda^2(\lambda-1)^2}.$$

Find the complex numbers λ' for which $E_\lambda \cong E_{\lambda'}$.

Proof. Obviously two elliptic curves over $\mathbb{C}$ are isomorphic if and only if their j-invariants are equal. Therefore, we only need to find all λ' s.t. $j(\lambda) = j(\lambda')$.

$E : y^2 = x(x-1)(x-\lambda)$ is symmetric curve under the permutation of the set $\{0, 1, \lambda\}$, these permutations are given by S_3, which corresponds to the following transformations:

- $0 \mapsto 0, 1 \mapsto 1, \lambda \mapsto \lambda$: $x \mapsto x$;
- $0 \mapsto 0, 1 \mapsto \lambda, \lambda \mapsto 1$: $x \mapsto 1/x$;
- $0 \mapsto 1, 1 \mapsto 0, \lambda \mapsto \lambda$: $x \mapsto 1-x$;
- $0 \mapsto 1, 1 \mapsto \lambda, \lambda \mapsto 0$: $x \mapsto 1/(1-x)$;
- $0 \mapsto \lambda, 1 \mapsto 1, \lambda \mapsto 0$: $x \mapsto x/(x-1)$;
- $0 \mapsto \lambda, 1 \mapsto 0, \lambda \mapsto 1$: $x \mapsto (x-1)/x$.

Thus,

$$\lambda' = \lambda,\ \frac{1}{\lambda},\ 1-\lambda,\ \frac{1}{1-\lambda},\ \frac{\lambda}{\lambda-1},\ \frac{\lambda-1}{\lambda}.$$

□

Exercise 1.9 (i) Find a formula for doubling a point on the elliptic curve $E : y^2 = x^3 + ax + b$. [In your answer you should expand each numerator as a polynomial in x.]

(ii) Find a polynomial in x whose roots are the x-coordinates of the points T with $3T = O_E$. [Hint: Write $3T = O_E$ as $2T = -T$.]

(iii) Show that the polynomial found in (ii) has distinct roots.

Proof. (i) For a point $P = (x, y)$ on the elliptic curve $E : y^2 = x^3 + ax + b$, the tangent slope k is $k = \dfrac{3x^2+a}{2y}$, then x' and y' are:

$$x' = m^2 - 2x, \quad y' = m(x-x') - y.$$

By substituting and simplifying, we obtain the following explicit formula:

$$x' = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3+ax+b)}, \quad y' = \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8y(x^3+ax+b)}.$$

(ii) Suppose $T = (x, y)$, then $-T = (x, -y)$. From the dot doubling formula,

$$x = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3+ax+b)}$$

Simplifying, we obtain

$$3x^4 + 6ax^2 + 12bx - a^2 = 0.$$

Thus, the polynomial we are looking for is

$$P(x) = 3x^4 + 6ax^2 + 12bx - a^2$$

(iii) Taking the derivative of $P(x)$, $P'(x) = 12x^3 + 12ax + 12b = 12(x^3 + ax + b)$. A polynomial has multiple roots if and only if $P(x)$ and $P'(x)$ have a common factor. Suppose there exists a linear polynomial $Q(x) = cx + d$ s.t.

$$P(x) = (cx + d)(x^3 + ax + b) = cx^4 + dx^3 + acx^2 + (ad + bc)x + bd,$$

Comparing the coefficients with $P(x)$ we find $a = 0$ and $b = 0$. In this case, the curve $y^2 = x^3$ is singular, and the discriminant $\Delta = -16(4a^3 + 27b^2) = 0$, which is not an elliptic curve. Therefore, $P(x)$ and $P'(x)$ have no common factors, and $P(x)$ has distinct roots. □

Exercise 1.10 Let C be the plane cubic $aX^3 + bY^3 + cZ^3 = 0$ with $a, b, c \in \mathbb{Q}^*$. Show that the image of the morphism $C \to \mathbb{P}^3; (X : Y : Z) \mapsto \left(X^3 : Y^3 : Z^3 : XYZ\right)$ is an elliptic curve E, and put E in Weierstrass form. [You should try to give an answer that is symmetric under permuting a, b and c.] What is the degree of the morphism from C to E?

Proof. Considering $\phi : C \to \mathbb{P}^3$, $(X, Y, Z) \mapsto (X^3, Y^3, Z^3, XYZ) = (U, V, W, T)$. Calculate $\operatorname{im}\phi$ satisfies $aU + bV + cW = 0$, $T^3 = UVW$. We awnt to symmetrize the equation, we set $T = 1$, i.e. its affine transformation, substitute

$$x = aU,\ y = bV,\ -x - y = cW$$

to the equation, yield

$$xy(x + y) + abc = 0, \quad \text{i.e.} \quad y^2 = x^3 - 432(abc)^2.$$

For a inverse image (X, Y, Z), if $(X', Y', Z') \mapsto (X^3, Y^3, Z^3, XYZ)$, then for 3rd unit root ω_1, ω_2, ω_3, we only need $\omega_1\omega_2\omega_3 = 1$, $\deg\phi = 3$. □

Exercise 1.11 Let $E/\mathbb{F}_2$ be the elliptic curve $y^2 + y = x^3$. Show that the group $\operatorname{Aut}(E)$ of auto-morphisms of E is a non-abelian group of order 24. [An automorphism of E is an isomorphism from E to itself. In this example all the automorphisms are defined over $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ where $\omega^2 + \omega + 1 = 0$.]

Proof. (i) Each automorphism has the form

$$f : E \to E,\ (x, y) \mapsto (u^2x + r, u^3y + su^2x + t),\ u, r, s, t \in \mathbb{F}_4,$$

substitute that coordinate transformtion into the curve equation and simplify it, we need

$$u^3 = 1 \text{ i.e. } u \in \{1, \omega, \omega^2\}, \quad r = s^2, \quad t^2 + t = r^3.$$

- if $s = 0$, then $r = 0$, $t^2 + t = 1$, $t = 0$ or 1;
- if $s \neq 0$, then $s^3 = 1$, $r^3 = s^6 = 1$, $t^2 + t = 1$, $t = \omega$ or ω^2, $r = 1$ or ω or ω^2, $s^2 = r$;

Hence, $|\operatorname{Aut}(E)| = 3 \times 2 + 3 \times 3 \times 2 = 24$.

(ii) Non-Abelian: let

$$\phi_1 : (x, y) \mapsto (\omega^2 x + 1, \omega y + \omega x + \omega); \quad \phi_2 : (x, y) \mapsto (\omega^2 x, \omega^2 y).$$

Calculate that

$$\phi_1 \circ \phi_2(x, y) = (\omega x + 1, \omega y + \omega x + \omega) \neq (\omega x + \omega^2, \omega y + \omega^2 x + \omega^2) = \phi_2 \circ \phi_1(x, y),$$

$\phi_1 \circ \phi_2 \neq \phi_2 \circ \phi_1$, $\operatorname{Aut}(E)$ is non-Abelian group. □

Exercise 1.12 Let $C \subset \mathbb{P}^2$ be a smooth plane cubic defined over $\mathbb{Q}$. Show that if $C(K) \neq \varnothing$ for $K/\mathbb{Q}$ a quadratic field extension then $C(\mathbb{Q}) \neq \varnothing$. Can you generalise this result to field extensions of degree n for other integers n?

Proof. (i) If $\forall P \in C(K)$, $P \notin \mathbb{Q}$, let $\operatorname{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$. Then $\sigma(P) \in C(K)$. Considering the line ℓ passing through P and $\sigma(P)$, since ℓ determind by P and $\sigma(P)$, then $\sigma(\ell) = \ell$, i.e. ℓ defined over $\mathbb{Q}$. Hence, we note the third point of ℓ intersects with C as Q, both ℓ and C are defined over $\mathbb{Q}$, then $Q \in C(\mathbb{Q})$. $C(\mathbb{Q}) \neq 0$.

(ii) It's wrong. Consider

$$C/\mathbb{Q} : x^3 + 2y^3 + 4z^3 = 0.$$

We have $C(\mathbb{Q}) = \varnothing$, but on the cubic expansion $\mathbb{Q}(\sqrt[3]{2})$ there is a rational point $P = (0 : \sqrt[3]{2} : -1)$. □

2 Example Sheet 2

Exercise 2.1 Find all points defined over the field $\mathbb{F}_{13}$ of 13 elements on the elliptic curve

$$y^2 = x^3 + x + 5,$$

and show that they form a cyclic group. Find an example of an elliptic curve over $\mathbb{F}_{13}$ for which this group is not cyclic. Are there any examples where the group requires more than two generators?

Proof. (i) Notice the quadratic residue of $\mathbb{F}_{13}$ is $\{1, 3, 4, 9, 10, 12\}$.

- $x = 0$: $y^2 = 5$, non-quadratic residue, no points.
- $x = 1$: $y^2 = 7$, non-quadratic residue, no points.
- $x = 2$: $y^2 = 15$, non-quadratic residue, no points.
- . . . . . .

We can find all finite points are $(3, 3)$, $(3, 10)$, $(7, 2)$, $(7, 11)$, $(10, 1)$, $(10, 12)$, $(12, 4)$, and $(12, 9)$, for a total of 8 points. Including the point O at infinity, the total number of points is 9.

Now prove that these points form a cyclic group. Compute the multiples of the point $P = (3, 3)$: $2P = (10, 12)$, $3P = (12, 4)$, $4P = (7, 11)$, $5P = (7, 2)$, $6P = (12, 9)$, $7P = (10, 1)$, $8P = (3, 10)$, $9P = O$. Thus, the point P has order 9 and generates the $\mathbb{F}_{13}$-rational point group, so the group is cyclic.

(ii) Consider the elliptic curve $E' : y^2 = x^3 + 1$ over $\mathbb{F}_{13}$. We calculate $(0, 1)$, $(0, 12)$, $(2, 3)$, $(2, 10)$, $(4, 0)$, $(5, 3)$, $(5, 10)$, $(6, 3)$, $(6, 10)$, $(10, 0)$, $(12, 0)$, and $O_{E'}$, for total 12 points. The computation of $E'(\mathbb{F}_{13})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, not cyclic.

(iii) We now prove that there are integers $m \geq 1$ and $n \geq 1$ with $\gcd(m, q) = 1$, s.t. $E(\mathbb{F}_q) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$. At first, by GTM106, CorIII.6.4, we know that when char $F = p$,

- if $\gcd(p, m) = 1$, then $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$;
- if $m = p^e$, then $\forall e \in \mathbb{Z}_{\geq 1}$, $E[p^e] = \{O_E\}$ or $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$.

Then the rank of $E[m] \leq 2$ for all $m \in \mathbb{F}_q$. If rank $E(\mathbb{F}_q) \geq 3$, by the structure of finite Abel group, we set

$$E(\mathbb{F}_q) \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z},\ n_3 \neq 0,\ n_i | n_{i+1}.$$

Thus, for $d | n_3$, $E[d] = (\mathbb{Z}/d\mathbb{Z})^{s_d}$, $s \leq 2$. In the structural decomposition, each $\mathbb{Z}/n_r\mathbb{Z}$ corresponds to a $\mathbb{Z}/d\mathbb{Z}$; but $n_i | n_{i+1}$, $d \nmid n_1$ for all factors d of n_3, $n_1 = 0$. Recursively, we can get $E(\mathbb{F}_q)$ to have at most two components, $E(\mathbb{F}_q) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$, thus $E(\mathbb{F}_q)$ has at most 2 generators. □

Exercise 2.2 Let A be an abelian group. Let $q : A \to \mathbb{Z}$ be a map satisfying

$$q(x + y) + q(x - y) = 2q(x) + 2q(y)$$

for all $x, y \in A$. Show that q is a quadratic form.

Proof. Taking $y = 0$, we have $q(x) + q(x) = 2q(x) + 2q(0)$, $q(0) = 0$. Taking $x = 0$, $q(y) + q(-y) =$

$2q(0)+2q(y)=2q(y)$, $q(-y)=q(y)$. Taking $y=x$, $q(2x)+q(0)=2q(x)+2q(x)=4q(x)$. By induction, we obtain that for any $n\in\mathbb{Z}$, $q(nx)=n^2q(x)$.

We define

$$B:A\times A\to\mathbb{Z},\quad B(x,y)=\frac{q(x+y)-q(x)-q(y)}{2}\in\mathbb{Z},$$

Verify

1. Symmetry: $B(y,x)=\dfrac{q(x+y)-q(x)-q(y)}{2}=B(x,y)$;
2. Bilinearity: $B(x+y,z)=B(x,z)+B(y,z)$,

Thus, B is a symmetric bilinear form. Note that $q(x)=B(x,x)$, so q is a quadratic form. □

Exercise 2.3 Find a translation-invariant differential ω on the multiplicative group $\mathbb{G}_m$. Show that if $[n]:\mathbb{G}_m\to\mathbb{G}_m$ is the endomorphism $x\mapsto x^n$, then $[n]^*\omega=n\omega$.

Proof. $\omega=\dfrac{\mathrm{d}x}{x}$. For the multiplication group $\mathbb{G}_m$, we consider the translation $T:x\mapsto ax$, then $T^*\omega=\dfrac{\mathrm{d}(ax)}{ax}=\dfrac{\mathrm{d}x}{x}=\omega$. Thus, ω is translation-invariant. Now consider $[n]:x\mapsto x^n$, calculate

$$[n]^*\omega=[n]^*\frac{\mathrm{d}x}{x}=\frac{\mathrm{d}x^n}{x^n}=\frac{nx^{n-1}\,\mathrm{d}x}{x^{n-1}\cdot x}=n\omega.$$

□

Exercise 2.4 Let E_1 and E_2 be elliptic curves over $\mathbb{F}_q$, and let $\psi:E_1\to E_2$ be an isogeny defined over $\mathbb{F}_q$. Let ϕ_i be the q-power Frobenius on E_i for $i=1,2$. Show that $\psi\circ\phi_1=\phi_2\circ\psi$ and deduce that $\#E_1(\mathbb{F}_q)=\#E_2(\mathbb{F}_q)$.

Proof. (i) For $i=1,2$, define the q-power Frobenius $\phi_i:E_i\to E_i$, $P=(x,y)\mapsto P^q=(x^q,y^q)$. Therefore, $\forall P\in E_1$,

$$\psi(\phi_1(P))=\psi(P^q)=(\psi(P))^q=\phi_2(\psi(P)),\quad \psi\circ\phi_1=\phi_2\circ\psi.$$

(ii) Rational points $|E_i(\mathbb{F}_q)|=\deg(1-\phi_i)$. Obviously

$$\psi\circ\phi_1=\phi_2\circ\psi\Rightarrow\psi\circ(1-\phi_1)=(1-\phi_2)\circ\psi,$$

then $\deg\psi\cdot\deg(1-\phi_1)=\deg(1-\phi_2)\cdot\deg\psi$, i.e. $\deg(1-\phi_1)=\deg(1-\phi_2)$, $|E_1(\mathbb{F}_q)|=|E_2(\mathbb{F}_q)|$. □

Exercise 2.5 Let $E/\mathbb{F}_{13}$ be the elliptic curve in Exercise 2.1. Without listing its elements, find the order of $E(\mathbb{F}_{13^2})$ and determine whether this group is cyclic.

Proof. We can calculate the trace

$$\operatorname{tr}\mathrm{Frob}=a=q+1-|E(\mathbb{F}_{13})|=13+1-9=5.$$

Let α, β be two roots of the equation $X^2 - 5X + 13 = 0$. We know that

$$|E(\mathbb{F}_{13^2})| = 13^2 + 1 - \alpha^2 - \beta^2 = 170 - 5(\alpha + \beta) + 26 = 170 - 25 + 26 = 171.$$

We have proved there are integers $m \geq 1$ and $n \geq 1$ with $\gcd(m, q) = 1$, s.t. $E(\mathbb{F}_q) = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$ in Exercise 2.1, $171 = 3^2 \cdot 19$, then

$$E(\mathbb{F}_{13^2}) \cong \mathbb{Z}/171\mathbb{Z}, \text{ or } E(\mathbb{F}_{13^2}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/57\mathbb{Z}.$$

Note that $E(\mathbb{F}_{13})$ is subgroup of $E(\mathbb{F}_{13^2})$, $|E(\mathbb{F}_{13})| = 9$ and $E(\mathbb{F}_{13})$ is cyclic, then the g.c.d of the order of all points must be divisible by 9, which implies $E(\mathbb{F}_{13^2}) \cong \mathbb{Z}/171\mathbb{Z}$, i.e. cyclic. □

Exercise 2.6 Show that if $\phi \in \mathrm{End}(E)$ then there exists $\mathrm{tr}(\phi) \in \mathbb{Z}$ s.t.

$$\deg([n] + \phi) = n^2 + n\,\mathrm{tr}(\phi) + \deg(\phi)$$

for all $n \in \mathbb{Z}$. Establish the following properties:

(i) $\mathrm{tr}(\phi + \psi) = \mathrm{tr}(\phi) + \mathrm{tr}(\psi)$,

(ii) $\mathrm{tr}(\phi^2) = \mathrm{tr}(\phi)^2 - 2\deg(\phi)$,

(iii) $\phi^2 - [\mathrm{tr}(\phi)]\,\phi + [\deg(\phi)] = 0$.

Proof. We know that the degree mapping $\deg : \mathrm{End}(E) \to \mathbb{Z}$, $f \mapsto \deg f$ is positive definite quadratic form, then exists a bilinear from $q(-,-)$, s.t.

$$\forall \phi, \psi \in \mathrm{End}(E),\ \deg(\phi + \psi) = \deg\phi + \deg\psi + q(\phi, \psi).$$

We can define the trace $\mathrm{tr}\,\phi := q(1, \phi)$, where $1 = \mathrm{id} \in \mathrm{End}(E)$. Thus,

$$\deg([n] + \phi) = \deg[n] + \deg\phi + q([n], \phi) = n^2 + \deg\phi + n \cdot \mathrm{tr}\,\phi.$$

We now establish these properties:

(i) $\mathrm{tr}(\phi + \psi) = q(1, \phi + \psi) = q(1, \phi) + q(1, \psi) = \deg\phi + \deg\psi$.

(ii) We can take traces in the results in (iii):

$$\mathrm{tr}(\phi^2) = \mathrm{tr}([\mathrm{tr}(\phi)]\phi - [\deg\phi]) = \mathrm{tr}(\phi) \cdot \mathrm{tr}(\phi) - \mathrm{tr}([\deg\phi]).$$

obviously $\mathrm{tr}([m]) = 2m$, in particular, $\mathrm{tr}([\deg\phi]) = 2\deg\phi$. Therefore,

$$\mathrm{tr}(\phi^2) = (\mathrm{tr}\,\phi)^2 - 2\deg\phi.$$

(iii) Let $\hat{\phi}$ be the dual isogeny of ϕ, then $\phi\hat{\phi} = [\deg\phi]$, note that $\phi + \hat{\phi}$ is self-dual, hence there exists an integer m s.t. $\phi + \hat{\phi} = [m]$. Note that

$$\deg(1 + \phi) = \deg 1 + \deg\phi + q(1, \phi) = 1 + \deg\phi + \mathrm{tr}(\phi),$$

using the dual and taking degrees, we have that

$$(1+\phi)(1+\hat{\phi}) = 1+\phi+\hat{\phi}+\phi\hat{\phi} = 1+[m]+[\deg\phi], \quad \deg(1+\phi)\cdot\deg(1+\hat{\phi}) = \deg(1+[m]+[\deg\phi]).$$

But $\deg(1+\hat{\phi}) = \deg(1+\phi)$ since $\deg\phi = \deg\hat{\phi}$, thus,

$$(1+\deg\phi+\mathrm{tr}(\phi))^2 = (1+m+\deg\phi)^2 \Rightarrow \mathrm{tr}(\phi) = m.$$

Therefore, $\phi+\hat{\phi} = [\mathrm{tr}(\phi)]$, $\hat{\phi} = [\mathrm{tr}(\phi)]-\phi$. Now multiply both sides by ϕ:

$$[\deg\phi] = \phi\hat{\phi} = \phi([\mathrm{tr}(\phi)]-\phi) = [\mathrm{tr}(\phi)]\phi-\phi^2 \Rightarrow \phi^2-[\mathrm{tr}(\phi)]\phi+[\deg\phi] = 0.$$

□

Exercise 2.7 **Let E be the elliptic curve $y^2 = x^3+d$. We put**

$$\xi = \frac{x^3+4d}{x^2},\ \eta = \frac{y\left(x^3-8d\right)}{x^3}.$$

(i) Show that $T = \left(0,\sqrt{d}\right)$ is a point of order 3, and that if $P = (x,y)$ then

$$\xi = x(P)+x\left(P+T\right)+x\left(P+2T\right).$$

(ii) Verify that $\eta^2 = \xi^3+D$ for some constant D (which you should find).

(iii) Let E' be the elliptic curve $y^2 = x^3+D$, and $\phi : E \to E'$ the isogeny given by $(x,y)\mapsto(\xi,\eta)$. Compute $\phi^*\left(\mathrm{d}x/y\right)$.

Proof. (i) Calculatic 2T : $k = \dfrac{3x^2}{2y} = 0$, tangent line $\ell : y = \sqrt{d}$, $-2T = T$ i.e. $3T = 0$, T is a point with order 3. Let $P = (x,y)$,

- calculate $P+T$: $k_1 = \dfrac{y-\sqrt{d}}{x}$, $x(P)+x(T)+x(P+T) = k_1^2$;
- calculate $P+2T = P-T$: $k_2 = \dfrac{y+\sqrt{d}}{x}$, $x(P)+x(2T)+x(P+2T) = k_2^2$.

Therefore,

$$\begin{aligned} x(P)+x(P+T)+x(P+2T) &= k_1^2+k_2^2-x(P)-2x(T) \\ &= \frac{\left(y-\sqrt{d}\right)^2}{x^2}+\frac{\left(y+\sqrt{d}\right)^2}{x^2}-x \\ &= \frac{2y^2+2d-x^3}{x^2} = \frac{2(x^3+d)+2d-x^3}{x^2} = \frac{x^3+4d}{x^2} = \xi. \end{aligned}$$

$$\begin{aligned} \text{(ii)}\ D = \eta^2-\xi^3 &= \frac{y^2(x^3-8d)^2}{x^6}-\frac{(x^3+4d)^3}{x^6} \\ &= \frac{(x^3+d)(x^3-8d)^2-(x^3+4d)^3}{x^6} = \frac{-27dx^6}{x^6} = -27d. \end{aligned}$$

(iii) $\mathrm{d}\xi = \mathrm{d}\left(\dfrac{x^3+4d}{x^2}\right) = \dfrac{x^3-8d}{x^3}\mathrm{d}x$. Then $\phi^*\dfrac{\mathrm{d}x}{y} = \dfrac{\mathrm{d}\xi}{\eta} = \dfrac{\frac{x^3-8d}{x^3}\mathrm{d}x}{\frac{y(x^3-8d)}{x^3}} = \dfrac{\mathrm{d}x}{y}$. □

Exercise 2.8 Let $E/\mathbb{F}_q$ be an elliptic curve and $K = \mathbb{F}_q(E)$. Show that ζ_K is meromorphic on $\mathbb{C}$ and satisfies the functional equation $\zeta_K(1-s) = \zeta_K(s)$.

Proof.

$$\zeta_K(s) = \prod_{\mathfrak{p}\in\Sigma_K}\left(1-\mathrm{N}(\mathfrak{p})^{-s}\right)^{-1} = \prod_{\mathfrak{p}\in\Sigma_K}\left(1-q^{-s\cdot\deg\mathfrak{p}}\right)^{-1}.$$

Thus, $\zeta_K(s)$ is defined as the value of the elliptic curve zeta function at $T = q^{-s}$, that is $\zeta_K(s) = Z_K(q^{-s})$, where $Z_K(T) = \dfrac{1-aT+qT^2}{(1-T)(1-qT)}$, $a = q+1-|E(\mathbb{F}_q)|$.

(i) Note that $Z_K(X)$ is rational function of X, $X = q^{-s}$ is integral function, then the composition $\zeta_K(s) = Z_K(q^{-s})$ is meromorphic on $\mathbb{C}$.

(ii) Note that for elliptic curves, we have

$$Z_K\left(\frac{1}{qT}\right) = Z_K(T),$$

Let $T = q^{-s}$, and we can compute $\zeta_K(1-s)$:

$$\zeta_K(1-s) = Z_K(q^{-(1-s)}) = Z_K(q^{s-1}).$$

We can also compute $\zeta_K(s)$:

$$\zeta_K(s) = Z_K(q^{-s}) = Z_K(T) = Z_K\left(\frac{1}{qT}\right) = Z_K(q^{s-1}).$$

Thus, $\zeta_K(1-s) = \zeta_K(s)$, and the functional equation holds. □

Exercise 2.9 Let $E/\mathbb{F}_p$ be an elliptic curve with p an odd prime. Show that there exists an elliptic curve $E'/\mathbb{F}_p$ with

$$\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2(p+1).$$

Show further that the groups $E(\mathbb{F}_p)\times E'(\mathbb{F}_p)$ and $E\left(\mathbb{F}_{p^2}\right)$ have the same order, but need not be isomorphic.

Proof. Let the elliptic curve $E: y^2 = f(x)$, where $f(x)$ is a cubic polynomial. Let $d \in \mathbb{F}_p$ be a non-square element, and define $E': dy^2 = f(x)$ as a quadratic twist of E. For any $x \in \mathbb{F}_p$, the Legendre symbol $\left(\dfrac{f(x)}{p}\right)$ of $f(x)$ takes the value $0, 1, -1$.

1. If $f(x) = 0$, then both E and E' have a point $(x, 0)$.
2. If $\left(\dfrac{f(x)}{p}\right) = 1$, then E has two points and E' has no points.
3. If $\left(\dfrac{f(x)}{p}\right) = -1$, then E has no points and E' has two points.

In addition, every curve has a point O at infinity. therefore,

$$|E(\mathbb{F}_p)| = 1 + \sum_{x\in\mathbb{F}_p}\left(1+\left(\frac{f(x)}{p}\right)\right) = p+1+\sum_{x\in\mathbb{F}_p}\left(\frac{f(x)}{p}\right),$$
$$|E'(\mathbb{F}_p)| = 1 + \sum_{x\in\mathbb{F}_p}\left(1+\left(\frac{df(x)}{p}\right)\right) = p+1-\sum_{x\in\mathbb{F}_p}\left(\frac{f(x)}{p}\right).$$

Thus, $|E(\mathbb{F}_p)| + |E'(\mathbb{F}_p)| = 2(p+1)$.

(ii) Let $|E(\mathbb{F}_p)| = p+1-a$, then $|E'(\mathbb{F}_p)| = p+1+a$,

$$|E(\mathbb{F}_p)\times E'(\mathbb{F}_p)| = (p+1-a)(p+1+a) = (p+1)^2 - a^2.$$

On the other hand, note that on $\mathbb{F}_{p^2}$, $\mathrm{Frob}_{p^2} = \mathrm{Frob}_p^2$, and its eigenvalue is α^2, β^2, where α, β is a root of the characteristic polynomial $T^2 - aT + p$ of Frob_p on E. Therefore, by Vieta's theorem and Weil's conjecture,

$$|E(\mathbb{F}_{p^2})| = 1 - (\alpha^2+\beta^2) + \alpha^2\beta^2 = 1 - (a^2-2p) + p^2 = (p+1)^2 - a^2.$$

Thus, $|E(\mathbb{F}_p)\times E'(\mathbb{F}_p)| = |E(\mathbb{F}_{p^2})|$.

(iii) Taking $p = 13$, the elliptic curves in Exercises 2.1 and 2.5 satisfy the above result. □

Exercise 2.10 **Let E be an elliptic curve over $\mathbb{F}_p$ (p a prime) with $\#E(\mathbb{F}_p) = p+1-a$, and let $\phi : E \to E$ be the p-power Frobenius, i.e. $\phi : (x,y) \mapsto (x^p, y^p)$. Let $\psi = [a] - \phi$. (i) Show that $\phi\circ\psi = \psi\circ\phi = [p]$. (ii) Show that if ψ is separable then $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$ for all $r \geq 1$. (iii) Show that if $p \geq 5$ and $E[p] = 0$ then $\#E(\mathbb{F}_p) = p+1$.**

Proof. (i) The Frobenius endomorphism ϕ satisfies the characteristic equation $\phi^2 - a\phi + [p] = 0$, where $a = p+1-|E(\mathbb{F}_p)|$. Then

$$\phi\circ\psi = \phi([a]-\phi) = [a]\phi - \phi^2 = [a]\phi - (a\phi - [p]) = [p].$$

Similarly,

$$\psi\circ\phi = ([a]-\phi)\phi = [a]\phi - \phi^2 = [a]\phi - (a\phi - [p]) = [p].$$

Thus, $\phi\circ\psi = \psi\circ\phi = [p]$.

(ii) Note that $\psi = [a] - \phi$ is essentially the dual Frobenius $\hat{\phi}$, $\deg\psi = p$. If ψ is separable, then its kernel is of size p. From $\phi\circ\psi = [p]$, we know that $\ker\psi \subseteq E[p]$, so $E[p]$ contains a subgroup of order p, so $E[p] \cong \mathbb{Z}/p\mathbb{Z}$. Furthermore, when ψ is separable, the formal group has height 1, which means that for any $r \geq 1$, we have $E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}$.

(iii) If $E[p] = 0$, then the characteristic polynomial of the Frobenius ϕ is $T^2 - aT + p$, and $a \equiv 0 \pmod p$, that is, $a = kp$ for some integer k. From the Hasse bound $|a| \leq 2\sqrt{p}$, substituting $a = kp$ yields

$$|k| \leq \frac{2}{\sqrt{p}} < 1, \quad (p \geq 5).$$

Thus, $k = 0$, that is, $a = 0$, $|E(\mathbb{F}_p)| = p + 1 - a = p + 1$. □

Exercise 2.11 Let $F \in R[[X, Y]]$ be a formal group over a ring R. Show that there is a unique power series $\iota(T)$ in $R[\![T]\!]$ with $\iota(0) = 0$ and $F(T, \iota(T)) = 0$. Find $\iota(T)$ for the multiplicative formal group $\widehat{\mathbb{G}}_m$.

Proof. (i) Assume the formal group law

$$F(X, Y) = X + Y + \sum_{i,j\geq 1} a_{ij} X^i Y^j \in R[[X, Y]]$$

Satisfies

$$F(X, 0) = X,\ F(0, Y) = Y,\ F(X, Y) \equiv X + Y \pmod{\deg 2},$$

Expand $F(T, \iota(T)) = 0$, and substitute the comparison coefficients to obtain

$$\iota(T) = -T - \sum_{i,j\geq 1} a_{ij} T^i (\iota(T))^j,$$

Assume $\iota(T) = \sum_{i=1}^{\infty} c_i T^i$, substitute the above equation and compare the coefficients to obtain $c_1 = -1$, c_n is determined recursively by the coefficients of the lower-order terms. Furthermore, expanding $F(X, \iota(0))$ and comparing the coefficients with $F(X, 0) = X$ yields

$$F(X, 0) \equiv X \pmod{\deg 3} \Rightarrow F(X, Y) \equiv X + Y + g \cdot XY \pmod{\deg 3}.$$

Thus, there exists a unique power series $\iota(T)$ such that $\iota(0) = 0$ and $F(T, \iota(T)) = 0$.

(ii) The multiplicative formal group $\widehat{\mathbb{G}}_m$ is defined as $F(X, Y) = X + Y + XY$, requiring $\iota(T)$ to satisfy:

$$F(T, \iota(T)) = T + \iota(T) + T \cdot \iota(T) = 0 \Rightarrow \iota(T)(1 + T) = -T,$$

i.e. $\iota(T) = -\dfrac{T}{1+T}$. □

Exercise 2.12 Let R be an integral domain of characteristic zero, with field of fractions K. Suppose that $f(T) = \sum_{n=1}^{\infty} (a_n/n!)\, T^n$ and $g(T) = \sum_{n=1}^{\infty} (b_n/n!)\, T^n$ are power series in $K[\![T]\!]$ satisfying $f(g(T)) = g(f(T)) = T$. Show that if $a_1 \in R^\times$ and $a_n \in R$ for all n, then $b_n \in R$ for all n. [Hint: You should repeatedly differentiate $f(g(T)) = T$ and then put $T = 0$.]

Proof. From $f(g(T)) = T$, taking the derivative of both sides with respect to T, we obtain $f'(g(T)) \cdot g'(T) = 1$. Substituting into $T = 0$,

$$f'(0) \cdot g'(0) = a_1 b_1 = 1 \Rightarrow b_1 = \frac{1}{a_1}.$$

We know that $a_1 \in R^\times$, so $b_1 \in R$.

Next, we prove $b_n \in R$ by induction for n. Assume that for all $j < n$, we have $b_j \in R$. Consider

the nth derivative of $f(g(T)) = T$ at $T = 0$. From Faà di Bruno's formula:

$$\frac{\mathrm{d}^n}{\mathrm{d}T^n} f(g(T)) = \sum_{k=1}^{n} f^{(k)}(g(T)) \cdot B_{n,k}(g'(T), g''(T), \ldots, g^{(n-k+1)}(T)),$$

where $B_{n,k}$ is a Bell polynomial. So at $T = 0$, we have

$$g(0) = 0 \Rightarrow f^{(k)}(0) = a_k, \quad g^{(j)}(0) = b_j.$$

Thus:

$$\sum_{k=1}^{n} a_k \cdot B_{n,k}(b_1, b_2, \ldots, b_{n-k+1}) = 0.$$

Separating the $k = 1$ term, noting that $B_{n,1}(b_1, \ldots, b_n) = b_n$ and $B_{n,k}$ is a polynomial in $b_1, \ldots, b_{n-k+1}$, the above summation becomes:

$$a_1 b_n + \sum_{k=2}^{n} a_k \cdot B_{n,k}(b_1, \ldots, b_{n-k+1}) = 0, \text{ i.e. } b_n = -\frac{1}{a_1} \sum_{k=2}^{n} a_k \cdot B_{n,k}(b_1, \ldots, b_{n-k+1}).$$

By the induction hypothesis, $b_1, \ldots, b_{n-1} \in R$, $a_1 \in R^\times$, so $b_n \in R$. We complete the proof by mathematical induction. □

3 Example Sheet 3

Exercise 3.1 Let E be the elliptic curve over $\mathbb{Q}$ given by

$$y^2 + xy = x^3 - 2x + 1$$

for which the discriminant Δ is equal to -61. For each prime p, let $\tilde{E}_p$ be the reduction of E modulo p.

(i) Compute the cardinality of $\tilde{E}_p(\mathbb{F}_p)$ for $p = 2, 3, 5, 7$.

(ii) Prove that the torsion subgroup of $E(\mathbb{Q})$ is trivial.

(iii) Prove that the torsion subgroup of $E(\mathbb{Q}_2)$ has order dividing 8.

(iv) If $P = (1, 0)$ in $E(\mathbb{Q})$, prove that $7P$ and $9P$ do not have integral coordinates.

Proof. (i) For $p = 2, 3, 5, 7$, we can calculate as follows:

- $p = 2$, $\tilde{E}_2/\mathbb{F}_2 : y^2 + xy = x^3 + 1$, $\tilde{E}_2(\mathbb{F}_2) = \{(0, 1), (1, 0), (1, 1), O\}$, 4 points;
- $p = 3$, $\tilde{E}_3/\mathbb{F}_3 : y^2 + xy = x^3 + x + 1$, $\tilde{E}_3(\mathbb{F}_3) = \{(0, 1), (0, 2), (1, 0), (1, 2), (2, 2), O\}$, 6 points;
- $p = 5$, $\tilde{E}_5(\mathbb{F}_5) = \{(0, 1), (0, 4), (1, 0), (1, 4), (2, 0), (2, 3), (4, 2), (4, 4), O\}$, 9 points;
- $p = 7$, $\tilde{E}_7(\mathbb{F}_7) = \{(0, 1), (0, 6), (1, 0), (1, 6), (6, 2), (6, 6), O\}$, 7 points.

(ii) We konw that $E(\mathbb{Q})_{\text{tor}}$ injects into all of these groups in (i), note that $\gcd(4, 6, 9, 7) = 1$. Hence $|E(\mathbb{Q})_{\text{tor}}| = 1$.

(iii) Note that $2 \nmid \Delta_E = -61$, then E has good reduction on $p = 2$. Thus, $E(\mathbb{Q}_2) \hookrightarrow \tilde{E}_2(\mathbb{F}_2)$. We konw $|\tilde{E}_2(\mathbb{F}_2)| = 4$ in (i), then $E(\mathbb{Q}_2)_{\text{tor}}$ has order dividing 4, furthermore, 8.

(iv) Note that points with integer coordinates will not be at infinity after reduction modulo $\forall p$. For $7P$: Reduced modulo $p = 7$, $\tilde{E}_7(\mathbb{F}_7)$ is a cyclic group. The point P modulo 7 is $(1, 0) \in \tilde{E}_7(\mathbb{F}_7)$, and the order of P in $\tilde{E}_7(\mathbb{F}_7)$ is 7. Therefore, $7P \equiv O \pmod 7$, so $7P$ has no integer coordinates. For $9P$: Reduced modulo $p = 5$, the order of $\tilde{E}_5(\mathbb{F}_5)$ is 9. The point P modulo 5 is $(1, 0) \in \tilde{E}_5(\mathbb{F}_5)$, and the order of P in $\tilde{E}_5(\mathbb{F}_5)$ is integer divisible by 9. Therefore, $9P \equiv O \pmod 5$, so $9P$ has no integer coordinates. □

Exercise 3.2 Find the torsion groups over $\mathbb{Q}$ for the elliptic curves (i) $y^2 + xy + y = x^3$, (ii) $y^2 - xy - 4y = x^3 - 4x^2$, (iii) $y^2 = x^3 + 5x^2 + 4x$.

Proof. We'll use Lutz–Nagell theorem: if $(x, y) \in E(\mathbb{Q})_{\text{tor}}$, $y^2 = x^3 + ax^2 + bx + c$, then $(x, y) \in \mathbb{Z}^2$, $y = 0$ or $y^2 | \Delta$.

(i) The substitution $y \mapsto \dfrac{1}{2}(y - x - 1)$ gives us an Weierstrass of the form

$$E' : y^2 = 4x^3 + x^2 + 2x + 1, \quad \Delta = -26.$$

By Lutz–Nagell theorem, if $(x, y) \in E(\mathbb{Q})_{\text{tor}}$, then

- $y = 0$: let $P = (0, 0)$, then $2P = (0, -1), 3P = O$;
- $y^2 | \Delta$: impossible.

Thus, the torsion group is $\mathbb{Z}/3\mathbb{Z}$.

(ii) The substitution $y \mapsto \frac{1}{2}(y + x + 4)$ gives us a Weierstrass form of the form

$$E' : y^2 = 4x^3 - 15x^2 + 8x + 16, \quad \Delta = -1664 = -2^7 \cdot 13.$$

By Lutz–Nagell theorem, if $(x, y) \in E(\mathbb{Q})_{\text{tor}}$, then

- $y = 0$: let $P = (0, 0)$, then $2P = (4, 8)$, $3P = (2, 2)$, $4P = (2, 4)$, $5P = (4, 0)$, $6P = (-1, -1)$, $7P = O$;
- $y^2 \mid \Delta$: no other points.

Thus, the torsion group is $\mathbb{Z}/7\mathbb{Z}$.

(iii) $E : y^2 = x^3 + 5x^2 + 4x$, $\Delta = 2304 = 2^8 \cdot 3^2$. By Lutz–Nagell theorem, if $(x, y) \in E(\mathbb{Q})_{\text{tor}}$, then

- $y = 0$: points $(0, 0)$, $(-1, 0)$, $(-4, 0)$;
- $y^2 \mid \Delta$: points $(-2, \pm 2)$, $(2, \pm 6)$.

We can calculate $(-1, 0)$ has order 2, $(2, 6)$ has order 4. Thus, the torsion group is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. □

Exercise 3.3 **Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + \lambda x$ where λ is an integer. For p a prime not dividing 2λ we write $\#\tilde{E}(\mathbb{F}_p) = p + 1 - a_p$. Show that if $p = 4k + 1$ then**

$$a_p \equiv \lambda^k \binom{2k}{k} \pmod{p}.$$

Deduce that $a_p \equiv 0 \pmod{p}$ if and only if $p \equiv 3 \pmod{4}$.

Proof. (i) Consider the elliptic curve $E : y^2 = x^3 + \lambda x$ over the finite field $\mathbb{F}_p$, then

$$|E(\mathbb{F}_p)| = 1 + \sum_{x=0}^{p-1} \left(1 + \left(\frac{x^3 + \lambda x}{p}\right)\right) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + \lambda x}{p}\right),$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. From $|E(\mathbb{F}_p)| = p + 1 - a_p$, we can deduce

$$a_p = -\sum_{x=0}^{p-1} \left(\frac{x^3 + \lambda x}{p}\right).$$

For $x = 0$, we have $\left(\frac{0}{p}\right) = 0$. For $x \neq 0$, we have:

$$\left(\frac{x^3 + \lambda x}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{x^2 + \lambda}{p}\right).$$

By Euler's criterion, the Legendre symbol satisfies $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ for $a \not\equiv 0 \pmod{p}$. Since

$p = 4k + 1$, we have

$$\left(\frac{x}{p}\right) \equiv x^{2k} \,(\mathrm{mod}\, p)\,, \left(\frac{x^2+\lambda}{p}\right) \equiv (x^2+\lambda)^{2k} \,(\mathrm{mod}\, p)\,, \quad a_p \equiv -\sum_{x=1}^{p-1} x^{2k}(x^2+\lambda)^{2k} \,(\mathrm{mod}\, p)\,.$$

By the binomial theorem, we can expand $(x^2+\lambda)^{2k}$ to the form

$$(x^2+\lambda)^{2k} = \sum_{j=0}^{2k} \binom{2k}{j} \lambda^j x^{4k-2j},$$

Thus:

$$a_p \equiv -\sum_{x=1}^{p-1} x^{2k} \sum_{j=0}^{2k} \binom{2k}{j} \lambda^j x^{4k-2j} = -\sum_{j=0}^{2k} \binom{2k}{j} \lambda^j \sum_{x=1}^{p-1} x^{6k-2j} \,(\mathrm{mod}\, p)\,.$$

Consider $m = 6k - 2j$. By Fermat's Little Theorem, $\sum_{x=1}^{p-1} x^m \equiv 0 \,(\mathrm{mod}\, p)$ when $p - 1 = 4k \nmid m$. Therefore, the nonzero terms satisfy $4k \mid m$, i.e., $2k \mid (3k - j)$. Since $0 \le j \le 2k$, then $j = k$. At this time, $x^{4k} = x^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$ for $x = 1, \cdots, p-1$, so

$$a_p \equiv -\binom{2k}{k} \lambda^k \sum_{x=1}^{p-1} x^{4k} \equiv -\binom{2k}{k} \lambda^k \cdot (-1) = \lambda^k \binom{2k}{k} \,(\mathrm{mod}\, p)\,.$$

(2). First, if $p = 4k + 1$, from (i) we have

$$a_p \equiv \lambda^k \binom{2k}{k} \not\equiv 0 \,(\mathrm{mod}\, p)\,.$$

Take $p = 4k + 3$, note that $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{0}{p}\right) = 0$and

$$\left(\frac{(-x)^3 + \lambda(-x)}{p}\right) = \left(\frac{-x^3 - \lambda x}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x^3+\lambda x}{p}\right),$$

From symmetry we obviously have

$$2a_p = -\sum_{x=1}^{p-1} \left(\left(\frac{x^3+\lambda x}{p}\right) + \left(\frac{-1}{p}\right)\left(\frac{x^3+\lambda x}{p}\right)\right) = 0,$$

Thus, $a_p = 0$, i.e., $a_p \equiv 0 \,(\mathrm{mod}\, p)$. □

Exercise 3.4 (i) Prove that the torsion subgroup of the group of $\mathbb{Q}$-points on the elliptic curve $y^2 = x^3 + d$ has order dividing 6. (ii) Show that the elliptic curve $y^2 = x^3 + 5$ has infinitely many $\mathbb{Q}$-points.

Proof. (i) Pending.

(ii) Take a point $P = (-1, 2) \in E(\mathbb{Q})$. If P is a torsion point, then from (i) we know that its order

is divisible by 6. However, calculating $2P$ yields

$$2P = \left(\frac{41}{16}, -\frac{299}{64}\right)$$

The coordinates are non-integer. However, according to the Lutz–Nagell theorem, the coordinates of the torsion points must be integers, a contradiction. Therefore, P is an infinite-order point, and thus $E(\mathbb{Q})$ has infinite points. □

Exercise 3.5 Show that if E has Weierstrass equation

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

with $a, b \in \mathbb{Z}$ and $P = (x, y) \in E(\mathbb{Q})$ is a point of finite order, then either $x = 0$ or x divides b and $x + a + b/x$ is a perfect square. [Thinking about how the proof of Lutz–Nagell works might help you find a short proof.]

Proof. Similar to the proof of Lutz–Nagell theorem, set $Q = (0, 0)$, note that $2Q = O$, Q is a 2-torsion point. If $P = (x, y) \in E(\mathbb{Q})_{\text{tor}}$ is a torsion point, then $P + Q$ is also. Calculate $k_{PQ} = y/x$,

$$x(P + Q) = k^2 - a - x = \left(\frac{y}{x}\right)^2 - a - x = \frac{x^3 + ax^2 + bx}{x^2} - a - x = \frac{b}{x}.$$

If $x = 0$, then $P = (0, 0) = Q \in E(\mathbb{Q})_{\text{tor}}$. If $x \neq 0$, $P + Q$ is also a torsion point, by Lutz–Nagell theorem, $x(P + Q) = b/x \in \mathbb{Z}$, $x|b$. At that time, $(y/x)^2 = x + a + b/x \in \mathbb{Z}$, i.e. $x + a + b/x$ is a square. □

Exercise 3.6 Let $p \geq 5$ be a prime, and let K be a finite extension of $\mathbb{Q}_p$. Show that every elliptic curve $E/\mathbb{Q}_p$ has a minimal Weierstrass equation of the form $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}_p$. What are the conditions on $v_p(a)$ and $v_p(b)$ for this to be a minimal Weierstrass equation? Show that if $E/\mathbb{Q}_p$ has good reduction then E/K has good reduction? Is the corresponding statement true if we replace "good" by "multiplicative"? What about the additive case?

Proof. (i) Existence of minimal Weierstrass equation: notice $p \neq 2, 3$, then we can simplify the Weierstrass equation into the form $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}_p$ through coordinate transformation. We can adjust a, b s.t. $a, b \in \mathbb{Z}_p$ by scaling

$$x \mapsto u^2 x,\ y \mapsto u^3 y,\ u \in \mathbb{Q}_p^\times \Rightarrow a' = u^4 a,\ b' = u^6 b,\ \Delta' = u^{12}\Delta.$$

We can choose one of that minimizes the p-adic valuation of Δ.

(ii) Let $x \mapsto u^{-2}x$, $y \mapsto u^{-3}y$, then $a' = u^{-4}a \in \mathbb{Z}_p$, i.e. $v_p(a) - 4v_p(u) \geq 0$. Similarly, $v_p(b) - 6v_p(u) \geq 0$, $v_p(\Delta') = v_p(\Delta) - 12v_p(u)$. Set $v_p(u) = k \geq 1$, notice the $v_p(\Delta')$ is minimal, then

that scaling must be the finally type, i.e.

$$v_p(a) < 4 \text{ or } v_p(b) < 6, \quad v_p(a), v_p(b) \in \mathbb{Z}.$$

(iii) If $E/\mathbb{Q}_p$ has good reduction, then exists a minimal Weierstrass equation s.t. $v_p(\Delta) = 0$. For any finite extension $K/\mathbb{Q}_p$, note v' as the extension of v, then $v'(\Delta) = ev_p(\Delta) = 0$, where e is the ramification index. Thus, E/K has a good reduction.

(iv) Multiplicative reduction and additive reduction:??? □

Exercise 3.7 Let K be a field of characteristic not 2. Let E/K be the curve defined by the singular Weierstrass equation $y^2 = x^2(x+1)$. Find a rational parametrisation $t \mapsto (\phi(t), \psi(t))$ with $t = 0, \infty$ mapping to the singular point and $t = 1$ mapping to the point at infinity. Use this to show that $E_{\text{ns}}(K) \cong K^\times$. [For the last part, try to find a method similar to the one used in lectures in the additive case.]

Proof. (i) The curve is singular at point $(0,0)$. We set $y = kx$ substitute into the equation:

$$(kx)^2 = x^2(x+1),\ x = k^2 - 1,\ y = kx = k(k^2-1).$$

This parametrization $(x, y) \mapsto (\alpha(k), \beta(k)) = (k^2 - 1, k(k^2-1))$ satisfies

- $k = \pm 1$: $\alpha(\pm 1) = \beta(\pm 1) = 0$, i.e. ± 1 mapping to the singular point;
- $k = \infty$: $\alpha(\infty) = \beta(\infty) = \infty$, i.e. ∞ mapping to the infinity point.

Let $t = \dfrac{k+1}{k-1}$, the required parametrization is

$$(x, y) \mapsto (\phi(t), \psi(t)) = \left(\frac{4t}{(t-1)^2}, \frac{4t(t+1)}{(t-1)^3} \right),$$

which satisfies

- $t = 0$: $\phi(0) = \psi(0) = 0$, i.e. 0 mapping to the singular point;
- $t = \infty$: $\phi(\infty) \to 0$, $\psi(\infty) \to 0$, i.e. ∞ mapping to the singular point;
- $t = 1$: $\phi(i) \to \infty$, $\psi(1) \to \infty$, i.e. 1 mapping to the infinity point.

(ii) Let $f : K^\times \to E_{\text{ns}}(K)$, $t \mapsto \begin{cases} (\phi(t), \psi(t)) & t \neq 1 \\ O_E & t = 1 \end{cases}$. (i) tells us f is a bijection. If

$$P = f(t_1) = \left(\frac{4t_1}{(t_1-1)^2}, \frac{4t_1(t_1+1)}{(t_1-1)^3} \right), \quad Q = f(t_2) = \left(\frac{4t_2}{(t_2-1)^2}, \frac{4t_2(t_2+1)}{(t_2-1)^3} \right),$$

we can calculate that $P + Q = f(t_1 t_2)$. If $P = O_E$, the result is also correct, i.e.the group structure of $E_{\text{ns}}(K)$ is correspond to multiplication group of $K^\times$, therefore, $E_{\text{ns}}(K) \cong K^\times$. □

Exercise 3.8 Let p be a prime number of the form $u^2 + 64$ for some integer u (e.g. $p = 73, 89, 113, 233, \ldots$). Choose the sign of u so that $u \equiv 1 \pmod 4$. Consider the two elliptic

curves

$$E : y^2 = x^3 + ux^2 - 16x$$

$$E' : y^2 = x^3 - 2ux^2 + px$$

Prove that E and E' are isogenous, and that both curves have good reduction at all primes different from p. Can you say anything about the Tamagawa numbers $c_p(E)$ and $c_p(E')$?

Proof. (i) From Exercise 4.1, for the general curve $y^2 = x^3 + ax^2 + bx$, the 2-isogeny with $(0, 0)$ as the kernel is $y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Here $a = u$ and $b = -16$, so the 2-isogeny is:

$$y^2 = x^3 - 2ux^2 + (u^2 + 64)x = x^3 - 2ux^2 + px$$

This is exactly E'. Therefore, E and E' are isogenous.

(ii) Compute the discriminant:

$$\Delta_E = 256p, \quad \Delta_{E'} = -256p^2.$$

Thus, for any odd prime $\ell \neq p$, we have $\ell \nmid \Delta_E$ and $\ell \nmid \Delta_{E'}$, so both E and E' have good reductions at $\ell \neq p$.

(iii) We know that for multiplicative reduction, the Tamagawa number depends on whether the reduction is split or non-split. First, note that $v_p(\Delta_E) = 1$, $v_p(\Delta_{E'}) = 2$, so E, E' are both multiplicative reductions at p.

For E: The modulus of the curve p is $y^2 = x^3 + ux^2 - 16x$. The singular point (s, y) satisfies $y = 0$ and $\partial f/\partial x \equiv 0 \pmod{p}$. Noting that $s^2 + us - 16 \equiv 0 \pmod{p}$, substituting $\partial f/\partial x$ yields $us \equiv 32 \pmod{p}$. Let $x = s + X$, $y = Y$, and substituting into the equation yields $Y^2 \equiv (3s + u)X^2 \pmod{p}$. Therefore, the slope of the tangent is $3s + u$. Calculation:

$$(3s + u)^2 = 9s^2 + 6us + u^2 = 9(-us + 16) + 6us + u^2 = 48 + u^2.$$

But $u^2 \equiv -64 \pmod{p}$, so $(3s + u)^2 \equiv -16 \pmod{p}$. And $p = u^2 + 64 \equiv 1 \pmod{4}$, so $3s + u$ is the square modulo p. This means the reduction type is splitting multiplication reduction, so $c_p(E) = 1$. Similarly, for E', we can also prove that the tangent slope is $-2u$, $(u/8)^2 \equiv -1$, and -1 is the fourth power, so $-2u$ is the square modulus p. Therefore, the reduction type is splitting multiplication reduction, so $c_p(E') = 1$. In summary, $c_p(E) = c_p(E') = 1$. □

Exercise 3.9 (i) Let E be an elliptic curve over an algebraically closed field K. Let $\phi : E \to E$ be a morphism of curves (not necessarily an isogeny). Show that if ϕ has no fixed points, then ϕ (and hence also ϕ^n) is a translation map.

(ii) Let $C/\mathbb{F}_q$ be a smooth projective curve of genus one. Show that $C(\mathbb{F}_q) \neq \varnothing$.

Proof. (i) Define the mapping:

$$f : E \to E, \quad f(P) = \phi(P) - P.$$

Since ϕ and group operations are morphisms, f is also a morphism. E is a projective curve, so f is either a constant-valued mapping or a surjective mapping. If f is a surjective mapping, then there exists $P \in E$ such that $f(P) = O$, i.e., $\phi(P) = P$, which contradicts the fact that ϕ has no fixed points. Therefore, f must be a constant-valued mapping, that is, there exists $Q \in E$ such that for any $P \in E$, we have:

$$\phi(P) = P + Q.$$

Thus, ϕ is a translation mapping. Furthermore, $\phi^n(P) = P + nQ$, also a translation mapping.

(ii) Note the Hasse–Weil bound:

$$||C(\mathbb{F}_p)| - (q+1)| \leq 2\sqrt{q} \Rightarrow |C(\mathbb{F}_p)| \geq q + 1 - 2\sqrt{q}.$$

For $q \geq 2$, $q + 1 - 2\sqrt{q} > 0$, so $C(\mathbb{F}_q) \neq \varnothing$. □

Exercise 3.10 Let $E/\mathbb{Q}_p$ be as in Question 6, with minimal discriminant Δ_E. Show that $v_p(\Delta_E)$ can take any positive integer value, but that if $v_p(\Delta_E) \geq 12$ then either E or its quadratic twist by p has multiplicative reduction.

Proof. Pending. □

Exercise 3.11 (Some group theory needed for Question 12.) For A an abelian group and $n \geq 2$ an integer we define

$$q(A) = \frac{\#\operatorname{coker}([n] : A \to A)}{\#\ker([n] : A \to A)}.$$

(It is undefined if either group is infinite.) Show that if $A \subset B$ is a subgroup of finite index, and either $q(A)$ or $q(B)$ is defined, then they are both defined and $q(A) = q(B)$.

Proof. First, the mapping is multiplication by n, so the kernel is the n-torsion point, and the cokernel is A/nA.

$$q(A) = \frac{\#\operatorname{coker}([n] : A \to A)}{\#\ker([n] : A \to A)} = \frac{|A/nA|}{|A[n]|}.$$

Thus, the finite group $C = B/A$ gives a short exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0,$$

Applying the mapping multiplication by n yields the commutative graph:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle [n]} & & \downarrow{\scriptstyle [n]} & & \downarrow{\scriptstyle [n]} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

The snake lemma gives an exact sequence

$$0 \to A[n] \to B[n] \to C[n] \to A/nA \to B/nB \to C/nC \to 0,$$

If $If q(A)$ is defined, then $|A/nA|$ and $|A[n]|$ are finite. Since the exact sequence and C are finite, we know that $|B[n]|$ and $|B/nB|$ are also finite, so $q(B)$ is defined. Similarly, if $q(B)$ is defined, then $q(A)$ is also defined. Furthermore, the order of the alternating product

$$\frac{|B[n]| \cdot |A/nA| \cdot |C/nC|}{|A[n]| \cdot |C[n]| \cdot |B/nB|} = 1.$$

Since C is a finite Abelian group, we have: $|C[n]| = |C/nC|$, so

$$\frac{|A/nA|}{|A[n]|} = \frac{|B/nB|}{|B[n]|}, \quad \text{i.e.} \quad q(A) = q(B).$$

□

Exercise 3.12 Let K be a finite extension of $\mathbb{Q}_p$. Let E/K be an elliptic curve and $n \geq 2$ an integer. Use Question 11 and the theory of formal groups to show that

(i) $\#(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n) = \#\mu_n(K) \cdot \#(\mathcal{O}_K/n\mathcal{O}_K)$**,**

(ii) $\#(E(K)/nE(K)) = \#E(K)[n] \cdot \#(\mathcal{O}_K/n\mathcal{O}_K)$**.**

Proof. (i) Consider the group $B = \mathcal{O}_K^\times$, so

$$q(B) = \frac{|\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^n|}{|\mu_n(K)|}.$$

Let π be the uniformizer of K, and take r large enough so that the logarithmic map $\log : 1 + \pi^r\mathcal{O}_K \to \mathcal{O}_K$ is a group isomorphism. This existence is due to the fact that K is a finite extension of $\mathbb{Q}_p$. Let $A = 1 + \pi^r\mathcal{O}_K$, then A is a finite exponential subgroup of B. Under the isomorphism $\log : A \to \mathcal{O}_K$, a $[n]$ mapping on A corresponds to a multiplication by n on $\mathcal{O}_K$, so

$$q(A) = \frac{|A/nA|}{|A[n]|} = |(\mathcal{O}_K/n\mathcal{O}_K)|.$$

Since A is a finite exponential subgroup of B, from Exercise 3.11 we have $q(B) = q(A)$, which is the result required in (i).

(ii) Consider the group $B = E(K)$, so

$$q(B) = \frac{|E(K)/nE(K)|}{|E(K)[n]|}.$$

Let π Let A be a uniformizer of K and let r be large enough so that the logarithmic map $\log : \hat{E}(\pi^r\mathcal{O}_K) \to \mathcal{O}_K$ is a group isomorphism, which exists because of the formal group theory of elliptic curves. Let $A = \hat{E}(\pi^r\mathcal{O}_K)$, then A is a finite exponential subgroup of B. Under the isomorphism $\log : A \to \mathcal{O}_K$, a $[n]$ mapping on A corresponds to a multiplication by n on $\mathcal{O}_K$, so

$$q(A) = \frac{|A/nA|}{|A[n]|} = |(\mathcal{O}_K/n\mathcal{O}_K)|.$$

Since A is a finite exponential subgroup of B, from Exercise 3.11 we have $q(B) = q(A)$, which is the

result required in (ii). □

4 Example Sheet 4

Exercise 4.1 Let E and E' be the elliptic curves (defined over a number field K) given by

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

with $a' = -2a$, $b' = a^2 - 4b$. Let $\phi : E \to E'$ be the 2-isogeny given by $\phi(x, y) = \left(y^2/x^2, y\left(x^2 - b\right)/x^2\right)$.

(i) Show that $T' = (0, 0)$ belongs to $\phi(E(K))$ if and only if $b' \in (K^\times)^2$.

(ii) Let $P = (x, y)$ in $E'(K)$ with $P \neq O, T'$. Let $t \in \bar{K}$ be a square root of x. Show that $\phi^{-1}(P) = \{(x_1, y_1), (x_2, y_2)\}$ where

$$x_1 = \frac{1}{2}(x - a + y/t),\ y_1 = x_1 t,\ x_2 = \frac{1}{2}(x - a - y/t),\ y_2 = -x_2 t.$$

(iii) Define $\alpha : E'(K) \to K^\times/(K^\times)^2$ via $\alpha(0) = 1, \alpha(T') = b'$ and $\alpha(x, y) = x$ if $x \neq 0$. Show that $\ker \alpha = \phi(E(K))$.

(iv) Suppose the line $y = \lambda x + \nu$ meets the curve E' in points P_1, P_2, P_3 (counted with multiplicity). Show that if $P_i = (x_i, y_i)$ for $i = 1, 2, 3$ then $x_1 x_2 x_3 = \nu^2$.

(v) Deduce that α is a group homomorphism. [There will be some special cases you need to check.]

Proof. (i) Take $Q = (x, y) \in E(K)$ s.t.

$$\phi(Q) = \left(\frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2}\right) = T' = (0, 0),$$

Substituting into $Q = (x, 0)$. Note that $\phi(0, 0) = O \neq T'$, so $x \neq 0$. Thus, x satisfies

$$0 = x^3 + ax^2 + bx = x(x^2 + ax + b) \Rightarrow x^2 + ax + b = 0,$$

This equation has a solution in K if and only if its discriminant $a^2 - 4b$ is a square in K. Since $a^2 - 4b = b'$, we have $b' \in (K^\times)^2$.

Conversely, if $b' \in (K^\times)^2$, then there exists $x \in K$ such that $x^2 + ax + b = 0$. Taking $Q = (x, 0)$, then $Q \in E(K)$ and:

$$\phi(Q) = \left(\frac{0}{x^2}, \frac{0 \cdot (x^2 - b)}{x^2}\right) = (0, 0) = T'.$$

(ii) Taking $t \in \overline{K}$ such that $t^2 = x$. definition:

$$x_1 = \frac{1}{2}\left(x - a + \frac{y}{t}\right), \quad y_1 = x_1 t, \quad x_2 = \frac{1}{2}\left(x - a - \frac{y}{t}\right), \quad y_2 = -x_2 t,$$

we check (x_1, y_1) and (x_2, y_2) on E and $\phi(x_i, y_i) = P$.

First, calculate $\phi(x_1, y_1)$. Take $\dfrac{y_1^2}{x_1^2} = \dfrac{(x_1 t)^2}{x_1^2} = t^2 = x$, verify:

$$\frac{y_1(x_1^2 - b)}{x_1^2} = \frac{x_1 t(x_1^2 - b)}{x_1^2} = t \cdot \frac{x_1^2 - b}{x_1} = y.$$

Calculate x_1^2:

$$x_1^2 = \frac{(x-a)^2}{4} + \frac{y^2}{4t^2} + \frac{(x-a)y}{2t} = \frac{(x-a)^2}{4} + \frac{y^2}{4x} + \frac{(x-a)y}{2t},$$

since $P \in E'$, substituting $y^2 = x^3 + a'x^2 + b'x = x^3 - 2ax^2 + (a^2 - 4b)x$, we obtain

$$x_1^2 = \frac{(x-a)^2 - 2b}{2} + \frac{(x-a)y}{2t},$$

note that $(x-a)^2 - 4b = \dfrac{y^2}{x} = \dfrac{y^2}{t^2}$, we obtain

$$x_1^2 - b = \frac{y^2}{2t^2} + \frac{(x-a)y}{2t} = \frac{1}{2t}\left(\frac{y^2}{t} + (x-a)y\right) = \frac{y}{2t}\left(\frac{y}{t} + (x-a)\right),$$

therefore

$$t \cdot \frac{x_1^2 - b}{x_1} = t \cdot \frac{y}{2t} \cdot \frac{\frac{y}{t} + (x-a)}{x_1} = \frac{y}{2} \cdot \frac{\frac{y}{t} + (x-a)}{x_1} = y,$$

This proves $\phi(x_1, y_1) = (x, y)$. Similarly, $\phi(x_2, y_2) = (x, y)$. Since ϕ is 2-isogeny, its kernel size is 2, so for $P \neq O, T'$, there are exactly two preimages, namely $\phi^{-1}(P) = \{(x_1, y_1), (x_2, y_2)\}$.

(iii) If $P \in \phi(E(K))$, then there exists $Q \in E(K)$ such that $\phi(Q) = P$. Obviously, when $P = O$ or $P = T'$, $\alpha(P) = 1$.

If $P = (x, y)$ and $x \neq 0$, then from (ii) we know that there exists $t \in \overline{K}$ such that $t^2 = x$, such that $x_1 = \dfrac{1}{2}(x - a + y/t) \in K$. From this we have $t = y/(2x_1 - (x-a)) \in K$, so x is square, that is, $\alpha(P) = 1$. Conversely, if $\alpha(P) = 1$, $P \neq O, T'$, take $t \in K$ such that $t^2 = x$, and let $x_1 = \dfrac{1}{2}(x - a + y/t) \in K$, then $(x_1, x_1 t) \in E(K)$ and $\phi(x_1, x_1 t) = P$, so $P \in \phi(E(K))$. Therefore $\ker \alpha = \phi(E(K))$.

(iv) Let $P_i = (x_i, y_i)$ be the intersection point and substitute into the E' equation, we have

$$(\lambda x + \nu)^2 = x^3 + a'x^2 + b'x \Rightarrow x^3 + (a' - \lambda^2)x^2 + (b' - 2\lambda\nu)x - \nu^2 = 0,$$

the roots of this cubic equation are x_1, x_2, x_3. By Vieta's Theorem,

$$x_1 x_2 x_3 = \nu^2.$$

(v) Consider the group structure of E, i.e., let $R = -(P + Q)$, then P, Q, R are collinear.

If the line does not pass through O, T', then the line is non-perpendicular and can be written as $y = \lambda x + \nu$. From (iv), if the x-coordinates of P, Q, R are all nonzero, then

$$x_P x_Q x_R = \nu^2 \Rightarrow \alpha(P)\alpha(Q)\alpha(R) = \alpha(P)\alpha(Q)\alpha(P+Q) = 1 \Rightarrow \alpha(P+Q) = \alpha(P)\alpha(Q),$$

note that the values of $\alpha(P)$ are all in the sense of $\left(\mathrm{mod}(K^\times)^2\right)$.

If the line passes through O, WLOG we may assume $P = O$, so $\alpha(P) = 1$, $P + Q = Q$,

$$\alpha(P+Q) = \alpha(Q) = 1 \cdot \alpha(Q) = \alpha(P)\alpha(Q).$$

If the line passes through T', WLOG we may assume $P = T'$, then $\alpha(P) = b'$, $\nu = 0$. Substituting into the curve equation, it is clear that $x_Q x_R = b'$, then

$$\alpha(T')\alpha(Q)\alpha(R) = b' \cdot x_Q \cdot x_R = b' \cdot b' = b'^2 \in (K^\times)^2,$$

then

$$\alpha(T')\alpha(Q)\alpha(R) = 1 \Rightarrow \alpha(R) = \alpha(T')\alpha(Q) = \alpha(T'+Q).$$

Thus α is a group homomorphism. □

Exercise 4.2 Prove that 2 is not a congruent number.

Proof. Let's recall the definition of a congruence number: a positive integer n is a congruence number if and only if the elliptic curve $E : y^2 = x^3 - n^2x$ has infinitely many rational points. For $n = 2$, consider the elliptic curve $E : y^2 = x^3 - 4x$, whose 2-isogeny curve is $E' : y^2 = x^3 + 16x$. Define the homomorphism:

$$\alpha_E : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \quad P = (x,y) \mapsto \begin{cases} x & x \neq 0 \\ -4 & x = 0 \end{cases} \left(\mathrm{mod}\,\mathbb{Q}^\times)^2\right).$$

$$\alpha_{E'} : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \quad P = (x,y) \mapsto \begin{cases} x & x \neq 0 \\ 16 & x = 0 \end{cases} \left(\mathrm{mod}\,\mathbb{Q}^\times)^2\right).$$

We can use the Lutz–Nagell theorem to find that the torsion points of E are $(0,0), (\pm 2, 0), O$, and the torsion points of E' are $(0,0), O$.

We calculate $\operatorname{im}\alpha_E$:

1. O: $\alpha_E(O) = 1$;
2. $(0,0)$: $\alpha_E(0,0) = -4 \equiv -1 \left(\mathrm{mod}(\mathbb{Q}^\times)^2\right)$;
3. $(\pm 2, 0)$: $\alpha_E(\pm 2, 0) = \pm 2$.

Thus, $|\operatorname{im}\alpha_E| = 4$. Then, we calculate $\operatorname{im}\alpha_{E'}$:

1. O: $\alpha_{E'}(O) = 1$;
2. $(0,0)$: $\alpha_{E'}(0,0) = 16 \equiv 1 \left(\mathrm{mod}(\mathbb{Q}^\times)^2\right)$.

Thus, $|\operatorname{im}\alpha_{E'}| = 1$. Then, we note that 2-descent gives

$$2^{\operatorname{rank} E(\mathbb{Q})} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4} = \frac{4 \times 1}{4} = 1,$$

So $\operatorname{rank} E(\mathbb{Q}) = 0$, therefore 2 is not a congruent number. □

Exercise 4.3 Compute the rank of $E(\mathbb{Q})$ for each of the following elliptic curves $E/\mathbb{Q}$. (i) $y^2 = x^3 + 6x^2 - 2x$ (ii) $y^2 = x^3 + 8x^2 - 7x$ (iii) $y^2 = x^3 - 3x^2 + 10x$ (iv) $y^2 = x^3 - 377x$.

Proof. Consider the elliptic curve $E : y^2 = x^3 + ax^2 + bx$, whose 2-isogeny curve is $E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Define the homomorphism:

$$\alpha_E : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \quad P = (x, y) \mapsto \begin{cases} x & x \neq 0 \\ b & x = 0 \end{cases} \left(\mathrm{mod}\, \mathbb{Q}^\times)^2\right).$$

$$\alpha_{E'} : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \quad P = (x, y) \mapsto \begin{cases} x & x \neq 0 \\ a^2 - 4b & x = 0 \end{cases} \left(\mathrm{mod}\, \mathbb{Q}^\times)^2\right).$$

(i) $E : y^2 = x^3 + 6x^2 - 2x$, then $E' : y^2 = x^3 - 12x^2 + 44x$, we calculate $\operatorname{im}\alpha_E$:

1. O: $\alpha_E(O) = 1$;
2. $(0, 0)$: $\alpha_E(0, 0) = -2 \left(\mathrm{mod}(\mathbb{Q}^\times)^2\right)$.

Thus, $|\operatorname{im}\alpha_E| = 2$. Then, we calculate $\operatorname{im}\alpha_{E'}$:

1. O: $\alpha_{E'}(O) = 1$;
2. $(0, 0)$: $\alpha_{E'}(0, 0) = 44 \equiv 11 \left(\mathrm{mod}(\mathbb{Q}^\times)^2\right)$.

Thus, $|\operatorname{im}\alpha_{E'}| = 2$. Then, we note that 2-descent gives

$$2^{\operatorname{rank} E(\mathbb{Q})} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4} = \frac{2 \times 2}{4} = 1,$$

So $\operatorname{rank} E(\mathbb{Q}) = 0$.

(ii) $E : y^2 = x^3 + 8x^2 - 7x$, then $E' : y^2 = x^3 - 16x^2 + 92x$, we calculate $\operatorname{im}\alpha_E$:

1. O: $\alpha_E(O) = 1$;
2. $(0, 0)$: $\alpha_E(0, 0) = -7 \left(\mathrm{mod}(\mathbb{Q}^\times)^2\right)$.

Thus, $|\operatorname{im}\alpha_E| = 2$. Then, we calculate $\operatorname{im}\alpha_{E'}$ similarly, $|\operatorname{im}\alpha_{E'}| = 4$. Then, we note that 2-descent gives

$$2^{\operatorname{rank} E(\mathbb{Q})} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4} = \frac{2 \times 4}{4} = 2,$$

So $\operatorname{rank} E(\mathbb{Q}) = 1$.

(iii) $E : y^2 = x^3 - 3x^2 + 10x$, then $E' : y^2 = x^3 + 6x^2 - 31x$, we calculate $\operatorname{im}\alpha_E$: $\operatorname{im}\alpha_E \subset K(S, 2)$, where $S = \{p|b\} = \{2, 5\}$, so the element in $K(S, 2)$ is $\pm1, \pm2, \pm5, \pm10$ and has size 8. We check whether the square-free divisor b_1 of b is in $\operatorname{im}\alpha_E$, that is, the equation $w^2 = b_1u^4 + au^2v^2 + b_2v^4$ has a solution on $\mathbb{Q}$ with $b_2 = 10/b_1$. The calculations show that there are solutions for all $b_1 > 0$ (i.e., $1, 2, 5, 10$), so $\operatorname{im}\alpha_E = \{1, 2, 5, 10\}$, $|\operatorname{im}\alpha_E| =$???. For E', $S' = \{p|b'\} = \{31\}$, the element in $K(S', 2)$ is $\pm1, \pm31$, with a size of 4. Similarly, checking b_1' in $\operatorname{im}\alpha_{E'}$ reveals that all b_1' (i.e., $1, -1, 31, -31$) have solutions, so $\operatorname{im}\alpha_{E'} = K(S', 2)$, $|\operatorname{im}\alpha_{E'}| = 4$. Then, we note that 2-descent

gives

$$2^{\text{rank } E(\mathbb{Q})} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4} = \frac{4 \times 4}{4} = 4,$$

So rank $E(\mathbb{Q}) = 2$.

(iv) $E : y^2 = x^3 - 377x$, then $E' : y^2 = x^3 + 1508x$, we calculate $\operatorname{im}\alpha_E$: the element in $K(S,2)$ is $\pm 1, \pm 13, \pm 29, \pm 377$, of size 8, all b_1 have solutions, so $\operatorname{im}\alpha_E = K(S,2)$, of size 8. For E', $S' = \{p|b'\} = \{2, 13, 29\}$, the element in $K(S',2)$ is $\pm 1, \pm 2, \pm 13, \pm 26, \pm 29, \pm 58, \pm 377, \pm 754$ and has size 16. We can find that $b_1' = 1, 13, 29, 377$ has a solution, and $b_1' = 2, 26, 58, 754$ has no solution. Therefore, $\operatorname{im}\alpha_{E'} = \{1, 13, 29, 377\}$ has a size of 4. Then, we note that 2-descent gives

$$2^{\text{rank } E(\mathbb{Q})} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4} = \frac{8 \times 4}{4} = 8,$$

So rank $E(\mathbb{Q}) = 3$. □

Exercise 4.4 Find the rank of $y^2 = x^3 - p^2x$ for p a prime with $p \equiv 3 \pmod 8$.

Proof. Consider the elliptic curve $E : y^2 = x^3 - p^2x$, whose 2-isogeny curve is $E' : y^2 = x^3 + 4p^2x$. Define the homomorphism:

$$\alpha_E : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \quad P = (x,y) \mapsto \begin{cases} x & x \neq 0 \\ -p^2 & x = 0 \end{cases} \left(\text{mod } \mathbb{Q}^\times\right)^2).$$

$$\alpha_{E'} : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \quad P = (x,y) \mapsto \begin{cases} x & x \neq 0 \\ 4p^2 & x = 0 \end{cases} \left(\text{mod } \mathbb{Q}^\times\right)^2).$$

Obviously

$$\Delta_E = 2^6 \cdot p^6, \quad \Delta_{E'} = -2^{12} \cdot p^6,$$

we can use the Lutz–Nagell theorem to find that the torsion points of E are $(0,0), (\pm p, 0), O$, and the torsion points of E' are $(0,0), O$.

We calculate $\operatorname{im}\alpha_E$:

1. O: $\alpha_E(O) = 1$;
2. $(0,0)$: $\alpha_E(0,0) = -p^2 \equiv -1 \left(\text{mod}(\mathbb{Q}^\times)^2\right)$;
3. $(\pm p, 0)$: $\alpha_E(\pm p, 0) = \pm p$.

Thus, $|\operatorname{im}\alpha_E| = 4$. Then, we calculate $\operatorname{im}\alpha_{E'}$:

1. O: $\alpha_{E'}(O) = 1$;
2. $(0,0)$: $\alpha_{E'}(0,0) = 4p^2 \equiv 1 \left(\text{mod}(\mathbb{Q}^\times)^2\right)$.

Thus, $|\operatorname{im}\alpha_{E'}| = 1$. Then, we note that 2-descent gives

$$2^{\text{rank } E(\mathbb{Q})} = \frac{|\operatorname{im}\alpha_E| \cdot |\operatorname{im}\alpha_{E'}|}{4} = \frac{4 \times 1}{4} = 1,$$

So rank $E(\mathbb{Q}) = 0$. □

Exercise 4.5 Let $\nu(x)$ be the number of distinct prime factors of an integer x. Show that if $E/\mathbb{Q}$ is an elliptic curve with Weierstrass equation $y^2 = x^3 + ax^2 + bx$ with $a, b \in \mathbb{Z}$ then

$$\operatorname{rank} E(\mathbb{Q}) \leq \nu(b) + \nu\left(a^2 - 4b\right).$$

By considering real solubility, show that the inequality is strict. [This last part is easier if $a = 0$, so assume that if you like.]

Proof. (i) Consider the elliptic curve $E : y^2 = x^3 + ax^2 + bx$, whose 2-isogeny curve is $E' : y^2 = x^3 - 2ax^2 + (a^2 - 4b)x$. Define the homomorphism:

$$\alpha_E : E(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \quad P = (x, y) \mapsto \begin{cases} x & x \neq 0 \\ b & x = 0 \end{cases} \left(\operatorname{mod} \mathbb{Q}^\times)^2\right).$$

$$\alpha_{E'} : E'(\mathbb{Q}) \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \quad P = (x, y) \mapsto \begin{cases} x & x \neq 0 \\ a^2 - 4b & x = 0 \end{cases} \left(\operatorname{mod} \mathbb{Q}^\times)^2\right).$$

Notice $\operatorname{im} \alpha_E \subset K(S, 2)$ where S is all primes dividing b, and $\operatorname{im} \alpha_{E'}$ is similar. Then

$$\begin{aligned} &|\operatorname{im} \alpha_E| \leq 2^{\nu(b)+1}, \quad \operatorname{im} \alpha_{E'} \leq 2^{\nu(a^2-4b)+1} \\ \Rightarrow &\operatorname{rank} E(\mathbb{Q}) = \log_2 \frac{|\operatorname{im} \alpha_E| \cdot |\operatorname{im} \alpha_{E'}|}{4} \leq \nu(b) + \nu(a^2 - 4b). \end{aligned}$$

(ii) In Exercise 4.3(iv), $\nu(b) + \nu(a^2 - 4b) = 2 + 3 = 5$, but rank $= 3 < 5$. Therefore, the inequality holds strictly. □

Exercise 4.6 Let E be an elliptic curve over $\mathbb{Q}$ and let $P \in E(\mathbb{Q})$. Show that P is a torsion point if and only if $\hat{h}(P) = 0$. [This gives another proof that the torsion subgroup is finite.]

Proof. We define the canonical height as:

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n}, \quad h(a/b, y) = \log \max\{|a|, |b|\}.$$

If P is a torsion point, then there exists a positive integer n such that $nP = O$,

$$0 = \hat{h}(O) = \hat{h}(nP) = n^2 \hat{h}(P) \Rightarrow \hat{h}(P) = 0.$$

If $\hat{h}(P) = 0$, then for any $n \in \mathbb{Z}_+$, $\hat{h}(2^n P) = 4^n \hat{h}(P) = 0$, then

$$|h(2^n P) - \hat{h}(2^n P)| < \varepsilon \quad \Rightarrow \quad h(2^n P) < \varepsilon.$$

Clearly, $\{2^n P \mid n \geq 0\}$ is a finite set, so there exist distinct m, n such that $2^m P = 2^n P$, i.e., $|2^m - 2^n|P = O$, with P being a torsion point. □

Exercise 4.7 Show that if $\phi : E \to E'$ and $\psi : E' \to E''$ are isogenies defined over a number

field K, then there is an exact sequence

$$E'(K)\left[\psi\right] \to S^{(\phi)}(E/K) \to S^{(\psi\phi)}(E/K) \to S^{(\psi)}\left(E'/K\right).$$

Deduce from results proved in lectures that $S^{(\phi)}(E/K)$ is finite.

Proof. We change the notation $S^{(\phi)}$ to Sel_ϕ. Consider the composition $\psi\phi : E \to E''$ is also an isogeny. There is a canonical exact sequence of kernel groups

$$0 \to E[\phi] \xrightarrow{\phi'} E[\psi\phi] \xrightarrow{\phi} E'[\psi] \to 0,$$

where ϕ' is inclution, $\phi : E[\psi\phi] \to E'[\psi]$ is surjective. Obviously we konw that $H^0(K, E[\phi]) = (E[\phi])^{\mathrm{Gal}_K} = E(K)[\phi]$, then this short exact sequence of Gal_K-modules induces a long exact sequence in Galois cohomology $H^i(K, -) \coloneqq H^i(\mathrm{Gal}_K, -)$:

$$\begin{array}{ccccccc} 0 & \longrightarrow & E(K)[\phi] & \longrightarrow & E(K)[\psi\phi] & \longrightarrow & E'(K)[\psi] \\ & & & & & \overset{\delta}{\swarrow} & \\ & & H^1(K, E[\phi]) & \xrightarrow[\alpha]{} & H^1(K, E[\psi\phi]) & \xrightarrow[\beta]{} & H^1(K, E'[\psi]). \end{array}$$

By definition of the Selmer group

$$\mathrm{Sel}_\phi(E/K) \coloneqq \left\{c \in H^1(K, E[\phi]) \,\middle|\, \mathrm{res}_v(c) \in \operatorname{im}\kappa_v,\ \forall v \in \Sigma_K\right\} \subset H^1(K, E[\phi]),$$

notice that the restriction is a chain map of any complex, then Galois cohomology induces a commutative diagram

$$\begin{array}{ccccccc} E'(K)[\psi] & \xrightarrow{\delta} & H^1(K, E[\phi]) & \xrightarrow{\alpha} & H^1(K, E[\psi\phi]) & \xrightarrow{\beta} & H^1(K, E'[\psi]) \\ \downarrow & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} \\ E'(K_v)[\psi] & \longrightarrow & H^1(K_v, E[\phi]) & \longrightarrow & H^1(K_v, E[\psi\phi]) & \longrightarrow & H^1(K_v, E'[\psi]) \end{array}$$

thus we show the maps α, β, δ can be restrict to maps between Selmer groups.

From the cohomology sequence, $\alpha\delta = 0$, then $\operatorname{im}\delta \subset \ker\alpha$. Conversely, if $c \in \ker\alpha \cap \mathrm{Sel}_\phi(E/K)$, by exactness of the cohomology sequence, $\exists Q \in E(K)[\psi]$, $c = \delta(Q) \in \mathrm{Sel}_\phi(E/K)$, $\ker\alpha \subset \operatorname{im}\delta$. Similarly, $\ker\beta = \operatorname{im}\alpha$. Then the sequence

$$E'(K)[\psi] \to \mathrm{Sel}_\phi(E/K) \to \mathrm{Sel}_{\psi\phi}(E/K) \to \mathrm{Sel}_\psi(E'/K)$$

is exact. □

Exercise 4.8 Let E be an elliptic curve over $\mathbb{Q}$. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer. The quadratic twist E_d of E by d was defined in Question 7 on Example Sheet 1. Show that there is a group homomorphism $E(\mathbb{Q}) \times E_d(\mathbb{Q}) \to E(K)$ with finite kernel and

cokernel. Deduce that

$$\operatorname{rank} E(K) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E_d(\mathbb{Q}).$$

Proof. Pending. □

Exercise 4.9 **Let E be an elliptic curve over $\mathbb{C}$. Let ω be an invariant differential on E. Show that the map $\operatorname{End}(E) \to \mathbb{C}; \phi \mapsto \phi^*\omega/\omega$ is an injective ring homomorphism. Use this to check that the 2-isogenies ϕ and $\widehat{\phi}$ (as defined in Question 1 and in lectures) are indeed dual isogenies.**

Proof. Pending. □

Exercise 4.10 **Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x(x+1)(x+4)$. (i) Compute the rank and torsion subgroup of $E(\mathbb{Q})$. [For the latter you may quote your answer from Question 2 on Example Sheet 3.] (ii) Show that if $r, s, t \in \mathbb{Q}^\times$ with $r^2, s^2, 1, t^2$ in arithmetic progression then**

$$\left(-2s^2, 2rst\right) \in E(\mathbb{Q}).$$

(iii) Deduce the result of Euler that there are no non-constant four term arithmetic progressions of square numbers.

Proof. Pending. □

Exercise 4.11 **Let E be an elliptic curve defined over a number field K with $E[2] \subset E(K)$, say $y^2 = f(x) = (x-e_1)(x-e_2)(x-e_3)$ with $e_1, e_2, e_3 \in K$. (i) Define a group homomorphism $\delta : E(K) \to K^\times/(K^\times)^2 \times K^\times/(K^\times)^2$ with kernel $2E(K)$. Using your answer to Question 1, or otherwise, show that it is given by**

$$(x,y) \mapsto \begin{cases} (x-e_1, x-e_2) & \text{if } x \neq e_1, e_2 \\ (f'(e_1), e_1 - e_2) & \text{if } x = e_1 \\ (e_2 - e_1, f'(e_2)) & \text{if } x = e_2 \end{cases}$$

(ii) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 - x$. Compute $\delta(T)$ for each $T \in E(\mathbb{Q})[2]$. Show, by adapting the proof in the first lecture, that these elements generate the image of δ. Deduce that $\operatorname{rank} E(\mathbb{Q}) = 0$.

Proof. Pending. □