-

MA426: Elliptic Curves

Samuele Anni

http://www2.warwick.ac.uk/fac/sci/maths/people/staff/anni/

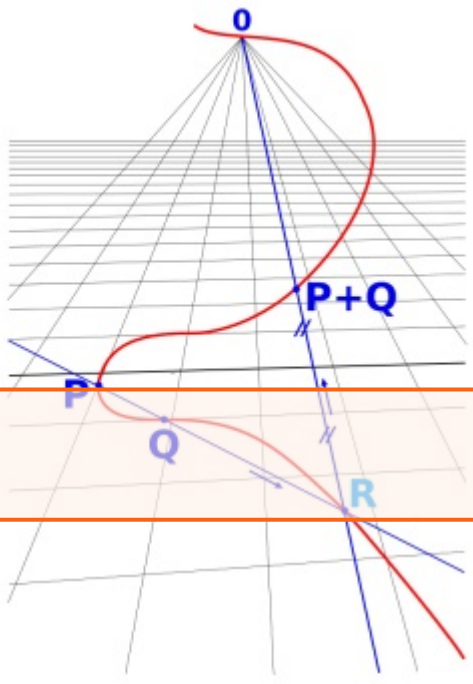
These lecture notes are based on a variety of sources, mainly:

- Notes from a course taught by Lassina Dembélé in 2013;
- Notes from a course taught by John Cremona in 2011;
- Notes from a course taught by Luis Dieulefait, Angelas Arenas and Núria Vila that I took at the Universitat de Barcelona in 2009;
- Notes from Peter Stevenhagen, Universiteit Leiden;
- Lawrence C. Washington, *Elliptic curves. Number theory and cryptography.* Second edition. Discrete Mathematics and its Applications. Chapman & Hall(2008);
- Joseph H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009;
- Dale Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, 111, Springer-Verlag, New York, 2004.

Send corrections, ask questions or make comments to

s.anni@warwick.ac.uk.

First printing, December 2014



Contents

1 Introduction 7

1.1 Plane curves 7
1.2 Projective space and homogenisation 8
1.3 Rational points on curves 10
1.4 Bachet-Mordell equation 12
1.5 Congruent number curves 13
1.6 A brief review on fields 14

2 Elliptic curves and group law 17

2.1 Weierstrass equations and elliptic curves 17
2.2 Discriminant 18
2.3 Bezout's theorem 22
2.4 Definition of the group law 23
2.4.1 Associativity of the group law 25
2.4.2 Computing with the group law 28
2.5 Singular curves 29

3 Applications I 33

3.1 Integer Factorization Using Elliptic Curves 33
3.1.1 Pollard's $(p-1)$-Method 33
3.1.2 Lenstra's Elliptic Curve Factorization Method 35
3.1.3 A Heuristic Explanation 36

4 Isomorphisms and j-invariant 37

4.1 Isomorphisms and j-invariant 37

5 Elliptic curves over $\mathbb{C}$ 41
5.1 Lattices and elliptic functions 41
5.2 Tori and elliptic curves 46
5.3 Torsion points. 49
5.4 Elliptic curves over $\mathbb{R}$ 49

6 Endomorphisms of elliptic curves 51
6.1 Rational functions and endomorphisms 51
6.2 Separable endomorphisms 54
6.3 Parallelogram identity and degree map 60
6.4 The endomorphism ring 64
6.5 Automorphisms of elliptic curves 65

7 Elliptic Curves over finite fields 67
7.1 j-invariant characteristic 2 and 3 67
7.1.1 Elliptic curves in characteristic 2 67
7.1.2 The j-invariant in characteristic 3 69
7.2 Isomorphism classes 69
7.3 The Frobenius endomorphism 69
7.4 Hasse's Inequality 70
7.5 Endomorphism ring 72

8 Points of finite order 73
8.1 Points of finite order 73
8.2 Division polynomials 76
8.3 Galois representations 76

9 Elliptic curves over $\mathbb{Q}$: torsion 79
9.1 Valuations 79
9.2 Integral models 81
9.3 Torsion subgroup: The Lutz-Nagell Theorem 82
9.4 Reduction mod p 87

10 The Mordell–Weil Theorem 91
10.1 Heights 92
10.2 Heights on elliptic curves 95
10.3 Isogenies and descent 98
10.3.1 Isogenies 98
10.3.2 2-isogenies and the descent map 99

10.4 The Weak Mordell-Weil Theorem **103**

10.5 The Mordell-Weil Theorem **106**

11 Applications II 109

11.1 Elliptic Curve Cryptography **109**

11.1.1 Cryptography 109
11.1.2 Diffie-Hellman 111
11.1.3 ElGamal Cryptosystem 112
11.1.4 Elliptic Curve Discrete Logarithm Problem 113

11.2 Schoof's algorithm **114**

12 Advanced topics 117

12.1 The Birch and Swinnerton-Dyer Conjecture **117**

12.2 Modularity **119**

Index 125

Plane curves

Projective space and homogenisation

Rational points on curves

Bachet-Mordell equation

Congruent number curves

A brief review on fields

1. Introduction

Elliptic curves link number theory, geometry, analysis and algebra, and they find applications in a wide range of areas including

- number theory, they are useful for solving Diophantine equations,i.e. polynomial equations in integers or rational numbers, such as the Fermat Last Theorem;
- algebra, one can use them to solve instances of the *Inverse Galois Problem*, for example for solving quintic polynomial equations;
- arithmetic, they are useful in the factorization of integers;
- cryptography, they are use in smart cards and in a lot of protocols.

Although the study of elliptic curves dates back to the ancient Greeks, there are still many open research problems. Elliptic curves are arguably one of the most interesting and fun research areas in mathematics. And now we begin our short journey.

Throughout these notes, K will denote a field.

1.1 Plane curves

Definition 1.1 A **plane curve** C over K is the set of solutions to an equation $f(x,y) = 0$, where $f(x,y)$ is a polynomial in two variables with coefficients in K. We say that C is a **line** (resp. a **conic** or a **cubic**) if the degree of f is 1 (resp. 2 or 3).

Example 1.1.0.1 (a) Lines are the simplest examples of plane curves. They are given by equations of the form

$$ax + by = c,$$

where $a, b, c \in K$ are not all zero.

(b) Let $K = \mathbb{Q}$, the plane curve $C : y - x^2 = 0$ is a parabola over $\mathbb{Q}$.

(c) Let $K = \mathbb{Q}$, the curve $C : y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Q}$, is a plane cubic.

(d) Let $n \in \mathbb{N}$, then the curve $C_n : x^n + y^n = 1$ is a plane curve. It is called a *Fermat curve* (see Figure 1.1).

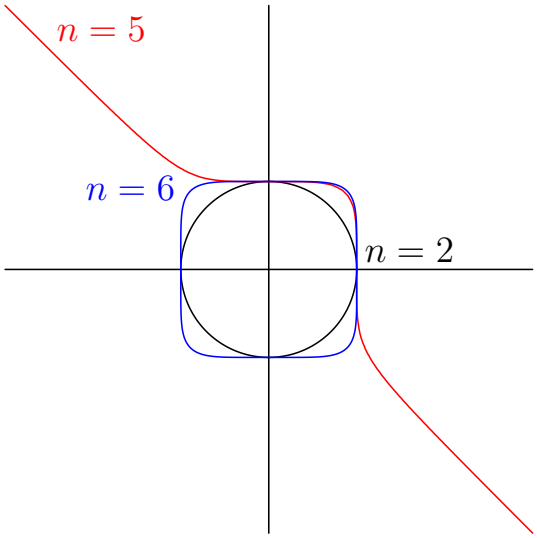


Figure 1.1: Examples of Fermat curves $x^n + y^n = 1$

1.2 Projective space and homogenisation

Definition 1.2 Let $d \geq 1$ be an integer. The d-dimensional **projective space** is defined by

$$\mathbf{P}^d(K) := \left(K^{d+1} \setminus \{(0,\dots,0)\}\right) / \sim$$

where $(x_0,\dots,x_d) \sim (y_0,\dots,y_d)$ if and only if there exists $\lambda \in K^\times$ such that $y_i = \lambda x_i$ for all $i = 0,\dots,d$. We denote the equivalence class of $(x_0,\dots,x_d)$ by $[x_0 : \cdots : x_d]$.
We call $\mathbf{P}^1(K)$ (resp. $\mathbf{P}^2(K)$) the **projective line** (resp. **projective plane**) over K.

By definition,

$$\mathbf{P}^1(K) := \left\{(x,y) \in K^2 : (x,y) \neq (0,0)\right\} / \sim .$$

There is a natural inclusion

$$\phi : K \hookrightarrow \mathbf{P}^1(K) \qquad x \mapsto [x : 1],$$

whose image is given by $\mathrm{im}(\phi) = \left\{[x : y] \in \mathbf{P}^1(K) : y \neq 0\right\}$.

Note that $[x : y] \in \mathbf{P}^1(K)$ is not in the image of ϕ if and only if $y = 0$. Hence,

$$\mathbf{P}^1(K) = \mathrm{im}(\phi) \sqcup \{[x : 0] : x \neq 0\} = \{[x : 1] : x \in K\} \sqcup \{[1 : 0]\} \simeq K \sqcup \{\infty\}.$$

The equivalence classes in $\mathbf{P}^1(K)$ are lines through the origin in the plane, and the last equality simply says that such lines are determined by their slopes. The point $[1 : 0]$, which corresponds to the line of ∞-slope, is called the *point at infinity* and is denoted by ∞.

Similarly, the projective plane $\mathbf{P}^2(K)$ can be described as follows:

$$\begin{aligned}\mathbf{P}^2(K) &:= \{(x,y,z) \in K^3 : (x,y,z) \neq (0,0,0)\} / \sim \\ &= \{[x:y:z] \in K^3 : z \neq 0\} \cup \{[x:y:0] : (x,y) \neq (0,0)\} \\ &= \{[x:y:1] : x,y \in K\} \sqcup \{z=0\} \simeq K^2 \sqcup \{z=0\},\end{aligned}$$

where the set $z=0$ is called the *line at* ∞.

Definition 1.3 (a) Let $F(X,Y,Z) \in K[X,Y,Z]$ be a polynomial of (total) degree d. We say that F is **homogeneous** if every term of F has degree d, *i.e*, if F is of the form

$$F(X,Y,Z) = \sum_{\substack{0 \leq i,j,k \leq d \\ i+j+k=d}} c_{ijk} X^i Y^j Z^k.$$

(b) Let $f(x,y) \in K[x,y]$ be a polynomial of degree d. The polynomial $F(X,Y,Z)$ given by

$$F(X,Y,Z) = Z^d f(\frac{X}{Z}, \frac{Y}{Z})$$

is homogeneous of degree d, called the **homogenisation** of f (with respect to the variable Z).

Let $F \in K[X,Y,Z]$ be a homogeneous polynomial of degree d. Then, we see that

$$F(\lambda X, \lambda Y, \lambda Z) = \lambda^d F(X,Y,Z) \text{ for all } \lambda \in K.$$

Hence, $F(a,b,c) = 0$ implies that $F(\lambda a, \lambda b, \lambda c) = 0$. Therefore the set of zeros is well-defined.

Definition 1.4 Let $F \in K[X,Y,Z]$ be a homogeneous polynomial, the **projective plane curve** $\mathscr{C}$ defined by F is the set of solutions to $F(a,b,c) = 0$ in the projective plane.

Example 1.2.0.2 The homogenisations of the curves in Example 1.1.0.1 are as follows:

(a) The parabola $C : y - x^2 = 0$ becomes $\mathscr{C} : ZY - X^2 = 0$.

(b) The plane cubic $C : y^2 = x^3 + ax + b$ becomes $\mathscr{C} : ZY^2 = X^3 + aXZ^2 + bZ^3$.

(c) The Fermat curve $C_n : x^n + y^n = 1$ becomes $\mathscr{C}_n : X^n + Y^n = Z^n$.

Example 1.2.0.3 It is possible also to dehomogenise projective curves. The dehomogenisation of the curve $\mathscr{C} : Y^2Z - X^3 + 2XZ^2 + 2Z^3 = 0$ with respect to the variable Z is the cubic $C : y^2 - x^3 + 2x + 2 = 0$. Moreover, given a projective curve we can easily find the intersection with the line at infinity, it is enough to set $Z = 0$. In this example this implies that $X^3 = 0$. So $Y \neq 0$ and $[X:Y:Z] = [0:1:0]$ is the unique point at infinity on the curve $\mathscr{C}$.

Definition 1.5 Let $\mathscr{C}$ be a projective curve and P be a point on $\mathscr{C}$. We say that P is **singular** if $\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0$. Otherwise, we say that P is **non-singular** or **smooth**. A projective curve is called **smooth** is for every P on $\mathscr{C}$ the curve is smooth at P.

Example 1.2.0.4 (a) The partial derivative of the curve in Example 1.2.0.3 are

$$\frac{\partial F}{\partial X} = -3X^2 + 2Z^2, \quad \frac{\partial F}{\partial Y} = 2YZ, \text{ and } \frac{\partial F}{\partial Z} = Y^2 + 4XZ + 6Z^2.$$

The point at infinity $[0:1:0]$ is non-singular. So if $P = [x:y:z] \neq [0:1:0]$ is singular, then $y = 0$ and $z \neq 0$. In this case, $\partial F/\partial Z = 2z(2x+3z) = 0$, which implies that $2x = -3z \neq 0$. Hence $\partial F/\partial X \neq 0$, which is a contradiction. So the curve is non-singular.

1.3 Rational points on curves

Definition 1.6 Let $C : f(x,y) = 0$ be a plane curve. We say that $P = (a,b)$, with $a,b \in K$, is a K-**rational point** on C if $f(a,b) = 0$. The set of all K-rational points on C will be denoted by $C(K)$.
Similarly, let $\mathscr{C} : F(x,y,z) = 0$ be a projective curve. Then, we say that $P = [a:b:c]$, with $a,b,c \in K$, is a K-**rational point** on $\mathscr{C}$ if $F(a,b,c) = 0$. We denote the set of all K-rational points on $\mathscr{C}$ by $\mathscr{C}(K)$.

Since ancient Greeks, the following problem has always fascinated mathematicians.

Question 1.3.1 Let $C : f(x,y) = 0$ be a plane curve over $\mathbb{Q}$. Does C have any rational point? In other words, is $C(\mathbb{Q})$ not empty? and if $C(\mathbb{Q})$ is not empty, can we describe this set?

We can reformulate this question using projective plane curves.

Question 1.3.2 Let $\mathscr{C} : F(x,y,z) = 0$ be a projective plane curve over $\mathbb{Q}$. Does $\mathscr{C}$ have any rational point? In other words, is $\mathscr{C}(\mathbb{Q})$ not empty? If $\mathscr{C}(\mathbb{Q})$ is not empty, can we describe this set?

Example 1.3.2.1 The curve $X^2 + Y^2 + Z^2 = 0$ has no rational (or real) points.

Example 1.3.2.2 The curve $x^2 + y^2 = 3$ has no rational points.

Proof. It is enough to show that the homogenized curve $\mathscr{C} : X^2 + Y^2 = 3Z^2$ has no rational point. For a contradiction, assume that $[a:b:c] \in \mathscr{C}$ is rational, i.e. $a^2 + b^2 = 3c^2$ with $a,b,c \in \mathbb{Q}$ not all zero. Then, without loss of generality, we can assume that $a,b,c \in \mathbb{Z}$, and are coprime. By reducing modulo 4, we would have: $a^2, b^2, c^2 \equiv 0$ or $1 \bmod 4$. This implies that $3c^2 \equiv 0, 3 \bmod 4$, and that a,b,c must all be even, which is a contradiction. ∎

Around 250 A.D., Diophantus of Alexandria studied Question 1.3.1 for lines, conics and cubics. In this course, we will see that our understanding of this problem for cubics is still far from being complete. In the 16th century, Diophantus' work was studied by Pierre de Fermat, who gave his name to the so-called Fermat's Last Theorem (FLT). This only became a theorem in 1995 thanks to the British mathematician Andrew Wiles.

Theorem 1.3.3 — Wiles. Let $n \geq 3$ be a natural number. A triple (a,b,c), with $a,b,c \in \mathbb{Z}$, satisfies the equation $a^n + b^n = c^n$ only if $abc = 0$.

Without loss of generality, assume that $c \neq 0$, and set $x = a/c$ and $y = b/c$ in $\mathbb{Q}$. Then, FLT says that, for $n \geq 3$, the curve $C_n : x^n + y^n = 1$ has no rational points, except for $(0, \pm 1), (\pm 1, 0)$ for n even, and $(0,1), (1,0)$ for n odd.

In contrast, for $n = 2$, we know that FLT has infinitely many solutions by Pythagoras Theorem. Indeed, recall that we can parametrize rational points on C_2 by using the map

$$\begin{array}{rcl} \mathbb{Q} & \to & C_2(\mathbb{Q}) \setminus \{(-1,0)\} \\ t & \mapsto & (\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}), \end{array}$$

which is a bijection, with inverse given by $(x,y) \mapsto \frac{y}{1+x}$.

We homogenize this parametric solution by setting $t = T/U$ to get the (projective) map

$$\begin{aligned} &\mathbf{P}^1(\mathbb{Q}) \to \mathscr{C}_2(\mathbb{Q}) \\ &[T:U] \mapsto [U^2 - T^2 : 2TU : U^2 + T^2]. \end{aligned}$$

We thus obtain the commutative diagram

$$\begin{array}{ccc} \mathbb{Q} & \longrightarrow & C_2(\mathbb{Q}) \\ \phi \downarrow & & \| \\ \mathbf{P}^1(\mathbb{Q}) & \longrightarrow & \mathscr{C}_2(\mathbb{Q}) \end{array}$$

The bottom arrow is a bijection, which yields all the rational points on $\mathscr{C}_2$. In particular, we recover the "missing point" on C_2: $(-1,0) \leftrightarrow [-1:0:1]$ for $t = \infty \leftrightarrow [1:0]$. As a consequence, all the triples $(a,b,c) \in \mathbb{Z}^3$ satisfying FLT for $n = 2$ are of the form:

$$a = m^2 - n^2, b = 2mn, c = m^2 + n^2,\ m,n \in \mathbb{Z} \text{ and } mn \neq 0.$$

It follows from the theorem below that there is no such parametric solution for $n \geq 3$.

Theorem 1.3.4 — FLT for polynomials. For $n \geq 3$, there are no polynomials $a(t), b(t), c(t)$ satisfying $a^n + b^n = c^n$, and which are non-constant and with no common factors.

Proof. Exercise: easy to prove. [*Hint*: differentiate.] ■

Let us see another example where the obstruction to the existence of rational solutions comes from arithmetic.

Example 1.3.4.1 The equation $Y^2 = X^3 + 6$ has no integral solutions.

Proof. Assume there is an integral solution (x,y). First we will show that x is odd, and in fact $x \equiv 3 \bmod 8$. If x is even then $y^2 \equiv 6 \bmod 8$, which is impossible. Thus x is odd, so y is odd and $x^3 = y^2 - 6 \equiv -5 \equiv 3 \bmod 8$. Since $x^3 \equiv x \bmod 8$, we have $x \equiv 3 \bmod 8$. Rewrite $y^2 = x^3 + 6$ as

$$y^2 + 2 = x^3 + 8 = (x+2)(x^2 - 2x + 4),$$

with $x^2 - 2x + 4 \equiv 3^2 - 2 \cdot 3 + 4 \equiv 7 \bmod 8$. For any prime factor p of $x^2 - 2x + 4$, we have $y^2 + 2 \equiv 0 \bmod p$, so -2 is a square $\bmod p$, and therefore $p \equiv 1, 3 \bmod 8$. Since $x^2 - 2x + 4 = (x-1)^2 + 3$ is positive and congruent to 7 mod 8, not all its factor can be congruent to 1 or 3 mod 8 (notice that $\{1,3\}$ is a subgroup in $\mathbb{Z}/8\mathbb{Z}^*$). So we have a contradiction. To get a contradiction using the factor $x+2$, note that this number is positive: if $x + 2 < 0$ then $y^2 + 2 \leq 0$, which is impossible. For any prime p dividing $x+2$, then $y^2 + 2 \equiv 0 \bmod p$, so $p \equiv 1$ or $3 \bmod 8$. Since $x \equiv 3 \bmod 8$, we have $x + 2 \equiv 5 \bmod 8$, so there exist a prime not congruent to 1 or 3 mod 8 dividing it. ■

1.4 Bachet-Mordell equation

Let $c \in \mathbb{Z}$ be non-zero, and consider the equation

$$y^2 - x^3 = c. \tag{1.1}$$

A rational solution (x,y) to the Bachet-Mordell equation (1.1) is a *rational point* on the plane cubic (1.1). Bachet discovered that if $P = (x,y)$ is a point on (1.1), then so is

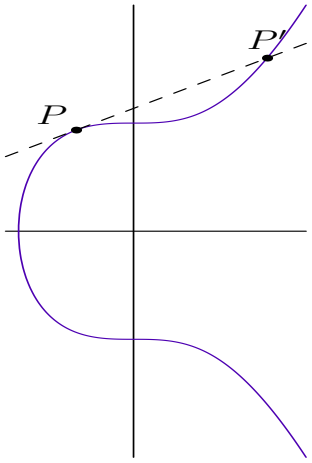
$$P' = \left(\frac{x^4 - 8cx}{4y^2}, \frac{-x^6 - 20cx^3 + 8c^2}{8y^3} \right).$$

Example 1.4.0.2 For $c = -2$, $P = (3,5)$ is a rational point on $y^2 - x^3 = -2$, and we have:

$$P = (3,5) \mapsto P' = \left(\frac{129}{100}, \frac{383}{1000} \right) \mapsto P'' = \left(\frac{2340922881}{(7660)^2}, \frac{113259286337279}{(7660)^3} \right) \mapsto \text{etc}$$

Fact: The sequence P, P', P",... never repeats. Hence, for $c = -2$, the equation (1.1) has infinitely many rational solutions.

A natural question is, where does this construction come from? The answer is from geometry!



Let $P = (x,y)$ be a point on $C : y^2 - x^3 = c$. Then the tangent to C at P has slope $\frac{3x^2}{2y}$ so has equation $Y - y = \frac{3x^2}{2y}(X - x)$. This tangent line L intersects C where

$$\left(y + \frac{3x^2}{2y}(X - x) \right)^2 - X^3 = c,$$

which is a cubic in X. By expansion, one gets

$$X^3 - \frac{9x^4}{4y^2}X^2 + \text{lower terms} = 0.$$

This has x as a double root and the sum of the roots equals $\frac{9x^4}{4y^2}$. So the third root is given by

$$\frac{9x^4}{4y^2} - 2x = \frac{9x^4 - 8xy^2}{4y^2} = \frac{x^4 + 8x(x^3 - y^2)}{4y^2} = \frac{x^4 - 8cx}{4y^2} = x', \text{ say.}$$

Now $P' = (x',y')$ where $y' = y + \frac{3x^2}{2y}(x' - x)$. Bachet knew this construction in 1621!

Question 1.4.1 For which $c \in \mathbb{Z}$ does equation (1.1) have infinitely many rational solutions?

The answer to that question was provided by the British mathematician Mordell. He prove that this is true for all c except $c = 1,432$ (provided that you have a rational point). We will see later that, using this and a similar construction for combining two points, the set of rational solutions to (1.1) form a group. For example,

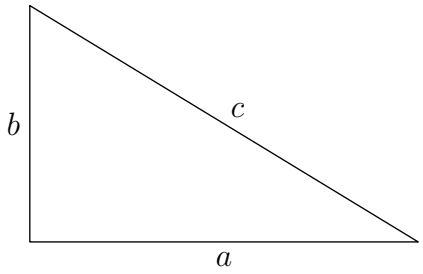
$$c = -2 \rightsquigarrow \text{infinite cyclic group generated by } (3,5) \text{ and } P' = -2P$$
$$c = 1,432 \rightsquigarrow C_6, C_3 \text{ (finite cyclic)}$$
$$c = 1358556 \rightsquigarrow \mathbb{Z}^6 \text{ (Womack 2000)}$$

The record in 2009 was $\mathbb{Z}^{12}$ again by Womack. Now it is $\mathbb{Z}^{15}$ for a massive number c.

R We recall, that for $c = 432$, the Bachet-Mordell equation only has finitely many solutions. Note that if $y^2 = x^3 - 432$ and we write $x = 12\frac{c}{a+b}$ and $y = 36\frac{a-b}{a+b}$, then we get $a^3 + b^3 = c^3$. Conversely, set $a = 36 + y$, $b = 36 - y$ and $c = 6x$. We recover the Fermat Last Theorem for $n = 3$.

1.5 Congruent number curves

Is there a right triangle with rational sides and area 5?



For this, we need: $ab/2 = 5$ and $a^2 + b^2 = c^2$, which implies that

$$ab = 10$$
$$\left(\frac{a+b}{2}\right)^2 = \frac{a^2+2ab+b^2}{4} = \frac{c^2+20}{4} = \left(\frac{c}{2}\right)^2 + 5$$
$$\left(\frac{a-b}{2}\right)^2 = \frac{a^2-2ab+b^2}{4} = \frac{c^2-20}{4} = \left(\frac{c}{2}\right)^2 - 5.$$

Let $x = \left(\frac{c}{2}\right)^2 \in \mathbb{Q}$. Then $x-5$, x and $x+5$ are three squares in arithmetic progression and $(x-5)x(x+5) = y^2$ with $y \in \mathbb{Q}$. So (x,y) is a rational point on the curve

$$E_5 : y^2 = x^3 - 25x.$$

Definition 1.7 We say that n is a congruent number if the right triangle problem has a solution.

More generally, for $n \in \mathbb{N}$, let $E_n : y^2 = x^3 - n^2x$. If n is a congruent number then there exists $P = (x,y) \in E_n(\mathbb{Q})$ such that $x = (\frac{c}{2})^2$ and $y \neq 0$. Conversely, if $P = (x,y) \in E_n(\mathbb{Q})$, such that $y \neq 0$, we will later see that the x-coordinate of $2P$ is a square. The curve E_n is called the congruent number curve for n.

Example 1.5.0.1 Let $E_5 : y^2 = x^3 - 25x$. The group of solutions is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ generated by $(0,0)$, $(5,0)$ and $(-4,6)$. Take $P = (-4,6)$, then

$$2P = \left(\left(\frac{41}{12} \right)^2, \frac{-62279}{1728} \right).$$

Let $x = (\frac{41}{12})^2$, then $x - 5 = (\frac{49}{12})^2$ and $x + 5 = (\frac{31}{12})^2$. Thus

$$c = \frac{41}{6},\ a + b = \frac{49}{6},\ a - b = \frac{31}{6},$$

which gives $a = \frac{20}{3}$ and $b = \frac{3}{2}$.

Fact: n is a congruent number if and only if E_n has a rational point $P = (x,y)$ with $y \neq 0$, and this is equivalent to saying that E_n has infinitely many rational points. The Birch and Swinnerton-Dyer conjecture (BSD) gives a criterion for this to happen. The following result was proved by Tunnell in the 80s.

Theorem 1.5.1 — Tunnell. Let n be an odd integer. Then if n is a congruent number then

$$\#\left\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = n, z \text{even}\right\} = \#\left\{(x,y,z) \in \mathbb{Z}^3 : 2x^2 + y^2 + 8z^2 = n, z \text{odd}\right\}$$

The converse is a consequence of BSD.

1.6 A brief review on fields

Definition 1.8 Let K be a field, and K' a field containing K. We say that an element $\alpha \in K'$ is **algebraic** over K if it satisfies a polynomial with coefficients in K. We say that K' is **algebraic** over K if every element in K' is algebraic over K.

Example 1.6.0.1 (a) Every element $a \in K$ is algebraic over K since it satisfies the polynomial $x - a$. In particular K is algebraic over itself.

(b) Let $K = \mathbb{Q}$ and $D \in \mathbb{Q}$ **not** a square, and define

$$\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} : a, b \in \mathbb{Q}\}.$$

Then $\mathbb{Q}(\sqrt{D})$ is algebraic over $\mathbb{Q}$. Indeed, let $\alpha = a + b\sqrt{D}$ and recall that the conjugate of α is $\bar{\alpha} = a - b\sqrt{D}$. We define

- the *trace* of α to be $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha} = 2a$.
- the *norm* of α to be $\mathrm{N}(\alpha) = \alpha\bar{\alpha} = a^2 - Db^2$.

It is not hard to see that α satisfies the polynomial $x^2 - \mathrm{Tr}(\alpha)x + \mathrm{N}(\alpha)$, so it is algebraic over $\mathbb{Q}$. Hence $\mathbb{Q}(\sqrt{D})$ is algebraic over $\mathbb{Q}$.

(c) Let $n \geq 1$ be an integer, and K' the subset of $\mathbb{C}$ defined by

$$K' := \mathbb{Q}(\zeta_n) := \left\{a_0 + a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1} : a_0, \ldots, a_{n-1} \in \mathbb{Q}\right\},$$

where $\zeta_n = e^{\frac{2\pi\sqrt{-1}}{n}}$. Then K' is a subfield of $\mathbb{C}$ which is algebraic over $\mathbb{Q}$. In particular, we have $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ where $\zeta_3 = \frac{1+\sqrt{-3}}{2}$, and $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ where $i^2 = -1$.

Definition 1.9 Let K be a field. We say that K is **algebraically closed** if every polynomial polynomial with coefficients in K has a root in K.

Let K be a field, and $\overline{K}$ a field which contains K. We say that $\overline{K}$ is an **algebraic closure** of K if $\overline{K}$ is algebraic over K and is algebraically closed.

Example 1.6.0.2 The field $\mathbb{R}$ is not algebraically closed since the polynomial x^2+1 does not have a root in it. However, the field $\mathbb{C}$ is algebraically closed (by the Fundamental Theorem of Algebra), and is an algebraic closure of $\mathbb{R}$.

Theorem 1.6.1 Every field K admits an algebraic closure $\overline{K}$ which is unique up to isomorphism.

Example 1.6.1.1 (a) By Theorem 1.6.1, every algebraic closure of $\mathbb{R}$ is isomorphic to $\mathbb{C}$.

(b) Let $\overline{\mathbb{Q}}$ be the subset of $\mathbb{C}$ given by

$$\overline{\mathbb{Q}} := \{x \in \mathbb{C} : x \text{is algebraic over} \mathbb{Q}\}.$$

It can be shown that $\overline{\mathbb{Q}}$ is the unique algebraic closure of $\mathbb{Q}$ contained in $\mathbb{C}$. Note that since every $x \in \overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$, it is enough to show that it is a subfield of $\mathbb{C}$, *i.e.*, it is closed under addition and multiplication.

Example 1.6.1.2 Let p be a prime number. The integers modulo p form a field $\mathbb{F}_p$ with p elements. By Theorem 1.6.1, $\mathbb{F}_p$ admits an algebraic closure $\overline{\mathbb{F}}_p$. Suppose that we fix an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. One can show the following propositions:

- The cardinality of every finite subfield of $\overline{\mathbb{F}}_p$ is of the form $q = p^n$, with $n \geq 1$.
- For every prime power $q = p^n$, there is a unique subfield $\mathbb{F}_q$ of $\overline{\mathbb{F}}_p$ of cardinality q. In fact, one can show that
$$\mathbb{F}_q = \left\{x \in \overline{\mathbb{F}}_p : x^q = x\right\}.$$

Weierstrass equations and elliptic curves

Discriminant

Bezout's theorem

Definition of the group law
Associativity of the group law
Computing with the group law

Singular curves

2. Elliptic curves and group law

In this chapter, we introduce the notion of elliptic curves. We will define the group law using the *chord and tangent process*, which dates back the ancient Greeks.

2.1 Weierstrass equations and elliptic curves

Let K be a field.

Definition 2.1 An **elliptic curve** E defined over K is a smooth plane cubic curve given by a **long Weierstrass equation**:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{2.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$.

The homogenization of the curve E in (2.1) is given by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{2.2}$$

The *only* point at infinity on this curve is $[0:1:0]$, we denote this point by ∞ from now on. We will see that this point is the *neutral* element in the group structure on E.

Example 2.1.0.3

- We already saw few examples of elliptic curves in the introduction:
  (a) The Bachet-Mordell equation $E : y^2 = x^3 + c$, where $c \in \mathbb{Z}$ is non-zero, is an elliptic curve.
  (b) The congruent number curve $E_n : y^2 = x^3 - n^2x$, with $n \in \mathbb{N}$, is an elliptic curve curve.
  (c) $y^2 = x^3 + x$ is an elliptic curve, etc.
- The curve $E : y^2 + y = x^3 - x$ is an elliptic curve over $\mathbb{Q}$. Indeed, let $P = (x,y)$ be a point on E. Then E is singular at P if and only if $2y+1 = 0$ and $3x^2 - 1 = 0$. So we must have $P = (-1/\sqrt{3}, -1/2)$ or $(1/\sqrt{3}, -1/2)$, which is impossible since none of these point lies on E. Hence E is non-singular.

In practice, it is often desirable to simplify Equation (2.1). This is possible provided that $\mathrm{char}(K) \neq 2,3$. Indeed, when $\mathrm{char}(K) \neq 2$, we can complete the square in (2.1). This amounts to making the change of coordinates

$$\begin{cases} x' = x \\ y' = y + \frac{1}{2}(a_1 x + a_3). \end{cases}$$

to obtain a curve with a **medium Weierstrass equation**

$$y^2 = x^3 + a_2' x^2 + a_4' x + a_6'. \tag{2.3}$$

If in addition $\mathrm{char}(K) \neq 3$, we can make one further change of coordinates

$$\begin{cases} x' = x + \frac{1}{3}a_2' \\ y' = y \end{cases}$$

to get a **short Weierstrass equation**

$$y^2 = x^3 + a_4'' x + a_6''. \tag{2.4}$$

R We will mostly work with short or medium Weierstrass equations.

We now give a criterion for a short Weierstrass cubic curve E to be an elliptic curve.

2.2 Discriminant

Definition 2.2 Let $f(x) = a_0 + a_1 x + \ldots + a_m x^m$, $g(x) = b_0 + b_1 x + \ldots + b_n x^n \in K[x]$ be polynomials of degree m and n respectively. The resultant of f and g, denoted by $R(f,g)$ is the determinant of the $(m+n) \times (m+n)$ matrix

$$\begin{bmatrix} a_0 & a_1 & \cdots & a_{m-1} & a_m & 0 & 0 & & \cdots & 0 \\ 0 & a_0 & \cdots & a_{m-2} & a_{m-1} & a_m & 0 & & \cdots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & \cdots & & & & a_0 & & & \cdots & a_m \\ b_0 & b_1 & & & & b_{n-1} & b_n & 0 & \cdots & 0 \\ 0 & b_0 & & & & b_{n-2} & b_{n-1} & b_n & \ldots & 0 \\ \vdots & & & & & & & & & \vdots \\ 0 & \cdots & & b_0 & b_1 & & & \cdots & & b_n \end{bmatrix}$$

Example 2.2.0.4 The resultant of the polynomials $f(x) = x^2 + 1$ and $g(x) = x^3 - x + 1$ is

$$R(f,g) = \begin{vmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & -1 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 1 \end{vmatrix} = 5.$$

Lemma 2.2.1 Let $f,g \in K[x]$ be two polynomials of degree m and n respectively. Then f and g have a common factor which is non-constant if and only if there exist non zero polynomials $\phi,\psi \in K[x]$ such that $\deg\phi < m$, $\deg\psi < n$ and $\psi f = \phi g$.

Proof. ($\Rightarrow$) If f and g have a common factor h which is non constant, then $f = \phi h$ and $g = \psi h$; so $\psi f = \phi g$.
($\Leftarrow$) Suppose that $\psi f = \phi g$; then every irreducible factor of g divides either f or ψ. However, since $\deg\psi < n$, one of those irreducible factors must divide f. ■

Theorem 2.2.2 Let $f,g \in K[x]$ be two polynomials of degree m and n respectively, given by

$$f(x) = \sum_{i=0}^{m} a_i x^i,\ g(x) = \sum_{j=0}^{n} b_j x^j.$$

Then f and g have a common factor which is non-constant if and only if $R(f,g) = 0$.

Let $F,G \in K[X,Y,Z]$ be two homogeneous polynomials of degree m and n respectively. We can view them as being polynomials in Z, and write them as:

$$F(X,Y,Z) = A_0 Z^m + A_1 Z^{m-1} + \cdots + A_m$$
$$G(X,Y,Z) = B_0 Z^n + B_1 Z^{n-1} + \cdots + B_n,$$

where $A_i, B_j \in K[X,Y]$ are homogeneous of degree i and j respectively. Similarly to Definition 2.2, we define the resultant of F and G with respect to Z. This is either a polynomial $R_{F,G}(X,Y) \in K[X,Y]$ or 0 by definition. Moreover, if it is different from 0, this polynomial is homogeneous of degree less or equal to mn. If $F(0,0,1)\cdot G(0,0,1) \neq 0$ then $R_{F,G}(X,Y)$, the resultant of F and G with respect to Z, is homogeneous of degree mn (similarly for $R_{F,G}(X,Z)$ and $R_{F,G}(Y,Z)$).
An analogous of Theorem 2.2.2 holds, namely:

Theorem 2.2.3 Let K be an infinite field, and $F,G \in K[X,Y,Z]$ be two homogeneous polynomials of degree m and n respectively. Then the resultant $R_{F,G}(X,Y)$ of F and G with respect to Z is either 0 or a homogeneous polynomial of degree less or equal to mn, and if $F(0,0,1)\cdot G(0,0,1) \neq 0$ then $\deg(R(X,Y)) = mn$ (similarly for $R_{F,G}(X,Z)$ and $R_{F,G}(Y,Z)$). The polynomials F and G have a common factor if and only if at least one between $R_{F,G}(X,Y)$, $R_{F,G}(X,Z)$ and $R_{F,G}(Y,Z)$ is equal to 0.

Example 2.2.3.1 The resultant of the polynomials $F(X,Y,Z) = X^2+Y^2-Z^2$ and $G(X,Y,Z) = Y^2Z - X^3 + XZ^2$ with respect to Z is

$$R(X,Y) = \begin{vmatrix} X^2+Y^2 & 0 & -1 & 0 \\ 0 & X^2+Y^2 & 0 & -1 \\ -X^3 & Y^2 & X & 0 \\ 0 & -X^3 & Y^2 & X \end{vmatrix} = -Y^6.$$

The resultant with respect to X is

$$R(Y,Z) = \begin{vmatrix} Y^2-Z^2 & 0 & 1 & 0 & 0 \\ 0 & Y^2-Z^2 & 0 & 1 & 0 \\ 0 & 0 & Y^2-Z^2 & 0 & 1 \\ Y^2Z & Z^2 & 0 & -1 & 0 \\ 0 & Y^2Z & Z^2 & 0 & -1 \end{vmatrix} = Y^6 - 2Z^6 - 4Y^4Z^2 + 5Y^2Z^4.$$

Example 2.2.3.2 The resultant of the polynomials $F(X,Y,Z) = XY + XZ$ and $G(X,Y,Z) = XY + YZ$ with respect to Z is

$$R(X,Y) = \begin{vmatrix} XY & X \\ XY & Y \end{vmatrix} = XY^2 - X^2Y.$$

In this example $F(0,0,1) = G(0,0,1) = 0$, and $deg(R(X,Y)) = 3 < deg(F)deg(G) = 4$.

Definition 2.3 Let f be a polynomial of degree n in $K[x]$, with leading coefficient a_n. The **discriminant** of f is defined by

$$\Delta_f = (-1)^{n(n-1)/2} a_n^{-1} R(f, f'),$$

where $R(f,f')$ is the resultant of f and its derivative f'.

Lemma 2.2.4 Let f be a polynomial of degree n in $K[x]$, with leading coefficient a_n, and write

$$f(x) = a_n \prod_{i=1}^{n} (x - e_i), \text{ with } e_i \in \overline{K}.$$

Then, we have

$$\Delta_f = a_n^{2n-2} \prod_{1 \le i < j \le n} (e_i - e_j)^2.$$

Proof. Straightforward computation. ■

In particular, we have the following result for cubic polynomials:

Lemma 2.2.5 Let $f(x) = x^3 + ax^2 + bx + c$ with $a,b,c \in K$. Then the discriminant of f is given by

$$\Delta_f = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = [(e_1 - e_2)(e_2 - e_3)(e_1 - e_3)]^2,$$

where e_1, e_2, e_3 are the roots of f.

Proof. By definition, we have

$$\Delta_f = -\begin{vmatrix} c & b & a & 1 & 0 \\ 0 & c & b & a & 1 \\ b & 2a & 3 & 0 & 0 \\ 0 & b & 2a & 3 & 0 \\ 0 & 0 & b & 2a & 3 \end{vmatrix} = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

■

Definition 2.4 Let $E : y^2 = f(x)$ be a Weierstrass cubic, where $f(x) = x^3 + ax^2 + bx + c$. Then, the **discriminant** Δ_E of E is Δ_f.

We are ready to state a simply criterion for a medium Weierstrass cubic to be non-singular.

Proposition 2.2.6 Let E be a curve given by a medium Weierstrass equation $y^2 = f(x)$, with $f(x) = x^3 + ax^2 + bx + c$ and $a, b, c \in K$. Then E is an elliptic curve if and only if $\Delta_E \neq 0$.

Proof. For simplicity, we assume that $\mathrm{char}(K) \neq 2$. Let $g(x,y) = y^2 - f(x)$, and $P = (x,y)$ be a point in $E(\overline{K})$. Then, by definition

$$E \text{ is singular at } P \iff \begin{cases} \frac{\partial g}{\partial x} = -f'(x) = 0 \\ \\ \frac{\partial g}{\partial y} = 2y = 0 \end{cases} \iff f(x) = f'(x) = 0.$$

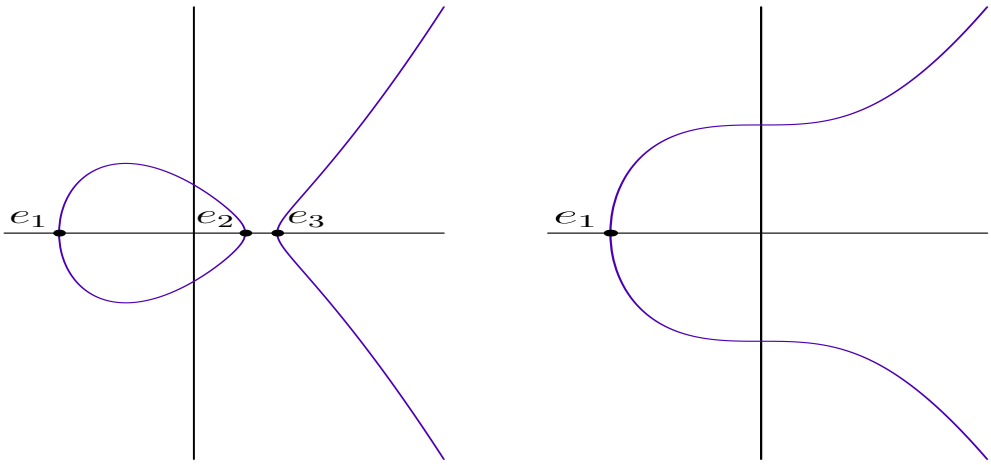
$$\iff f \text{ has a double root} \iff \Delta_E = -R(f, f') = 0,$$

where the last deduction follows from Theorem 2.2.2. ∎

Corollary 2.2.7 A short Weierstrass cubic curve $E : y^2 = x^3 + ax + b$, where $a, b \in K$, is an elliptic curve if and only if (its discriminant) $\Delta_E = -4a^3 - 27b^2 \neq 0$.

Let $E : y^2 = f(x)$ be a medium Weierstrass cubic, and e_1, e_2, e_3 the roots of $f(x)$. By Lemma 2.2.5 and Proposition 2.2.6, E is smooth if and only if $\Delta_E \neq 0$, or equivalently, if and only if e_1, e_2, e_3 are distinct. In other words, E is an elliptic curve if and only if $f(x)$ has **no** repeated root.

Let us assume $K \subseteq \mathbb{R}$, then we can consider the $\mathbb{R}$ points of E. If $\Delta_E > 0$ then $f(x)$ has 3 real roots and the graph of $E(\mathbb{R})$ has two components. Meanwhile, if If $\Delta_E < 0$ then $f(x)$ has 1 real roots and the graph of $E(\mathbb{R})$ has only one component. See Figures 2.1(b) and 2.1(a) for illustrations of the set $E(\mathbb{R})$.



(a) $\Delta > 0 \Leftrightarrow e_1, e_2, e_3 \in \mathbb{R}$. (b) $\Delta < 0 \Leftrightarrow e_1$ is real, $e_2 = \bar{e}_3 \notin \mathbb{R}$.

Figure 2.1: $E(\mathbb{R})$

2.3 Bezout's theorem

Let $C : f(x,y) = 0$ be a plane curve, where $f \in K[x,y]$ is a polynomial of degree m. Let $C' : y = h(x)$ be another plane curve, where $h \in K[x]$ is a polynomial of degree n (in one variable). To find the intersection of C and C', we substitute $h(x)$ for y, and solve the equation $f(x,h(x)) = 0$. However, the curve C' cannot always be given in this form. The notion of resultant, introduced in the previous section, allows one to determine all intersection points even when the polynomial defining the curves are not polynomials in one variable: we will see this procedure at the end of this section.
Note that we cannot always expect to obtain all the intersection points unless K is an algebraically closed field.

Theorem 2.3.1 — Weak Bezout Theorem. Let K be an infinite field. Let $F, G \in K[X,Y,Z]$ be two homogeneous polynomials of degree m and n respectively, **without** a common irreducible factor, and let

$$\mathscr{C}_F(K) = \{[x:y:z] \in \mathbf{P}^2(K) : F(x,y,z) = 0\}, \qquad \mathscr{C}_G(K) = \{[x:y:z] \in \mathbf{P}^2(K) : G(x,y,z) = 0\}.$$

Then the set $\mathscr{C}_F(K) \cap \mathscr{C}_G(K)$ is **finite**, and contains at most mn points.

Proof. Let $P_i = [x_i : y_i : z_i] \in \mathscr{C}_F(K) \cap \mathscr{C}_G(K)$ for $1 \leq i \leq k$ be distinct points. Consider all the lines through the pairs (P_i, P_j), with $1 \leq i < j \leq k$. Since K is infinite, we can find a point P_0 which doesn't belong to any of these lines. Furthermore, by a change of coordinates, we can assume that $P_0 = [0:0:1]$. The fact that the points P_0, P_i, P_j are not co-linear for $1 \leq i < j \leq k$, implies that the points $[x_i : y_i]$ and $[x_j : y_j]$ are distinct in $\mathbf{P}^1(K)$.
Now consider the polynomials $f_i(Z) = F(x_i, y_i, Z)$ and $g_i = G(x_i, y_i, Z)$. Since P_i belongs to $\mathscr{C}_F(K) \cap \mathscr{C}_G(K)$, we have $f_i(z_i) = g_i(z_i) = 0$. Therefore, by Theorem 2.2.2, $f_i(Z)$ and $g_i(Z)$ have a common factor, which is non-constant. This means that $R_{F,G}(X,Y)$ must vanish at $[x_i : y_i]$, i.e. at P_i. Since, this is a homogeneous polynomial of degree at most mn, we must have $k \leq mn$. ■

Let $P_i = [x_i : y_i : z_i] \in \mathscr{C}_F(K) \cap \mathscr{C}_G(K)$, for $1 \leq i \leq k$, then $R_{F,G}(X,Y)$ vanishes at all $[x_i : y_i]$. If K is algebraically closed, this means that

$$R_{F,G}(X,Y) = \prod_{i=1}^{k} (y_i X - x_i Y)^{m_i}.$$

Note that there is a bijection between the points P_i and and the linear factors of $R_{F,G}(X,Y)$. We define the **multiplicity** of P_i to be m_i. Analogously, the multiplicity $I(P; \mathscr{C}_F(K), \mathscr{C}_G(K))$ of $P \in \mathscr{C}_F(K) \cap \mathscr{C}_G(K)$ is that of the corresponding linear factor in $R_{F,G}(X,Y)$. This gives immediately the following theorem.

Theorem 2.3.2 — Strong Bezout Theorem. Let K be an algebraically closed field. Let $F, G \in K[X,Y,Z]$ be two homogeneous polynomials of degree m and n respectively, **without** a common irreducible factor, and let

$$\mathscr{C}_F(K) = \{[x:y:z] \in \mathbf{P}^2(K) : F(x,y,z) = 0\}, \qquad \mathscr{C}_G(K) = \{[x:y:z] \in \mathbf{P}^2(K) : G(x,y,z) = 0\}.$$

Then the set $\mathscr{C}_F \cap \mathscr{C}_G$ is **finite**, and we have

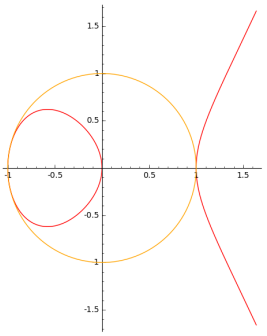
$$\sum_{P \in \mathscr{C}_F \cap \mathscr{C}_G} I(P; \mathscr{C}_F, \mathscr{C}_G) = mn.$$

Corollary 2.3.3 Let K be an algebraically closed field, and $F \in K[X,Y,Z]$ an homogeneous polynomial of degree d. Let $\mathscr{C} : F(X,Y,Z) = 0$ be a projective curve of degree d, and L a line not contained in $\mathscr{C}$. Then $L \cap \mathscr{C}$ has exactly d points counted with multiplicity.

R The definition of the multiplicity $I(P;\mathscr{C}_F,\mathscr{C}_G)$ given above clearly depends on the choice of coordinates. One can show that this is in fact not the case.

Example 2.3.3.1

Find the intersection of the curves $\mathscr{C} : X^2+Y^2-Z^2=0$ and $\mathscr{C}' : Y^2Z - X^3 + XZ^2 = 0$ over $K = \overline{K}$ with $\mathrm{char}(K) \neq 2$. We already compute the resultant of the defining polynomials in Example 2.2.3.1: $R(X,Y) = -Y^6$. So $R(X,Y) = 0$ if and only if $Y = 0$. Substituting this in our equations leads to $X^2 - Z^2 = (X+Z)(X-Z) = 0$ and $-X^3 + XZ^2 = X(Z-X)(Z+X) = 0$. Since $[X:Y:Z]$ must be a point in $\mathbf{P}^2(K)$, we must have $X \neq 0$. This gives $X = \pm Z \neq 0$, and we get the points $P = [1:0:1]$ and $Q = [-1:0:1]$.



To compute the multiplicities of these points, we observe that one cannot apply Theorem 2.3.2 directly, since $P_0 = [0:0:1]$, as in the proof of Theorem 2.3.1, belongs to the line joining P and Q. To remedy this, we make the change of coordinates $X = U - W$, $Y = V - W$ and $Z = W$. Then, P and Q become $P' = [2:1:1]$ and $Q' = [0:1:1]$, and the equations of the curves are

$$U^2 - 2UW + V^2 - 2VW + W^2 = 0$$
$$-U^3 + 3U^2W - 2UW^2 + V^2W - 2VW^2 + W^3 = 0$$

This yields the resultant

$$R(U,V) = U^6 - 4U^5V + 4U^4V^2 = U^4(U-2V)^2.$$

From this, we deduce that the multiplicities of P' and Q', and hence those of P and Q, are 2 and 4 respectively.

Alternatively, we can work in the affine plane since the curves do not intersect at infinity. The dehomogenized curves with respect to z are given by $C : f(x,y) = x^2+y^2-1 = 0$ and $C' : g(x,y) = y^2 - x^3 + x = 0$. The resultant of $f(x,y)$ and $g(x,y)$ with respect to y is

$$R_{f,g}(x) = \begin{vmatrix} x^2-1 & 0 & 1 & 0 \\ 0 & x^2-1 & 0 & 1 \\ -x^3+x & 0 & 1 & 0 \\ 0 & -x^3+x & 0 & 1 \end{vmatrix} = x^6 + 2x^5 - x^4 - 4x^3 - x^2 + 2x + 1 = (x-1)^2(x+1)^4.$$

The projections of P and Q to the affine plane are $(1,0)$ and $(-1,0)$ respectively, which have multiplicities 2 and 4. Thus the multiplicities of P and Q are 2 and 4 respectively.

2.4 Definition of the group law

We will now proceed to define the group structure on E. To this end, we first recall the following definition:

Definition 2.5 Let E be an elliptic curve over K given by a Weierstrass equation (2.1). Let K' be a field containing K. The set of K'-rational points of E is defined by

$$E(K') := \left\{[x:y:z] \in \mathbf{P}^2(K') : zy^2 + a_1xyz + a_3xz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3\right\}.$$

In other words, it is the set of K'-rational points on the homogenization of E.

Since $\mathbf{P}^2(K') = \mathbf{A}^2(K') \sqcup \{Z = 0\}$, and $[0:1:0]$ is the only point at ∞ on E, we can write

$$E(K') := \left\{(x,y) \in K'^2 : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6\right\} \sqcup \{\infty\}.$$

Example 2.4.0.2 Let $K = \mathbb{Q}$, and $E : y^2 = x^3 - 2$. The set of $\mathbb{Q}$-rational points $E(\mathbb{Q})$ contains $P = (3,5)$. We have the natural inclusions

$$E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C}).$$

To define the group structure, we need to work with the $\overline{K}$-rational points, *i.e.*, the set

$$E(\overline{K}) = \{(x,y) \in \overline{K}^2 : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6\} \sqcup \{\infty\}.$$

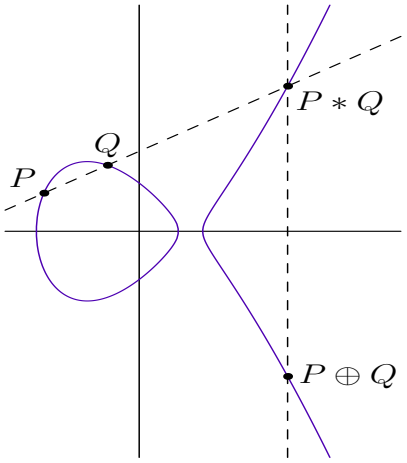
Recall that, if L be a line in $\mathbf{P}^2(\overline{K})$, then Bezout's Theorem implies that $L \cap E$ has *three* points P, Q and R counted with multiplicity. For $P, Q \in E(\overline{K})$, we denote the third point of intersection of the line through P and Q with E by $P * Q$.

We are now ready to define the group structure on $E(\overline{K})$.

Definition 2.6 The addition law $\oplus$ on $E(\overline{K})$ is defined as follows: for $P, Q \in E(\overline{K})$ set

$$P \oplus Q := (P * Q) * \infty.$$

In words, to obtain the sum $P \oplus Q$, we first draw the line L through P and Q (if $P \neq Q$) or the tangent line (if $P = Q$), and let $P * Q$ be its third intersection point with $E(\overline{K})$. Then, we draw the line through $P * Q$ and ∞, and let $P \oplus Q$ be its third intersection point with $E(\overline{K})$.



Theorem 2.4.1 Let E be an elliptic curve defined over a field K. Then, $E(\overline{K})$ is an abelian group under the operation $\oplus$, with identity element $\infty (= [0:1:0])$. In other words, we have

(i) $P \oplus Q = Q \oplus P \ \forall P, Q \in E(\overline{K})$ (commutativity);

(ii) $P \oplus \infty = P \ \forall P \in E(\overline{K})$ (i.e., ∞ is the identity element);

(iii) Let $P' = P * \infty$. Then $P \oplus P' = \infty$ (i.e., the opposite of P is $\ominus P = P * \infty$);

(iv) $P \oplus (Q \oplus R) = (P \oplus Q) \oplus R, \ \forall P, Q, R \in E(\overline{K})$ (associativity).

Proof. The first statement is an immediate consequence of the definition. Indeed, the third point of intersection of the line through P and Q is $R = P * Q = Q * P$, and the line through R and ∞ intersects E at $P \oplus Q = Q \oplus P$.

To prove (ii) and (iii), let $P \in E(\overline{K})$. If $P = \infty$ then, the (tangent) line at infinity $Z = 0$ intersects E at ∞ three times by Bezout's Theorem; so

$$\infty = \infty * \infty = \infty \oplus \infty.$$

Otherwise, the line through P and ∞ is a *vertical* line, whose third point of intersection with $E(\overline{K})$ is $P' = P * \infty$. Then, by definition, we have $P * P' = \infty$; so

$$\begin{aligned} P \oplus P' &= (P * P') * \infty = \infty * \infty = \infty, \text{ and} \\ P \oplus \infty &= (P * \infty) * \infty = P' * \infty = P. \end{aligned}$$

The last statement (iv) is harder and we will come back to it later, after some preliminaries. ■

2.4.1 Associativity of the group law

We now turn to the proof of associativity of the group law which is a consequence of Bezout's Theorem. We start with some lemmas on the intersection of conic and cubic curves.

Lemma 2.4.2 Let $P_1, \ldots, P_5$ be 5 distinct points in $\mathbf{P}^2(\overline{K})$. Then there is one conic $\mathscr{C}$ passing through them. The conic $\mathscr{C}$ is unique if no 4 of these points are on the same line.

Proof. Let $\mathscr{V}$ be the set of all homogeneous polynomials in $K[X,Y,Z]$ of degree 2. Then every element of $\mathscr{V}$ is of the form

$$F(X,Y,Z) = v_0X^2 + v_1XY + v_2XZ + v_3Y^2 + v_4YZ + v_5Z^2,$$

where $v_0, \ldots, v_5 \in \overline{K}$. This is a vector space since

$$\begin{aligned} &\lambda \in \overline{K}, F \in \mathscr{V} \Rightarrow \lambda F \in \mathscr{V}, \\ &F_1, F_2 \in \mathscr{V} \Rightarrow F_1 + F_2 \in \mathscr{V}. \end{aligned}$$

The dimension of $\mathscr{V}$ is 6.
Let $\mathscr{C}$ be a conic in $\mathbf{P}^2(\overline{K})$. Then, by definition, $\mathscr{C}$ is given by an element $F \in \mathscr{V}$. Note that $\mathscr{C}$ is also the zero locus of λF for all $\lambda \in \overline{K}^\times$. Let $\mathscr{W}$ be the subset of $\mathscr{V}$ consisting of the polynomials corresponding to all conics passing through $P_1, \ldots, P_5$. The conic $\mathscr{C}$ passes through the point $P = [x : y : z]$ if and only if

$$F(x,y,z) = v_0x^2 + v_1xy + v_2xz + v_3y^2 + v_4yz + v_5z^2 = 0.$$

This is linear equation in $(v_0, \ldots, v_5)$. Therefore, the elements in $\mathscr{W}$ are the solutions to a homogeneous linear system of 5 equations in 6 variables. Hence, it is a vector subspace of dimension at least 1. This means that, there is at least *one* conic passing through $P_1, \ldots, P_5$.
We are now going to show that, if no 4 of the points $P_1, \ldots, P_5$ are on the same line, then $\dim \mathscr{W} = 1$. Assume that $\dim \mathscr{W} > 1$. Then, there are two polynomials F_1, F_2, which are linear independent, such that the conics

$$\mathscr{C}_i(\overline{K}) = \mathscr{C}_i := \left\{ [x : y : z] \in \mathbf{P}^2(\overline{K}) : F_i(x,y,z) = 0 \right\}, \; i = 1,2,$$

go through $P_1, \ldots, P_5$. So $\#\mathscr{C}_1 \cap \mathscr{C}_2 \geq 5 > 4$. So by Theorem 2.3.2, F_1 and F_2 have a common factor which is non-constant. Since they are linearly independent (of degree 2 each), this common factor must be a linear factor. In other words, $\mathscr{C}_1 \cap \mathscr{C}_2$ contains a line, which contradicts our assumption on the points $P_1, \ldots, P_5$. So $\dim \mathscr{W} = 1$ as required. ■

Lemma 2.4.3 Let $P_1,\dots,P_8 \in \mathbf{P}^2(\overline{K})$ be distinct. Suppose that no 4 of them are co-linear; and no 7 of them lie on the same conic. Then, the subspace of homogeneous cubic polynomials which vanish at $P_1,\dots,P_8$ has dimension 2.

Proof. Let $\mathscr{V}$ be the space of all homogeneous polynomials of degree 3 in $\overline{K}[X,Y,Z]$. Then, every element $F \in \mathscr{V}$ is of the form

$$F = v_0X^3 + v_1X^2Y + v_2XY^2 + v_3Y^3 + v_4X^2Z + v_5XZ^2 + v_6Z^3 + v_7Y^2Z + v_8YZ^2 + v_9XYZ,$$

where $(v_0,\dots,v_9) \in \overline{K}^{10}$. As in the proof of Lemma 2.4.2, we see that $\dim \mathscr{V} = 10$.
Now, let $P = [x : y : z] \in \mathbf{P}^2(\overline{K})$, then F vanishes at $P \iff (v_0,\dots,v_9)$ satisfies the linear equation

$$F(x,y,z) = v_0x^3 + v_1x^2y + v_2xy^2 + v_3y^3 + v_4x^2z + v_5xz^2 + v_6z^3 + v_7y^2z + v_8yz^2 + v_9xyz = 0.$$

So the set of all $F \in \mathscr{V}$ passing through $P_1,\dots,P_8$ is the solution space to a homogeneous system of 8 equations in 10 variables. So it is a vector subspace, which we call $\mathscr{W}$. We see that $\dim \mathscr{W} \geq 10-8 = 2$. We will now show that $\dim \mathscr{W} = 2$.

Case 1. Assume that three of the points, say P_1,P_2,P_3, are on the same line with equation $L = 0$. We choose P_9 on the same line. Every $F \in \mathscr{V}$ which vanishes at $P_1,\dots,P_9$ is of the form $F = LQ$, where Q defines a conic passing through $P_4,\dots,P_8$. Since no 4 of the $P_4,\dots,P_8$ belong to the same line, Lemma 2.4.2 implies that the space of homogeneous polynomials of degree 2 which vanish on those five points in 1-dimensional. So, there is a conic $Q_0 = 0$ such that F is a multiple of LQ_0. So the dimension of such cubics is $d_0 = 1$, and hence $\dim \mathscr{W} \leq d_0 + 1 = 2$.

Case 2. Suppose that six of the points, say $P_1,\dots,P_6$, are on the same conic $Q = 0$. We choose P_9 on $Q = 0$. Every cubic which vanishes at $P_1,\dots,P_9$ is of the form $F = LQ$, where $L = 0$ is the equation of the line through P_7 and P_8. As before, the space of such cubics is 1-dimensional, and $\dim \mathscr{W} \leq 1+1 = 2$.

Case 3. Suppose no 3 of the $P_1,\dots,P_8$ are co-linear, and no 6 of them are on same conic. We choose two extra points P_9,P_{10} on the line joining P_1 and P_2, with equation $L = 0$. If $\dim \mathscr{W} \geq 3$, there would exist a non-trivial cubic $F = 0$ passing through $P_1,\dots,P_{10}$. In that case, we would have $F = LQ$, where $Q = 0$ is the conic passing through $P_3,\dots,P_8$. But this contradicts our assumption. So $2 \leq \dim \mathscr{W} < 3$, and this concludes the proof the lemma. ■

Lemma 2.4.4 Let C_1 and C_2 be two cubics, one of which is **irreducible**. Let $P_1,\dots P_9$ be the points of intersection of C_1 and C_2. Let C be another cubic which passes through $P_1,\dots,P_8$. Then C also passes through P_9.

Proof. We keep the notations of the previous lemma; and let F_1, F_2 and F be the defining polynomials for C_1, C_2 and C respectively. Suppose that C_1 is irreducible, then it doesn't contain a line or a conic. This means that no 4 of the $P_1,\dots,P_8$ are on the same line, and no 7 of them are on the same conic. So, by Lemma 2.4.3, the set of such cubics corresponds to a 2-dimensional subspace $\mathscr{W}$ of $\mathscr{V}$ generated by F_1 and F_2. Therefore, we can write $F = \lambda_1F_1 + \lambda_2F_2$, with $\lambda_1,\lambda_2 \in \overline{K}^\times$. So, we must have

$$F(P_9) = \lambda_1F_1(P_9) + \lambda_2F_2(P_9) = 0.$$

Hence C passes through P_9. ■

R A curve is irreducible if the corresponding polynomial is irreducible, i.e. it cannot be factored. Every elliptic curve is irreducible: it does not contain any line or conics. Indeed, every elliptic curve is a smooth curve which satisfies a Weierstrass equation. This equation is a polynomial equation in two variables, which is irreducible (this follows because the curve is smooth).

Proof of associativity, sketch. (iv) To show $P\oplus(Q\oplus R)=(P\oplus Q)\oplus R$ it is enough to show that $P*(Q\oplus R)=(P\oplus Q)*R$, since the reflexion of the two points with respect to the x-axis will be the same. To this end, define six lines L_1,L_2,L_3,M_1,M_2,M_3 by their intersection with E:

- $L_1\cap E : P,Q,P*Q$
- $L_2\cap E : Q*R,Q\oplus R,\infty$
- $L_3\cap E : P\oplus Q,R,(P\oplus Q)*R$
- $M_1\cap E : P*Q,\infty,P\oplus Q$
- $M_2\cap E : Q,R,Q*R$
- $M_3\cap E : Q\oplus R,P,P*(Q\oplus R)$

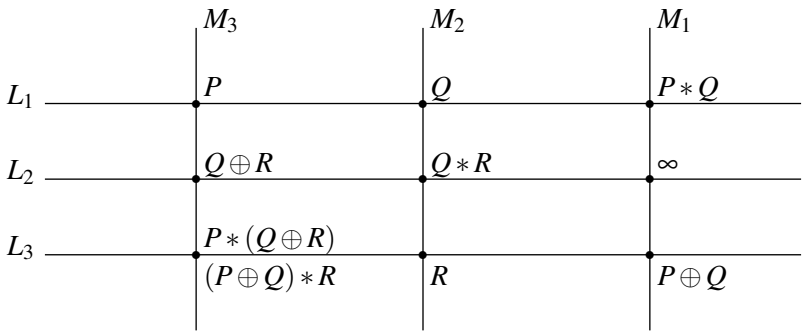


Figure 2.2: Associativity of addition law

Consider the two reducible cubics $C=L_1L_2L_3$ and $C'=M_1M_2M_3$. By construction, we have

- C and E intersect in

$$P,Q,P*Q,P\oplus Q,R,\underline{(P\oplus Q)*R},Q*R,\infty,Q\oplus R,$$

- C' and E intersect in

$$P,Q,P*Q,P\oplus Q,R,\underline{P*(Q\oplus R)},Q*R,\infty,Q\oplus R.$$

So if the point are all distinct, we apply Lemma 2.4.4 since the elliptic curve is an irreducible cubic. Then

$$(P\oplus Q)*R=P*(Q\oplus R).$$

The other cases are analogous, but we will not discuss them: the intersection points do not need to be distinct, some of them could be ∞, etc. ■

R We can equivalently define the group law by saying that $P \oplus Q \oplus R = 0 (= \infty)$ if and only if P, Q, R are the three points of intersection of a line L with E (counted with multiplicities). The extreme case is when L is a line of inflection. In that case $L \cap E$ is one point P with multiplicity 3, which means $3P = 0$.

2.4.2 Computing with the group law

Proposition 2.4.5 Let K be a field (we are not assuming the field to be algebraically closed). Let E be an elliptic curve over K, and let L be a line defined over K. Let P_1, P_2 and P_3 be the intersection points of E and L over $\overline{K}$. If any two of the P_i for $i = 1,2,3$ is K-rational, so is the third.

Proof. Let us assume for simplicity that E is given by a short Weierstrass equation (the general case is analogous and it involves more calculations). Let E be given by $y^2 = f(x) = x^3 + ax + b$. Let L be a vertical line $L : x = c$, with $c \in K$ by hypothesis. If no point (c, y) belongs to E, then the intersection is given by the point ∞ with multiplicity 3 and ∞ is always a K-rational point. Therefore, let us assume that $L \cap E$ consists of $(c, \pm\sqrt{f(c)})$ and ∞, where $\sqrt{f(c)} \in K$, since by hypotheses at least two points are K-rational. The statement then is equivalent to say that $\sqrt{f(c)} \in K$ if and only if $-\sqrt{f(c)} \in K$. Notice that if $\sqrt{f(c)} = 0$ then L is the tangent line to E at $(c, 0)$.
Let $L : y = mx + c$ with $m, c \in K$. The intersection $L \cap E$ is given by

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

By moving all terms to the same side, expanding and then factorizing, we get

$$x^3 - m^2x^2 + (a - 2mc)x + (b - c^2) = (x - x_1)(x - x_2)(x - x_3) = 0, \qquad \text{in } \overline{K}$$

where $x_1, x_2, x_3 \in \overline{K}$ are the roots of the cubic. Since two intersection points are K-rational then two between x_1, x_2 and x_3 are in K. By equating the terms of degree 2, we get $x_1 + x_2 + x_3 = m^2$. Hence, since the line L is defined over K, we have that $x_1, x_2, x_3 \in K$. ■

We now give a more explicit description of the group law on $E(\overline{K})$, but only for a curve E given by a short Weierstrass equation.

Proposition 2.4.6 Let $E : y^2 = x^3 + ax + b$ be an elliptic curve given by a short Weierstrass equation. Let $P_1, P_2 \in E(\overline{K})$. Then $P_1 \oplus P_2$ is given by

(1) If $P_1 = \infty$ then $P_1 \oplus P_2 = P_2$; if $P_2 = \infty$, then $P_1 \oplus P_2 = P_1$.

(2) Assume that $P_1, P_2 \neq \infty$, so that $P_i = (x_i, y_i)$, $i = 1, 2$.
If $x_1 = x_2$ and $y_1 = -y_2$ then $P_1 \oplus P_2 = \infty$.

(3) Assume that $P_1, P_2 \neq \infty$, so that $P_i = (x_i, y_i)$, $i = 1, 2$.
If $x_1 = x_2$ and $y_1 = y_2 \neq 0$ then set $m = \frac{3x_1^2 + a}{2y_1}$; otherwise, set $m = \frac{y_1 - y_2}{x_1 - x_2}$.
Let $x_3 = m^2 - x_1 - x_2$ and $y_3 = y_1 + m(x_3 - x_1)$, then $P_1 \oplus P_2 = (x_3, -y_3)$.

Proof. We note that (1) and (2) are just a restatement of Theorem 2.4.1 (*ii*) and (*iii*). So we only need to prove (3). In that case, let $L : y = mx + c$ be the line through P_1 and P_2. If $P_1 = P_2$, then L is the tangent line at P_1 with $m = \frac{3x_1^2 + a}{2y_1}$ and $c = y_1 - mx_1$. Otherwise, L is the line with slope $m = \frac{y_2 - y_1}{x_2 - x_1}$ and x-intercept $c = y_1 - mx_1 = y_2 - mx_2$. The intersection $L \cap E$ is then given by

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

By moving all terms to the same side, expanding and then factorizing, we get

$$x^3 - m^2x^2 + (a - 2mc)x + (b - c^2) = (x - x_1)(x - x_2)(x - x_3) = 0,$$

where $x_1, x_2, x_3 \in \overline{K}$ are the roots of the cubic, counted with multiplicity. By equating the terms of degree 2, we get $x_1 + x_2 + x_3 = m^2$, and the points (x_1, y_1), (x_2, y_2) and (x_3, y_3). We note that if $x_i \in K$ then $y_i = mx_i + c \in K$ and the intersection point (x_i, y_i) is defined over K. We also note that, if two of the roots x_1, x_2, x_3 are defined over K, then so is the third one since $x_1 + x_2 + x_3 = m^2 \in K$. ■

Example 2.4.6.1 Let $E : y^2 = x^3 + 73$, and $P = (2, 9)$, $Q = (3, 10)$.

(a) By definition $\ominus P = (2, -9)$.

(b) The slope of the tangent line at P is $m = \frac{3x_P^2}{2y_P} = \frac{3(2)^2}{2(9)} = \frac{2}{3}$; so its equation is $y = \frac{2}{3}x + \frac{23}{3}$. Let $R = (x_R, y_R)$ be the third point of intersection of this line with E. Then, we have $2x_P + x_R = m^2$. So $x_R = (\frac{2}{3})^2 - 2(2) = -\frac{32}{9}$, and $y_R = \frac{2}{3}(-\frac{32}{9}) + \frac{23}{3} = \frac{143}{27}$. Hence $2P = \ominus R = \ominus(x_R, y_R) = (x_R, -y_R) = (-\frac{32}{9}, -\frac{143}{27})$.

(c) The slope of the line through P and Q is $m = \frac{y_Q - y_P}{x_Q - x_P} = \frac{10-9}{3-2} = 1$, and the equation of the line is $y = x + 7$. Let $R = (x_R, y_R)$ be the third point of intersection of this line with E. Then, we have $x_P + x_Q + x_R = m^2$. So $x_R = (1)^2 - 2 - 3 = -4$, and $y_R = x_R + 7 = -4 + 7 = 3$. Hence $P \oplus Q = \ominus R = (-4, -3)$.

R If $E : y^2 = f(x)$ is given by a medium Weierstrass equation (2.3), then the negative $\ominus P$ of a point P is easy to find. Indeed, if $P = (x, y)$ then the line through P and ∞ is the vertical line $X = x$. So the third point of intersection of that line with E is $\ominus P = P * \infty = (x, -y)$. Otherwise, since $P = \infty$ is the identity element, we have $\ominus P = \infty$.
If E is given by a long Weierstrass equation (2.1), then the negative $\ominus P$ of a point $P = (x, y) \neq \infty$ is given by $\ominus P = P * \infty = (x, -y - a_1x - a_3)$.

Corollary 2.4.7 If $K \subseteq K' \subseteq \overline{K}$ is a subfield, then $E(K')$ is a subgroup of $E(\overline{K})$.

Proof. By definition, the identity element $\infty \in E(K')$; also $P = (x, y) \in E(K')$ implies that $\ominus P = (x, -y - a_1x - a_3) \in E(K')$. So we only need to show that

$$P, Q \in E(K') \Rightarrow P \oplus Q \in E(K').$$

If $P, Q \in E(K')$, then the slope of the line through P and Q belongs to K', and (generalizations of) the formulas in Proposition 2.4.6 show that the coordinates of $P \oplus Q$ are in K'. ■

2.5 Singular curves

A Weierstrass cubic $y^2 = x^3 + ax + b = f(x)$ is *singular* if its discriminant $\Delta = -(4a^3 + 27b^2) = 0$, so, if and only if $f(x)$ has at least a **double** root e. In that case, there is a *unique* singular point $P_0 = (e, 0)$. Even though such curves are **not** elliptic curves, they are still useful. Let $E_{ns}(\overline{K})$ be the set of all non-singular points, that is

$$E_{ns}(\overline{K}) = E(\overline{K}) \setminus \{P_0\}.$$

We will show that $E_{ns}(\overline{K})$ is a group.

Claim: $E_{ns}(\overline{K})$ is an abelian group with the same group law $\oplus$ as before. This works because

$$P,Q \neq P_0 \Rightarrow P*Q \neq P_0.$$

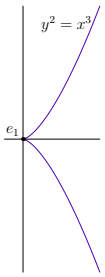
There are two sub-cases.

Case1 :
The cubic $f(x)$ has a triple root $e \in K$. By expanding $f(x) = (x-e)^3 = x^3+ax+b$, we see that $e = a = b = 0$. So $E : y^2 = x^3$, and the point $(0,0)$ is a **cusp**. This is called the **additive case**.

Proposition 2.5.1 The map

$$\begin{aligned} \varphi : E_{ns}(\overline{K}) &\to \overline{K}_+ \\ (x,y) &\mapsto \frac{x}{y}, \\ \infty &\mapsto 0, \end{aligned}$$

where $\overline{K}_+$ is the additive group of $\overline{K}$, is an isomorphism of abelian groups.



Proof. We need to check that φ is a group homomorphism, which is also a bijection. Let $(x,y) \in E_{ns}(\overline{K}) \setminus \{\infty\}$, then $xy \neq 0$ and $y^2 = x^3$. Setting $t = \frac{y}{x}$, we see that $(x,y) = (t^2,t^3)$, and that φ is indeed a bijection, whose inverse is the map

$$\begin{aligned} \psi : \overline{K}_+ &\to E_{ns}(\overline{K}) \\ t &\mapsto (t^2,t^3), t \neq 0, \\ 0 &\mapsto \infty. \end{aligned}$$

So it only remains to show that φ is a group homomorphism.
Let L be a line which doesn't pass through $P_0 = (0,0)$. Then L has an equation of the form $\lambda x + \mu y = 1$ (up to scaling), and intersects E at (t^2,t^3) if and only if $\lambda t^2 + \mu t^3 = 1$. Letting $u = \frac{x}{y} = \frac{1}{t}$, we see that u satisfies $\frac{\lambda}{u^2} + \frac{\mu}{u^3} = 1$ or, equivalently, the cubic $u^3 - \lambda u - \mu = 0$. This has three roots u_1,u_2,u_3 with $u_1+u_2+u_3 = 0$. If the associated points on $E_{ns}(\overline{K})$ are $P = (t_i^2,t_i^3) = (u_i^{-2},u_i^{-3})$, $i = 1,2,3$, then $P_1 \oplus P_2 \oplus P_3 = 0(\infty)$ and $u_1+u_2+u_3 = 0$. It follows that the map is a group homomorphism. ■

As in Corollary 2.4.7, an immediate consequence of the proof is that $E_{ns}(K)$ is a subgroup of $E_{ns}(\overline{K})$ which is isomorphic to K_+.

R In the proof above, we used the following fact. Let $\phi : G \to H$ be a map between two groups. Then ϕ is a group homomorphism if and only if $\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2)$. To show this it is equivalent to check that, whenever $g_1 *_G g_2 *_G g_3 = e_G$ (the identity element in G) then $\phi(g_1) *_H \phi(g_2) *_H \phi(g_3) = e_H$ and also that $\phi(e_G) = e_H$.

Case2 :
The cubic $f(x)$ has a double root $e_1 = e_2 = e \neq 0$ and a simple root e_3. Since the sum of the roots must be zero, it follows that $e_3 = -2e$. So we can write $E : y^2 = (x-e)^2(x+2e)$. In that case, the singular point $P_0 = (e,0)$ is a **node**. By making a translation, we can assume that $E : y^2 = x^2(x+a)$, with $a \in K^\times$, and $P_0 = (0,0)$. This is called the **multiplicative case**. Let α be a root of the polynomial $x^2 - a$ in $\overline{K}$.

Proposition 2.5.2 The map

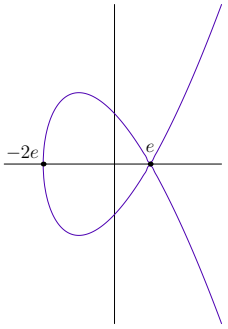
$$\begin{aligned} \varphi : E_{ns}(\overline{K}) &\to \overline{K}^{\times} \\ (x,y) &\mapsto u := \frac{y+\alpha x}{y-\alpha x}, \\ \infty &\mapsto 1, \end{aligned}$$

where $\overline{K}^{\times}$ is the multiplicative group of $\overline{K}$, is an isomorphism of abelian groups.

(1) If $\alpha \in K$, then φ is an isomorphism of $E_{ns}(K)$ onto $K^{\times}$.

(2) If $\alpha = \sqrt{a} \notin K$, let $L = K(\alpha)$. Then φ gives an isomorphism

$$E_{ns}(K) \simeq \left\{ s + r\alpha \in L \middle| s,r \in K, s^2 - ar^2 = 1 \right\}.$$



Proof. To show that φ is a bijection, let $(x,y) \neq (0,0)$ and set $t = y/x$. Then

$$u = \frac{y/x+\alpha}{y/x-\alpha} = \frac{t+\alpha}{t-\alpha}$$

Solving this for t, we get

$$t = \alpha \frac{u+1}{u-1}.$$

Now, since $y^2 = x^2(x+a)$, we get $x+a = (y/x)^2 = t^2$, and

$$x = t^2 - a = \alpha^2 \left(\frac{u+1}{u-1} \right)^2 - \alpha^2 = \alpha^2 \frac{(u+1)^2 - (u-1)^2}{(u-1)^2} = \frac{4\alpha^2 u}{(u-1)^2} = \frac{4au}{(u-1)^2}.$$

Since $y = x(y/x)$, we get

$$y = \alpha \frac{u+1}{u-1} \cdot \frac{4au}{(u-1)^2} = \frac{4a\alpha u(u+1)}{(u-1)^3}.$$

So φ is again a bijection whose inverse ψ is given by

$$x := \frac{4au}{(u-1)^2} \quad \text{and} \quad y := \frac{4a\alpha u(u+1)}{(u-1)^3}$$

To see that φ is a group homomorphism, let $L : \lambda x + \mu y = 1$ be a line which intersects E at $P_1, P_2, P_3 \neq P_0$, with u-parameters u_1, u_2, u_3. We must show that $u_1 u_2 u_3 = 1$. But these parameters are the roots of

$$\lambda \frac{4ua}{(u-1)^2} + \mu \frac{4ua\alpha(u+1)}{(u-1)^3} = 1,$$

or equivalently

$$\lambda 4ua(u-1) + \mu 4ua\alpha(u+1) = (u-1)^3.$$

This is a cubic in u whose constant term is $-u_1 u_2 u_3 = -1$, hence $u_1 u_2 u_3 = 1$.
In case (1), since $\alpha \in K$, $(x,y) \in E_{ns}(K) \Rightarrow u \in K^{\times}$. So φ induces an isomorphism $E_{ns}(K) \simeq K^{\times}$ in that case.
In case (2), let $\alpha = \sqrt{a} \notin K$, and recall that

$$L = K(\alpha) = \{ s + r\sqrt{a} : s,r \in K \}.$$

By case (1) applied to E on the field L, we have $E_{ns}(L) \cong L^\times$. Since the *conjugation map* $(u := s + r\sqrt{a} \mapsto \bar{u} := s - r\sqrt{a})$ is an automorphism of L which preserves K, $E_{ns}(K)$ is a subgroup of $E_{ns}(L)$ (see Corollary 2.4.7). So we only need to find the image of $E_{ns}(K)$ inside $L^\times$. But we see that

$$u = \frac{y+\alpha x}{y-\alpha x} = \frac{(y+\alpha x)^2}{(y-\alpha x)(y+\alpha x)} = \frac{y^2+2\alpha xy+\alpha^2 x^2}{y^2-\alpha^2 x^2} = \frac{(y^2+ax^2)+2xy\alpha}{y^2-ax^2} = s+r\alpha,$$
$$u\bar{u} = (s+r\alpha)(s-r\alpha) = s^2-ar^2 = 1.$$

So

$$E_{ns}(K) \cong \left\{u \in L^\times : u\bar{u} = 1\right\}.$$

■

Example 2.5.2.1 Let $K = \mathbb{R}$, $L = \mathbb{C}$ and $E : y^2 = x^2(x-1)$. Then $E(\mathbb{C}) = \mathbb{C}^\times$ and $E(\mathbb{R})$ is isomorphic to the unit circle inside $\mathbb{C}^\times$.

Definition 2.7 In Proposition 2.5.2, the curve E is said to be **split-multiplicative** when it satisfies case (1), and **non-split-multiplicative** in case (2).

Integer Factorization Using Elliptic Curves
Pollard's $(p-1)$-Method
Lenstra's Elliptic Curve Factorization Method
A Heuristic Explanation

3. Applications I

3.1 Integer Factorization Using Elliptic Curves

In 1987, Hendrik Lenstra published a landmark paper that introduces and analyzes the Elliptic Curve Method (ECM), which is a powerful algorithm for factoring integers using elliptic curves. Lenstra's algorithm is well suited for finding "medium-sized" factors of an integer N, which today means a number with between 10 to 40 decimal digits. The ECM method is used as a crucial step in the "number field sieve," which is the best known algorithm for hunting factorizations. In this section we will give a very basic introduction to the ECM.

3.1.1 Pollard's $(p-1)$-Method

Lenstra's discovery of ECM was inspired by Pollard's $(p-1)$-method, which we describe in this section.

Definition 3.1 Let B be a positive integer. If n is a positive integer with prime factorization $n = \prod p_i^{e_i}$, then n is **B-power smooth** if $p_i^{e_i} \leq B$ for all i.

For example, $30 = 2 \cdot 3 \cdot 5$ is B power smooth for $B = 5, 7$, but $150 = 2 \cdot 3 \cdot 5^2$ is not 5-power smooth (it is $B = 25$-power smooth).

Let N be a positive integer that we wish to factor. We use the Pollard $(p-1)$-method to look for a nontrivial factor of N using the following strategy.
First, we choose a positive integer B, usually with at most six digits. Suppose that there is a prime divisor p of N such that $p-1$ is B-power smooth. We try to find p.
If $a > 1$ is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$. Let $m = \operatorname{lcm}(1, 2, 3, \ldots, B)$, and observe that our assumption that $p-1$ is B-power smooth implies that $p-1 \mid m$, so

$$a^m \equiv 1 \pmod{p}.$$

Thus

$$p \mid \gcd(a^m - 1, N) > 1.$$

If $\gcd(a^m - 1, N) < N$ also then $\gcd(a^m - 1, N)$ is a nontrivial factor of N.
If $\gcd(a^m - 1, N) = N$, then $a^m \equiv 1 \pmod{q^r}$ for every prime power divisor q^r of N. In this case, repeat the above steps but with a smaller choice of B or possibly a different choice of a. It

is also a good idea to check from the start whether or not N is not a perfect power M^r and, if so, replace N by M. We formalize the algorithm as follows:

Algorithm 3.1 — Pollard $p-1$ Method. Given a positive integer N and a bound B, this algorithm attempts to find a nontrivial factor g of N. Each prime $p \mid g$ is likely to have the property that $p-1$ is B-power smooth (see the observation below).

Step 1: Compute $m = \text{lcm}(1,2,\ldots,B)$.

Step 2: Set $a = 2$.

Step 3: Compute $x = a^m - 1 \pmod N$ and $g = \gcd(x,N)$.

Step 4: If $g \neq 1$ or N, output g and terminate.

Step 5: If $a < 10$ (say), replace a by $a+1$ and go to Step 3. Otherwise, terminate.

For a fixed B, this algorithm succeed in splitting N when N is divisible by a prime p such that $p-1$ is B-power smooth. Approximately 15 percent of primes p in the interval from 10^{15} and $10^{15}+10000$ are such that $p-1$ is 10^6 power smooth, so the Pollard method with $B = 10^6$ already fails nearly 85 percent of the time at finding 15-digit primes in this range. The following examples illustrate the Pollard $(p-1)$-method.

Example 3.1.0.2 In this example, Pollard works perfectly. Let $N = 5917$. We try to use the Pollard $p-1$ method with $B = 5$ to split N. We have $m = \text{lcm}(1,2,3,4,5) = 60$; taking $a = 2$, we have

$$2^{60} - 1 \equiv 3416 \pmod{5917}$$

and

$$\gcd(2^{60}-1, 5917) = \gcd(3416, 5917) = 61,$$

so 61 is a factor of 5917.

Example 3.1.0.3 In this example, we replace B with a larger integer. Let $N = 779167$. With $B = 5$ and $a = 2$, we have

$$2^{60} - 1 \equiv 710980 \pmod{779167},$$

and $\gcd(2^{60}-1, 779167) = 1$. With $B = 15$, we have

$$m = \text{lcm}(1,2,\ldots,15) = 360360,$$

$$2^{360360} - 1 \equiv 584876 \pmod{779167},$$

and

$$\gcd(2^{360360}-1, N) = 2003,$$

so 2003 is a nontrivial factor of 779167.

Example 3.1.0.4 In this example, we replace B by a smaller integer. Let $N = 4331$. Suppose $B = 7$, so $m = \text{lcm}(1,2,\ldots,7) = 420$, $2^{420} - 1 \equiv 0 \pmod{4331}$, and $\gcd(2^{420}-1, 4331) =$

4331, so we do not obtain a factor of 4331. If we replace B by 5, Pollard's method works: $2^{60} - 1 \equiv 1464 \pmod{4331}$, and $\gcd(2^{60} - 1, 4331) = 61$, so we split 4331.

Example 3.1.0.5 In this example, $a = 2$ does not work, but $a = 3$ does. Let $N = 187$. Suppose $B = 15$, so $m = \text{lcm}(1, 2, \ldots, 15) = 360360$, $2^{360360} - 1 \equiv 0 \pmod{187}$, and $\gcd(2^{360360} - 1, 187) = 187$, so we do not obtain a factor of 187. If we replace $a = 2$ by $a = 3$, then Pollard's method works: $3^{360360} - 1 \equiv 66 \pmod{187}$, and $\gcd(3^{360360} - 1, 187) = 11$. Thus $187 = 11 \cdot 17$.

Fix a positive integer B. If $N = pq$ with p and q prime, and we assume that $p - 1$ and $q - 1$ are not B-power smooth, then the Pollard $(p-1)$-method is unlikely to work. For example, let $B = 20$ and suppose that $N = 59 \cdot 101 = 5959$. Note that neither $59 - 1 = 2 \cdot 29$ nor $101 - 1 = 4 \cdot 25$ is B-power smooth. With $m = \text{lcm}(1, 2, 3, \ldots, 20) = 232792560$, we have

$$2^m - 1 \equiv 5944 \pmod{N},$$

and $\gcd(2^m - 1, N) = 1$, so we do not find a factor of N. As remarked above, the problem is that $p - 1$ is not 20-power smooth for either $p = 59$ or $p = 101$. However, notice that $p - 2 = 3 \cdot 19$ is 20-power smooth. Lenstra's ECM replaces $(\mathbb{Z}/p\mathbb{Z})^*$, which has order $p - 1$, by the group of points on an elliptic curve E over $\mathbb{F}_p$.

3.1.2 Lenstra's Elliptic Curve Factorization Method

Algorithm 3.2 — Elliptic Curve Factorization Method . Given a positive integer N and a bound B, this algorithm attempts to find a nontrivial factor g of N or outputs "Fail."

Step 1: Compute $m = \text{lcm}(1, 2, \ldots, B)$.

Step 2: Choose a random elliptic curve: choose a random $a \in \mathbb{Z}/N\mathbb{Z}$ such that

$$4a^3 + 27 \in (\mathbb{Z}/N\mathbb{Z})^*.$$

Then $P = (0, 1)$ is a point on the elliptic curve $y^2 = x^3 + ax + 1$ over $\mathbb{Z}/N\mathbb{Z}$.

Step 3: Attempt to compute mP. If at some point we cannot compute a sum of points because some denominator is not coprime to N, we compute the greatest common divisor g of this denominator with N. If g is a nontrivial divisor, output it. If every denominator is coprime to N, output "Fail."

If Algorithm 3.2 fails for one random elliptic curve, then we may repeat the above algorithm with a different elliptic curve or change the point P with another point on the curve.

Example 3.1.0.6 For simplicity, we use an elliptic curve of the form

$$y^2 = x^3 + ax + 1,$$

which has the point $P = (0, 1)$ already on it. We factor $N = 5959$ using the elliptic curve method. Let $B = 20$ and let $m = \text{lcm}(1, 2, \ldots, 20) = 232792560$.
First, we choose $a = 1201$ at random and consider $y^2 = x^3 + 1201x + 1$ over $\mathbb{Z}/5959\mathbb{Z}$: maybe this is not a field, but we suppose otherwise and continue. If $\mathbb{Z}/5959\mathbb{Z}$ is a field, then 5959 is a prime, otherwise we will obtain a contradiction with the group law on the

elliptic curve considered. Using the duplication formula we compute $2^i \cdot P = 2^i \cdot (0,1)$ for $i \in \{4,5,6,7,8,13,21,22,23,24,26,27\}$, and then we add in order to compute mP. It turns out that, during this computation we can always add points, so we do not split N using $a = 1201$.
Next, we try $a = 389$ and at some stage in the computation we add the points $P = (2051,5273)$ and $Q = (637,1292)$. When computing the group law explicitly, we try to compute the slope of the line through P and Q, i.e. $(y_1 - y_2)/(x_1 - x_2)$, in $(\mathbb{Z}/5959\mathbb{Z})^*$, but we fail since $x_1 - x_2 = 1414$ and $\gcd(1414,5959) = 101$. We thus find the nontrivial factor 101 of 5959.

3.1.3 A Heuristic Explanation

Let N be a positive integer and, for simplicity of exposition, assume that $N = p_1 \cdots p_r$ with the p_i distinct primes. By the Chinese Remainder Theorem there is a natural isomorphism

$$f : (\mathbb{Z}/N\mathbb{Z})^* \to (\mathbb{Z}/p_1\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_r\mathbb{Z})^*.$$

When using Pollard's method, we choose an $a \in (\mathbb{Z}/N\mathbb{Z})^*$, compute a^m and $\gcd(a^m - 1, N)$. This gcd is divisible exactly by the primes p_i such that $a^m \equiv 1 \pmod{p_i}$. To reinterpret Pollard's method using the above isomorphism, let $(a_1,\ldots,a_r) = f(a)$. Then $(a_1^m,\ldots,a_r^m) = f(a^m)$, and the p_i that divide $\gcd(a^m - 1, N)$ are exactly the p_i such that $a_i^m = 1$. These p_i include the primes p_j such that $p_j - 1$ is B-power smooth, where $m = \operatorname{lcm}(1,\ldots,m)$.

We will not define $E(\mathbb{Z}/N\mathbb{Z})$ when N is composite, since this is not needed for the algorithm, where we assume that N is prime and hope for a contradiction. However, for the remainder of this paragraph, we pretend that $E(\mathbb{Z}/N\mathbb{Z})$ is meaningful and describe a heuristic connection between Lenstra and Pollard's methods. The significant difference between Pollard's method and the elliptic curve method is that the isomorphism f is replaced by an isomorphism (in quotes)

$$\text{“}g : E(\mathbb{Z}/N\mathbb{Z}) \to E(\mathbb{Z}/p_1\mathbb{Z}) \times \cdots \times E(\mathbb{Z}/p_r\mathbb{Z})\text{”}$$

where E is $y^2 = x^3 + ax + 1$, and the a of Pollard's method is replaced by $P = (0,1)$. We put the isomorphism in quotes to emphasize that we have not defined $E(\mathbb{Z}/N\mathbb{Z})$. When carrying out the elliptic curve factorization algorithm, we attempt to compute mP, and if some components of $g(Q)$ are 0, for some point Q that appears during the computation, but others are nonzero, we find a nontrivial factor of N.

4. Isomorphisms and j-invariant

In this chapter, we define the j-invariant of an elliptic curve. This is an invariant which tells us when two elliptic curves are isomorphic. We will assume throughout this chapter that K is a field of **characteristic different from 2 and 3**. These cases will be covered later on.

From now, the group law on an elliptic curve E, would simply be denoted by $+$. We will also denote the point at $\infty(=[0:1:0])$ by 0.

4.1 Isomorphisms and j-invariant

Let $E: y^2 = x^3 + Ax + B$, with $A, B \in K$, be a short Weierstrass cubic curve.
Let $\mu \in \overline{K}^\times$, and put

$$E': y^2 = x^3 + A'x + B', \tag{4.1}$$

where $A' = \mu^4 A$, $B' = \mu^6 B$. Moreover, E is an elliptic curve if and only if E' is: indeed, $\Delta' = \mu^{12}\Delta$. In fact more is true.

Theorem 4.1.1 Let $E: y^2 = x^3 + Ax + B$, with $A, B \in K$, be an elliptic curve and $\mu \in \overline{K}^\times$. Let E' be the curve given by (4.1). Then the map

$$\begin{aligned} \phi : E(\overline{K}) &\to E'(\overline{K}) \\ (x,y) &\mapsto (\mu^2 x, \mu^3 y) \end{aligned}$$

is a group isomorphism.

Proof. It is easy to see that $(x,y) \in E(\overline{K}) \Leftrightarrow (\mu^2 x, \mu^3 y) \in E'(\overline{K})$, and that the inverse of ϕ is the map $\psi : (x,y) \mapsto (\mu^{-2}x, \mu^{-3}y)$. So it only remains to show that ϕ is a group homomorphism. It is enough to show that $\phi(\infty) = \infty$, and that

$$P + Q + R = \infty \Rightarrow \phi(P) + \phi(Q) + \phi(R) = \infty.$$

In projective coordinates, the map ϕ is given by

$$\begin{aligned} \phi : E(\overline{K}) &\to E'(\overline{K}) \\ [X:Y:Z] &\mapsto [\mu^2 X : \mu^3 Y : Z]. \end{aligned}$$

So,

$$\phi(\infty) = \phi([0:1:0]) = [0:\mu^3:0] = [0:1:0] = \infty.$$

Let $L: aX + bY + cZ = 0$ be the line which intersects E at P, Q and R. Then the image of L under ϕ is the line $L': a'X + b'Y + c'Z = 0$, where $a' = a/\mu^2$, $b' = b/\mu^3$ and $c' = c$. By Bezout's Theorem, L' intersects E' at three points (counted with multiplicity), which must necessarily be $\phi(P)$, $\phi(Q)$ and $\phi(R)$. So $\phi(P) + \phi(Q) + \phi(R) = \infty$. ■

R When $\mu \in K^\times$, then the curve E' in (4.1) is defined over K, and the map ϕ in Theorem 4.1.1 induces an isomorphism $\phi : E(K) \simeq E'(K)$.

Definition 4.1 Let $E: y^2 = x^3 + Ax + B$, $E': y^2 = x^3 + A'x + B'$, with $A, A', B, B' \in K$ be two elliptic curves. we say that E and E' are **isomorphic** if there exists $\mu \in \overline{K}^\times$ such that $A' = \mu^4 A$, $B' = \mu^6 B$. We say that E and E' are **isomorphic over** K if in addition $\mu \in K^\times$. The group isomorphism in Theorem 4.1.1

Example 4.1.1.1 Consider the elliptic curves

$$E_1: y^2 = x^3 + x + 1$$
$$E_2: y^2 = x^3 + 16x + 64$$
$$E_3: y^2 = x^3 + 4x + 8$$

Then we see that

- E_1 is isomorphic to E_2 over $\mathbb{Q}$, simply take $\mu = 2$.
- E_1 is isomorphic to E_3 over $\mathbb{Q}(\sqrt{2})$, but **not** over $\mathbb{Q}$, take $\mu = \sqrt{2}$.

We will now give a simple criterion which allows us to determine when two elliptic curves are isomorphic.

Definition 4.2 Let $E: y^2 = x^3 + Ax + B$, with $A, B \in K$, be an elliptic curve with discriminant $\Delta = -4A^3 - 27B^2$. We define the **j-invariant** of E by

$$j(E) := -1728\frac{4A^3}{\Delta}.$$

Theorem 4.1.2 Let $E: y^2 = x^3 + Ax + B$, and $E': y^2 = x^3 + A'x + B'$, with $A, A', B, B' \in K$, be two elliptic curves. Then E is isomorphic to E' if and only if $j(E) = j(E')$.

Proof. Assume that E is isomorphic to E' so that there is $\mu \in \overline{K}^\times$ such that $A' = \mu^4 A$ and $B' = \mu^6 B$. In this case, we already showed that $\Delta' = \mu^{12}\Delta$. Hence we have

$$j(E') = -1728\frac{4A'^3}{\Delta'} = -1728\frac{4(\mu^4 A)^3}{\mu^{12}\Delta} = -1728\frac{4A^3}{\Delta} = j(E).$$

Conversely, assume that $j(E) = j(E') = j$. We will show that E and E' are isomorphic.

Case 1. Assume that $j \neq 0, 1728$. Then, from Definition 4.2, we see that

$$j - 1728 = -1728\frac{4A^3}{\Delta} - 1728 = -1728\frac{4A^3 + \Delta}{\Delta} = 1728\frac{27B^2}{\Delta}.$$

So

$$\frac{j}{j-1728} = -\frac{4A^3}{27B^2}.$$

Hence $j(E) = j(E') = j$ implies that

$$\frac{4A^3}{27B^2} = \frac{4A'^3}{27B'^2} \Leftrightarrow \left(\frac{A}{A'}\right)^3 = \left(\frac{B}{B'}\right)^2.$$

Now, let μ be a solution to the (quadratic) equation

$$\mu^2 = \frac{A}{A'}\frac{B'}{B}.$$

Then, from the above identity, we see that

$$\mu^4 = \left(\frac{A}{A'}\right)^2\left(\frac{B'}{B}\right)^2 = \left(\frac{A}{A'}\right)^2\left(\frac{A'}{A}\right)^3 = \frac{A'}{A} \Rightarrow A' = \mu^4 A.$$

Similarly, we have

$$\mu^6 = \left(\frac{A}{A'}\right)^3\left(\frac{B'}{B}\right)^3 = \left(\frac{B}{B'}\right)^2\left(\frac{B'}{B}\right)^3 = \frac{B'}{B} \Rightarrow B' = \mu^6 B.$$

Case 2. Assume that $j = 0$. This implies that $A = A' = 0$, and that $B, B' \neq 0$. We choose μ such that

$$\mu^6 = \frac{B'}{B}.$$

Case 3. Assume that $j = 1728$. This implies that $B = B' = 0$, and that $A, A' \neq 0$. We choose μ such that

$$\mu^4 = \frac{A'}{A}.$$

■

Example 4.1.2.1 In Example 4.1.1.1, it is easy to see that

$$j(E_1) = j(E_2) = j(E_3) = \frac{6912}{31} = \frac{2^8 3^3}{31}.$$

R From the proof of Theorem 4.1.2, we see that:

(i) When $j \neq 0, 1728$ (Case 1) and $\mu^2 = \frac{A}{A'}\frac{B'}{B}$ has a root in K, then the curves E and E' are isomorphic over K. Otherwise, they are isomorphic over $K(\mu)$, which is a quadratic extension of K.

(ii) When $j = 0$ (Case 2), then $\mu^6 = \frac{B'}{B}$ and the curves are isomorphic over an extension K' of K of degree 6 at most.

(iii) When $j = 1728$ (Case 3), then $\mu^4 = \frac{A'}{A}$ and the curves are isomorphic over an extension K' of K of degree at most 4.

Example 4.1.2.2 (a) In the Bachet-Mordell family $E_c : y^2 = x^3 + c$, with $0 \neq c \in \mathbb{Z}$, all elliptic curves are isomorphic over $\overline{\mathbb{Q}}$ since $j(E_c) = 0$ ($A = 0, B = c$). However, $E_{c_1} \cong E_{c_2}$ (over $\mathbb{Q}$) if and only if c_1/c_2 is a 6th power (in $\mathbb{Q}$).

(b) Similarly, in the family $E_a : y^2 = x^3 + ax$, with $0 \neq a \in \mathbb{Z}$, all curves are isomorphic over $\overline{\mathbb{Q}}$ since $j(E_a) = 1728$. But, $E_{a_1} \cong E_{a_2}$ if and only if a_1/a_2 is a 4th power.

Definition 4.3 Let E, E' be two elliptic curves over K. We say that E and E' are **twists** of each other if they are isomorphic. We say that E and E' are **quadratic twists** if they are isomorphic over a quadratic extension of K at most.

Example 4.1.2.3 (a) In Example 4.1.1.1, E_1 and E_3 are quadratic twists.

(b) The congruence number curves $E_1 : y^2 = x^3 - 25x$ and $E_2 : y^2 = x^3 - 4x$ are quadratic twist (take $\mu = \sqrt{10}/2$). Note that the fact that E_1 and E_2 are **not** isomorphic over $\mathbb{Q}$ implies that $E_1(\mathbb{Q}) \not\simeq E_2(\mathbb{Q})$. We will see later (in examples 10.5.1.1 and 10.5.1.2) that

$$E_1(\mathbb{Q}) = \{\infty, (0,0), (-5,0), (5,0)\} \times \langle P \rangle \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z},$$

where $P = (-4,6)$ is a point of *infinite* order, and that

$$E_2(\mathbb{Q}) = \{\infty, (0,0), (-2,0), (2,0)\} \simeq (\mathbb{Z}/2\mathbb{Z})^2.$$

Lattices and elliptic functions

Tori and elliptic curves

Torsion points.

Elliptic curves over $\mathbb{R}$

5. Elliptic curves over $\mathbb{C}$

In this chapter, we show that every complex torus can be identified with an elliptic curve in a way that is compatible with the group structure and vice versa.

5.1 Lattices and elliptic functions

In this section we recall the basic properties of elliptic functions. We use several results on meromorphic functions without proofs. Most of these results can be found in most undergraduate textbooks on complex analysis in one variable.

Definition 5.1 A **lattice** $L \subset \mathbb{C}$ is a subset given by

$$L := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\},$$

where $\omega_1, \omega_2 \in \mathbb{C}$ are linearly independent over $\mathbb{R}$ (see Figure 5.1).

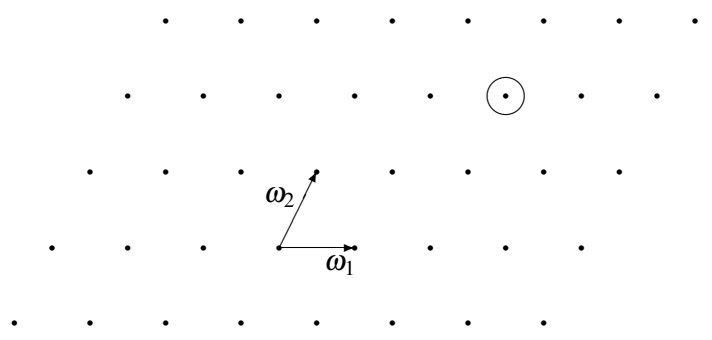


Figure 5.1: Lattice generated by ω_1 and ω_2

Let $L \subset \mathbb{C}$ be a lattice, then L is a **subgroup**: as a group $L \simeq \mathbb{Z} \times \mathbb{Z}$ and L is **discrete**, i.e. let $0 < r < \min\{|\omega_1|, |\omega_2|\}$, and put $D(0,r) = \{z \in \mathbb{C} : |z| < r\}$; then $D(0,r) \cap L = \{0\}$. So, for every $\omega \in L$, $\omega + D(0,r) = D(\omega, r)$ and $D(\omega, r) \cap L = \{\omega\}$.

Definition 5.2 Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ be a lattice. We define the **fundamental parallelogram** of L to be the region (see Figure 5.2)

$$\Pi := \{x\omega_1 + y\omega_2 : 0 \leq x, y < 1\}.$$

Let $L \subset \mathbb{C}$ be a lattice. Since it is a (normal) subgroup, the quotient $\mathbb{C}/L$ is an abelian group. Let $\pi_L : \mathbb{C} \to \mathbb{C}/L$ be the quotient map. Then, for every $z \in \mathbb{C}$,

$$\pi_L(z) = z + L = \{z + \omega : \omega \in L\}.$$

We will denote $\pi_L(z)$ by $[z]_L$, or simply $[z]$ if there is no ambiguity about the lattice. As a topological space $\mathbb{C}/L$ is isomorphic to a torus (see Figure 5.2). Every equivalence class $[z]$ has a *unique* representative $z_0 \in \Pi$. Indeed, write $z = x\omega_1 + y\omega_2$, and let $z_0 = x_0\omega_1 + y_0\omega_2$, where $x_0 = x - \lfloor x \rfloor, y_0 = x - \lfloor y \rfloor$. Then $z - z_0 \in L$, and z_0 is unique inside Π.

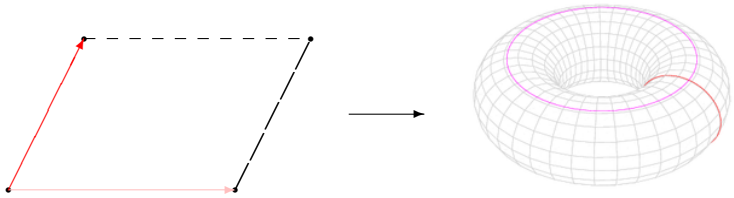


Figure 5.2: Fundamental parallelogram Π and quotient $\mathbb{C}/L$

Definition 5.3 Let $f : \mathbb{C} \to \mathbb{C}$ be a function.

(i) We say that f is **meromorphic** if, for every $z_0 \in \mathbb{C}$, f admits a power series expansion

$$f(z) = \sum_{m \geq r} a_m (z - z_0)^m, \text{ with } r \in \mathbb{Z} \text{ and } a_r \neq 0.$$

We call the integer r the **order** of f at z_0, and denote it by $\mathrm{ord}_{z_0}(f)$.

(ii) We say that z_0 is a **pole** if $\mathrm{ord}_{z_0}(f) < 0$, and that it is a **zero** if $\mathrm{ord}_{z_0}(f) > 0$.

(iii) We say that f is **holomorphic** (or **analytic**) if it is meromorphic and $\mathrm{ord}_z(f) \geq 0$ for all $z \in \mathbb{C}$. (In particular, constant functions are analytic.)

Example 5.1.0.4 (a) Every polynomial function over $\mathbb{C}$ is a holomorphic function.

(b) Every rational function, i.e. quotient of polynomial function is a meromorphic function.

(c) The exponential map $z \mapsto e^z$, $z \in \mathbb{C}$, is a holomorphic function.

The following theorem summarizes the results we will need about meromorphic functions.

Theorem 5.1.1 Let $\mathscr{M}(\mathbb{C})$ be the set of all meromorphic functions over $\mathbb{C}$. Then $\mathscr{M}(\mathbb{C})$ is a field. In other words,

(i) the sum of two meromorphic functions is a meromorphic function,

(ii) the product of two meromorphic functions is a meromorphic function, and

(iii) if f is a meromorphic function, then so is the function $z \mapsto \frac{1}{f(z)}$.

We now turn to the basic properties of elliptic functions.

Definition 5.4 Let L be a lattice, and $f : \mathbb{C} \to \mathbb{C}$ a meromorphic function. We say that f is an **elliptic function** for L (or is **doubly periodic** with respect of L) if

$$f(z+\omega) = f(z) \text{ for all } \omega \in L \text{ and all } z \in \mathbb{C}.$$

Theorem 5.1.2 Let $L \subset \mathbb{C}$ be a lattice, and $f : \mathbb{C} \to \mathbb{C}$ an elliptic function for L.

(i) If f has no pole, then f is constant.

(ii) If f is non-constant, then it has **finitely** many zeros and poles in the fundamental region Π. Let m_i be the orders of the poles in Π, and n_i the order of the zeros, both counted with multiplicities. Then
$$\sum_i n_i = -\sum_j m_j.$$

(iii) The integer $n = \sum_i n_i$ in (ii) is called the **order** of f. For every $a \in \mathbb{C}$, the function f takes the value a exactly n times, counted with multiplicities, inside Π (and hence inside $\omega + \Pi, \omega \in L$).

(iv) If f is not identically zero, then
$$\sum_{z \in \Pi} \operatorname{ord}_z(f) z \in L.$$

The Weierstrass $\wp$-function is the simplest example of an elliptic function. We now discuss its basic properties.

Definition 5.5 Let L be a lattice. The **Weierstrass $\wp$-function** $\wp_L(z)$ attached to L is given by

$$\wp_L(z) := \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{5.1}$$

In Theorem 5.1.6, we will prove that the series in (5.1) converges. But first, we need the following preliminary lemmas.

Lemma 5.1.3 The series

$$\sum_{\substack{(m,n)\in\mathbb{Z}\times\mathbb{Z}\\(m,n)\neq(0,0)}} \frac{1}{(m^2+n^2)^s}, s\in\mathbb{R},$$

converges if and only if $s>1$.

Proof. By the integral test, the series converges if and only if

$$I=\int\int_{x^2+y^2\geq 1}\frac{dxdy}{(x^2+y^2)^s}$$

converges. Let's make the change of variable $x=r\cos\theta$ and $y=r\sin\theta$, then we have

$$I=\int_0^{2\pi}\int_1^{\infty}\frac{rd\theta dr}{r^{2s}}=\int_0^{2\pi}\int_1^{\infty}\frac{d\theta dr}{r^{2s-1}}=2\pi\int_1^{\infty}\frac{dr}{r^{2s-1}}.$$

This integral converges if and only if $2s-1>1 \iff s>1$. ■

Lemma 5.1.4 Let $L\subset\mathbb{C}$ be a lattice. Then, for every $s>2$, the series

$$\sum_{\omega\in L\setminus\{0\}}\frac{1}{|\omega|^s}$$

converges.

Proof. Write $L=\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$. Then, by making use of Lemma 5.1.3, it is enough to prove that there exists $\delta>0$ (depending only on ω_1,ω_2) such that

$$|m\omega_1+n\omega_2|^2\geq\delta(m^2+n^2).$$

To this end, it is enough to show that the function

$$f(x,y)=\frac{|x\omega_1+y\omega_2|^2}{x^2+y^2},\ (x,y)\in\mathbb{R}^2\setminus\{(0,0)\},$$

has a strictly positive minimum. But we see that $f(x,y)$ is homogeneous, *i.e.,*

$$f(\lambda x,\lambda y)=f(x,y)\text{ for all }\lambda\neq 0.$$

So it is enough to prove that f has a positive minimum on the unit circle

$$S^1:=\left\{(x,y)\in\mathbb{R}^2:x^2+y^2=1\right\}.$$

Hence, this follows since S^1 is compact. ■

Lemma 5.1.5 Let $R>0$ be a real number. Then, the series

$$\sum_{\substack{\omega\in L\\|\omega|\geq 2R}}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)$$

converges absolutely uniformly on the closed disc $\overline{D}(0,R)$.

Proof. For any $z \in \overline{D}(0,R)$, since $|\omega| \geq 2R$, we have $|z-\omega| \geq \frac{|\omega|}{2}$ and $|z-2\omega| \leq 3|\omega|$, so

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \frac{|z||z-2\omega|}{|\omega|^2|z-\omega|^2} \leq \frac{12R}{|\omega|^3}. \tag{5.2}$$

So the series converges absolutely uniformly by Lemma 5.1.4. ■

We are now ready to prove our main result on Weierstrass $\wp$-functions.

Theorem 5.1.6 Let $L \subset \mathbb{C}$ be a lattice, and $\wp_L(z)$ be its Weierstrass $\wp$-function. Then, we have

(a) $\wp_L(z)$ is *meromorphic* and has a *double pole* at each $\omega \in L$.

(b) $\wp_L(z) = \wp_L(-z)$, for all $z \in \mathbb{C}$ (*even*).

(c) $\wp_L(z+\omega) = \wp_L(z)$, for all $z \in \mathbb{C}$ (*doubly periodic*).

Proof. (a) Keeping the notations of Lemma 5.1.5, the truncated series in (5.2) converges absolutely uniformly, hence is analytic. Since we have only omitted a finite number of terms, this implies that $\wp_L(z)$ is analytic for every $z \in \mathbb{C} \setminus L$. For every $\omega \in L$, $\wp_L(z)$ is analytic near ω, but the term $\frac{1}{(z-\omega)^2}$ causes it to have a pole of order 2 at ω. This completes (a).

(b) Since L is a subgroup of $\mathbb{C}$, $\omega \in L \iff -\omega \in L$. This means that the sum giving $\wp_L(z)$ is unchanged if we replace z by $-z$ since

$$\frac{1}{(-z-(-\omega))^2} - \frac{1}{\omega^2} = \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

So $\wp_L(z) = \wp_L(-z)$ for all $z \in \mathbb{C} \setminus L$.

(c) Since $\wp_L(z)$ converges uniformly on compact sets, we can differentiate it termwise. Furthermore, since $\wp_L(z)$ is even, $\wp'_L(z)$ is odd.

$$\wp'_L(z) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3}, \, z \in \mathbb{C} \setminus L.$$

Let $\omega_0 \in L$, then the translation $(L \to L, \, \omega \mapsto \omega - \omega_0)$ is a bijection, so

$$\wp'_L(z+\omega_0) = -2 \sum_{\omega \in L} \frac{1}{(z-(\omega-\omega_0))^3} = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3} = \wp'_L(z), \; z \in \mathbb{C} \setminus L.$$

This means that the function $\wp'_L(z)$ is doubly periodic. Since $\wp'_L(z+\omega_0) = \wp'_L(z)$, we have

$$\wp_L(z+\omega_0) - \wp_L(z) = c_{\omega_0},$$

for some constant $c_{\omega_0} \in \mathbb{C}$.
Applying this to $z_1 = -\frac{1}{2}\omega_1 \notin L$, and using the fact that $\wp_L(z)$ is even, we see that

$$\wp_L(z_1+\omega_1) - \wp_L(z_1) = \wp_L\left(-\frac{1}{2}\omega_1 + \omega_1\right) - \wp_L\left(-\frac{1}{2}\omega_1\right) = 0 = c_{\omega_1}.$$

Hence

$$\wp_L(z+\omega_1) = \wp_L(z), \text{ for all } z \in \mathbb{C} \setminus L.$$

Similarly,

$$\wp_L(z+\omega_2) = \wp_L(z), \text{ for all } z \in \mathbb{C} \setminus L.$$

Thus for all $\omega \in L$, we have

$$\wp_L(z+\omega) = \wp_L(z), \text{ for all } z \in \mathbb{C} \setminus L.$$

■

Lemma 5.1.7 Let $L \subset \mathbb{C}$ be a lattice, and $z_1, z_2 \in \mathbb{C}$ be two arbitrary points. Then

$$\wp_L(z_1) = \wp_L(z_2) \iff z_1 - z_2 \in L \text{ or } z_1 + z_2 \in L.$$

Proof. Let consider the function $(z \mapsto \wp_L(z) - \wp_L(z_1))$, it is an elliptic function of order 2. So, by Theorem 5.1.2 (iii), it has two zeros modulo L (or in Π), counted with multiplicities. These are obviously $[z_1] = [z_2]$ and $[z_1] = -[z_2]$. ■

5.2 Tori and elliptic curves

Here will show that a complex torus $\mathbb{C}/L$ is naturally isomorphic to the complex points of an elliptic curve.

Definition 5.6 Let $L \subset \mathbb{C}$ be a lattice, and $k \geq 3$ an integer. The **Eisenstein series** of weight k evaluated at L is given by

$$G_k(L) := \sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^k}.$$

We will sometimes denote $G_k(L)$ by G_k if there is no ambiguity about the lattice L. We note that when k is odd, $G_k(L) = 0$ since the terms for ω and $-\omega$ cancel out.

Lemma 5.2.1 Let $L \subset \mathbb{C}$ be a lattice. Then, for $0 < |z| < \min\{|\omega| : 0 \neq \omega \in L\}$,

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

Proof. When $|z| < |\omega|$,

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \omega^{-2}\left(\frac{1}{(1-(z/\omega))^2} - 1\right) = \omega^{-2}\left(\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^n}\right).$$

Therefore, for $|z|$ small enough, we have

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \sum_{n=1}^{\infty} (n+1)\frac{z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)\left(\sum_{\substack{\omega \in L \\ \omega \neq 0}} \frac{1}{\omega^{n+2}}\right) z^n,$$

and the result follows. ■

Theorem 5.2.2 Let $L \subset \mathbb{C}$ be a lattice. Let $\wp_L(z)$ be the Weierstrass $\wp$-function associated to L. Then we have

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

Proof. The Taylor expansion in Lemma 5.2.1 gives

$$\wp_L(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \cdots$$
$$\wp_L'(z) = -2z^{-3} + 6G_4 z + 20G_6 z^3 + \cdots.$$

By cubing the first equation, we get

$$\wp_L(z)^3 = z^{-6} + 9G_4 z^{-2} + 15G_6 + \cdots,$$

and by taking squares in the second, we have

$$\wp_L'(z)^2 = 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \cdots .$$

From this, we obtain the function

$$f(z) = \wp_L'(z)^2 - 4\wp_L(z)^3 + 60G_4\wp_L(z) + 140G_6 = c_1 z + c_2 z^2 + \cdots .$$

This is a power series with no constant term and no negative powers of z, hence it is holomorphic at $z = 0$ with $f(0) = 0$. But f is doubly periodic with its *only* possible poles being at those of $\wp_L(z)$ and $\wp_L'(z)$, i.e. , the points of L. Since it is holomorphic at $z = 0$, it is holomorphic everywhere. Therefore, by Theorem 5.1.2 (i), it is a constant function. In fact, f is identically zero since $f(0) = 0$. ■

Let $L \subset \mathbb{C}$ be a lattice. We will write $g_2 = 60\,G_4$ and $g_3 = 140\,G_6$.

Theorem 5.2.3 Let $L \subset \mathbb{C}$ be a lattice. Let $\wp_L(z)$ be the Weierstrass $\wp$-function associated to L, and let

$$E : y^2 = 4x^3 - g_2 x - g_3.$$

Then

(i) $16(g_2^3 - 27g_3^2) \neq 0$, so E is an elliptic curve over $\mathbb{C}$.

(ii) The map

$$\begin{aligned} \phi : \mathbb{C}/L &\to E(\mathbb{C}) \\ [z] &\mapsto \begin{cases} (\wp_L(z), \wp_L'(z)) & \text{if } z \notin L \\ \infty & \text{otherwise,} \end{cases} \end{aligned}$$

where $[z] = z + L$ is the equivalence class of z, is an isomorphism of groups.

Proof. (i) Since $\wp_L'(z)$ is doubly periodic and odd, we have

$$\wp_L'\left(\frac{\omega_1}{2}\right) = \wp_L'\left(\frac{\omega_1}{2} - \omega_1\right) = \wp_L'\left(-\frac{\omega_1}{2}\right) = -\wp_L'\left(\frac{\omega_1}{2}\right),$$

so $\wp_L'(\frac{\omega_1}{2}) = 0$, and $\frac{\omega_1}{2}$ is a zero of $\wp_L'(z)$. Similarly, one shows that $\frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$ are also zeros of $\wp_L'(z)$ inside the fundamental parallelogram Π. By Theorem 5.1.2 (iii), these are the only heroes of $\wp_L'(z)$ inside Π. Let

$$e_1 := \wp_L\left(\frac{\omega_1}{2}\right),\ e_2 := \wp_L\left(\frac{\omega_2}{2}\right),\ e_3 := \wp_L\left(\frac{\omega_1+\omega_2}{2}\right).$$

Then, e_1, e_2, e_3 are the only zeros of the cubic $4\wp_L(z)^3 - g_2\wp_L(z) - g_3$ inside Π, and they are distinct (by Lemma 5.1.7). So we have

$$\wp_L'(z)^2 = 4(\wp_L(z) - e_1)(\wp_L(z) - e_2)(\wp_L(z) - e_3),$$

and the discriminant of this cubic is

$$16(g_2^3 - 27g_3^2) = 4^2[(e_1 - e_2)(e_1 - e_3)(e_2 - e_3)]^2 \neq 0.$$

(ii) **Surjectivity.** Let $(x,y) \in E(\mathbb{C}) \setminus \{0\}$. Since $\wp_L$ is surjective, there exists $z \in \mathbb{C}$ such that $\wp_L(z) = x$. From the algebraic relation satisfied by the pair $(\wp_L(z), \wp_L'(z))$, we must have $\wp_L'(z) = \pm y$. So we have

$$(\wp_L(z), \wp_L'(z)) = (x,y) \text{ or } (\wp_L(-z), \wp_L'(-z)) = (x,y).$$

Injectivity. Let $z_1, z_2 \in \mathbb{C} \setminus L$ be such that $\wp_L(z_1) = \wp_L(z_2)$. By Lemma 5.1.7, $z_1 - z_2 \in L$ or $z_1 + z_2 \in L$. In the first case, we are done. So assume that $z_1 + z_2 \in L$. Then, we have $\wp_L'(z_1) = -\wp_L'(z_1)$, which implies that $\wp_L'(z_1) = 0$. Thus $2z_1 \in L$, and so

$$[z_1] = [-z_1] = [z_2].$$

Homomorphism. Let us consider three points

$$\begin{aligned} P_1 &= (x_1, y_1) = (\wp_L(z_1), \wp_L'(z_1)), \\ P_2 &= (x_2, y_2) = (\wp_L(z_2), \wp_L'(z_2)), \\ P_3 &= (x_3, y_3) = (\wp_L(z_3), -\wp_L'(z_3)), \end{aligned}$$

where $z_3 = -(z_1 + z_2)$. We assume that x_1, x_2 and x_3 are pairwise distinct. We will only prove the statement in this case: the general case follows applying continuity and l'Hôpital's rule.

Claim. The determinant

$$\begin{vmatrix} 1 & x_3 & -y_3 \\ 1 & x_2 & y_2 \\ 1 & x_1 & y_1 \end{vmatrix} = 0. \tag{5.3}$$

Proof of claim. Consider the function

$$f(z) := \begin{vmatrix} 1 & \wp_L(z) & \wp_L'(z) \\ 1 & x_2 & y_2 \\ 1 & x_1 & y_1 \end{vmatrix}.$$

It is of the form $f(z) = A + B\wp_L(z) + C\wp_L'(z)$, with $C = x_2 - x_1 = \wp_L(z_2) - \wp_L(z_1) \neq 0$. So f is an elliptic function of order 3, and it has two zeros located at z_1 and z_2. So by Theorem 5.1.2, (iv), the third zero is $z_3 = -(z_1 + z_2) \mod L$. ■

Since the determinant in (5.3) is zero, the points P_1, P_2, P_3 lie on the same line $y = mx + c$. The slope of this line is

$$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{\wp_L'(z_2) - \wp_L'(z_1)}{\wp_L(z_2) - \wp_L(z_1)}.$$

But the three points also lie on the elliptic curve E, so they all satisfy the cubic equation

$$(mx + c)^2 - 4x^3 + g_2 x + g_3 = 0.$$

So we must have

$$x_1 + x_2 + x_3 = \frac{m^2}{4}.$$

This means exactly that ϕ is a homomorphism. ■

The converse of the theorem above is true. Namely, we have the following result.

Theorem 5.2.4 Let $E : y^2 = 4x^3 - Ax - B$, with $A, B \in \mathbb{C}$, be an elliptic curve. Then there exist a lattice $L \subset \mathbb{C}$ such that $A = g_2(L)$, $B = g_3(L)$, and a group isomorphism $\phi : \mathbb{C}/L \simeq E(\mathbb{C})$.

The elements of the lattice L in Theorem 5.2.4 are called **periods** of E.

5.3 Torsion points.

Let E be an elliptic curve over $\mathbb{C}$, and $n \geq 1$ an integer. The n-torsion subgroup of E is the subgroup of $E(\mathbb{C})$ given by

$$E(\mathbb{C})[n] = \{P \in E(\mathbb{C}) : nP = 0\}.$$

Theorem 5.2.3 provides a very simple approach to studying these groups through the Weierstrass isomorphism $\mathbb{C}/L \simeq E(\mathbb{C})$. Let $P \in E(\mathbb{C})$ correspond to $[z] \in \mathbb{C}/L$. Then,

$$\begin{aligned} P \text{ is an } n\text{-torsion point} &\Leftrightarrow nP = 0 \Leftrightarrow n[z] = [nz] = 0 \in \mathbb{C}/L \\ &\Leftrightarrow nz \in L \Leftrightarrow nz = a\omega_1 + b\omega_2 \text{ with } a, b \in \mathbb{Z} \\ &\Leftrightarrow z = \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 \text{ with } \frac{a}{n}, \frac{b}{n} \in \mathbb{Q} \\ &\Leftrightarrow z \in \left\{ \frac{a}{n}\omega_1 + \frac{b}{n}\omega_2 : 0 \leq a, b \leq n-1 \right\}, \\ &\Leftrightarrow z \in \frac{1}{n}L/L \simeq \left(\frac{1}{n}\mathbb{Z}/\mathbb{Z}\right)^2. \end{aligned}$$

The set on the right has cardinality n^2. We deduce that $E(\mathbb{C})[n] \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$.

Example 5.3.0.1 $E(\mathbb{C})[2]$ consists of $0(\infty)$ and the three points $(e_1, 0), (e_2, 0)$ and $(e_3, 0)$ described during the proof of Theorem 5.2.3.

R If $K \subset \mathbb{C}$ is a subfield, then $E(K) \leq E(\mathbb{C})$ (subgroup). Thus $E(K)[n] \leq E(\mathbb{C})[n]$. This implies that $\#E(K)[n]$ divides n^2.

5.4 Elliptic curves over $\mathbb{R}$

We now apply the previous discussion to elliptic curve defined over $\mathbb{R}$. To this end, we need the following important fact:

Fact. Let E be an elliptic curve over $\mathbb{C}$, and L a lattice such that $\mathbb{C}/L \simeq E(\mathbb{C})$. Then E is defined over $\mathbb{R} \Leftrightarrow L = \overline{L}$, *i.e.,* $\omega \in L \Rightarrow \overline{\omega} \in L$.

So if E is defined over $\mathbb{R}$, we must have $\omega_1 \pm \overline{\omega}_1$, $\omega_2 \pm \overline{\omega}_2 \in L$. This implies that $2\mathrm{Re}(\omega_1)$, $2\mathrm{Re}(\omega_2)$, $2i\mathrm{Im}(\omega_1)$, $2i\mathrm{Im}(\omega_2) \in L$. We can assume that $\mathrm{Re}(\omega_1), \mathrm{Re}(\omega_2), \mathrm{Im}(\omega_1), \mathrm{Im}(\omega_2)$ are all positive. Also, we can assume that $\omega_1 \in \mathbb{R}$. Then $\mathrm{Re}(\omega_2) = 0$ or $\mathrm{Re}(\omega_2) = \frac{\omega_1}{2}$ since $\omega_1 \in \Pi$. Let $P \in E(\mathbb{C})$ correspond to $[z] \in \mathbb{C}/L$, where $z = s\omega_1 + t\omega_2$ with $0 \leq s, t < 1$. Then,

$$\begin{aligned} P \in E(\mathbb{R}) &\Leftrightarrow [z] \text{ is } \textit{real} \Leftrightarrow [z] \text{ is } \textit{fixed} \text{ by complex conjugation} \\ &\Leftrightarrow [z] = [\overline{z}] \Leftrightarrow z - \overline{z} \in L. \end{aligned}$$

Case 1. $\Delta < 0$. The lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\omega_1 \in \mathbb{R}$ and $\mathrm{Re}(\omega_2) = \frac{1}{2}\omega_1$.

In this case, we see that $i\mathrm{Im}(\omega_2) \notin L$, therefore

$$z - \bar{z} = t\,(2i\,\mathrm{Im}(\omega_2)) \in L \;\Leftrightarrow\; t = 0.$$

So

$$z = s\omega_1 \in \mathbb{R}, \;\; 0 \leq s < 1.$$

This means that $E(\mathbb{R})$ has one component, so as a group

$$E(\mathbb{R}) \simeq \mathbb{R}/\mathbb{Z}.$$

The n-torsion subgroup given by

$$E(\mathbb{R})[n] := \{P \in E(\mathbb{R}) : nP = 0\}$$

is cyclic of order n since

$$n(x+\mathbb{Z}) = nx + \mathbb{Z} = 0 \;\Leftrightarrow\; nx \in \mathbb{Z} \Rightarrow x = \frac{a}{n} \text{ with } a \in \mathbb{Z}.$$

Case 2. $\Delta > 0$. The lattice L has basis $\omega_1 \in \mathbb{R}, \omega_2 \in i\mathbb{R}$.

Here $z - \bar{z} = 2t\omega_2$. So

$$z - \bar{z} \in L \;\Leftrightarrow\; t = 0 \text{ or } t = \frac{1}{2}.$$

So we must have

(a) $z = s\omega_1 \in \mathbb{R}$, $0 \leq s < 1$, or

(b) $z = s\omega_1 + \frac{\omega_2}{2}$, $0 \leq s < 1$.

In this case, $E(\mathbb{R})$ has two components, so

$$E(\mathbb{R}) \simeq C_2 \times (\mathbb{R}/\mathbb{Z}).$$

The points on the non-identity component cannot have *odd* order. So for *n odd*, $E(\mathbb{R})[n]$ is again *cyclic* of order n. While for *n even* $E(\mathbb{R})[n] \simeq C_2 \times C_n$ which is **not** cyclic.

Rational functions and endomorphisms

Separable endomorphisms

Parallelogram identity and degree map

The endomorphism ring

Automorphisms of elliptic curves

6. Endomorphisms of elliptic curves

In this chapter, we study the endomorphism ring of an elliptic curve. We will assume through out that K is a field such that $\text{char}(K) \neq 2,3$, unless otherwise stated. This allows us to work only with elliptic curves in short Weierstrass equation: $E : y^2 = x^3 + Ax + B = f(x)$ an elliptic curve over K.

6.1 Rational functions and endomorphisms

Let E be an elliptic curves over K in short Weierstrass equation: $E : y^2 = x^3 + Ax + B = f(x)$. A **rational function** $R(x,y)$ on E is given by

$$R(x,y) = \frac{P(x,y)}{Q(x,y)} = \frac{a_0(x) + a_1(x)y + \cdots + a_r(x)y^r}{b_0(x) + b_1(x)y + \cdots + b_s(x)y^s},$$

where $P, Q \in \overline{K}[x,y]$ have no common factor and Q is not the zero-polynomial. Since all $(x,y) \in E(\overline{K})$ satisfy $y^2 = f(x)$, we can replace

(i) y^n by $f(x)^k$ when $n = 2k$ is even,

(ii) y^n by $f(x)^k y$ when $n = 2k+1$ is odd,

and obtain a rational function that gives the same values as $R(x,y)$ on $E(\overline{K})$. Therefore, we may assume that

$$R(x,y) = \frac{p_1(x) + p_2(x)y}{p_3(x) + p_4(x)y},$$

where $p_1(x), \ldots, p_4(x)$ are polynomials in $\overline{K}[x]$. Moreover, we can rationalise the denominator by multiplying the top and bottom by $p_3(x) - p_4(x)y$ and then replacing y^2 by $f(x)$ to get

$$R(x,y) = \frac{q_1(x) + q_2(x)y}{q_3(x)} = r_1(x) + r_2(x)y. \tag{6.1}$$

Hence, a rational function $R(x,y)$ on an elliptic curve E given in short Weierstrass equation is given by $R(x,y) = r_1(x) + r_2(x)y$, where $r_1(x)$ and $r_2(x)$ are rational functions. The rational function $R(x,y)$ is defined for all points where the denominators of $r_1(x)$ and $r_2(x)$ do not vanish.

Definition 6.1 Let E be an elliptic curve over a field K. An **endomorphism** of E is a homomorphism $\phi : E(\overline{K}) \to E(\overline{K})$ given by rational functions. In other words,

- $\phi(0) = 0$,
- $\phi(P+Q) = \phi(P) + \phi(Q)$,

and there are rational functions (i.e quotients of polynomials) $R_1(x,y), R_2(x,y)$ with coefficients in $\overline{K}$ such that $\forall P = (x,y) \in E(\overline{K})$:

$$\phi(x,y) = (R_1(x,y), R_2(x,y)).$$

Example 6.1.0.2 Let E be given by $y^2 = x^3 + Ax + B$, and let $\phi(P) = 2P$ (the multiplication by 2 map). Then ϕ is a homomorphism and we have

$$\phi(x,y) = (R_1(x,y), R_2(x,y))$$

where

$$R_1(x,y) = \left(\frac{3x^2+A}{2y}\right)^2 - 2x$$
$$R_2(x,y) = \left(\frac{3x^2+A}{2y}\right)\left(3x - \left(\frac{3x^2+A}{2y}\right)^2\right) - y$$

are obtained by using the **duplication formula**. Since ϕ is a homomorphism given by rational functions, it is an endomorphism of E.

Returning to Definition 6.1, let $\phi \in \mathrm{End}(E)$ and write it as

$$\phi(x,y) = (R_1(x,y), R_2(x,y)),$$

where $R_1(x,y) = r_1(x) + s_1(x)y$ and $R_2(x,y) = s_2(x) + r_2(x)y$.
Since ϕ is a homomorphism, we must have

$$\phi(-P) = -\phi(P) \Leftrightarrow \phi(x,-y) = -\phi(x,y) \Leftrightarrow \begin{cases} R_1(x,-y) = R_1(x,y) \\ \\ R_2(x,-y) = -R_2(x,y) \end{cases}$$

Therefore, we have $s_1(x) = s_2(x) = 0$. Therefore, there are rational functions $r_1(x), r_2(x)$ such that

$$\phi(x,y) = (r_1(x), r_2(x)y).$$

We can now show that ϕ is defined on all of $E(\overline{K})$. To this end, write $r_1(x) = p(x)/q(x)$ and $r_2(x) = s(x)/t(x)$ where $p(x)$ and $q(x)$ (resp. $s(x)$ and $t(x)$) have no common factor and $q(x)$ (resp. $t(x)$) is not the constant zero-polynomial.
If $q(x_0) = 0$ for some $P = (x_0, y_0)$, we set $\phi(P) = 0$. We need to show that $t(x_0) = 0$ when $q(x_0) = 0$, therefore the endomorphism ϕ is defined on all points in $E(\overline{K})$.
By definition, $\phi(x,y) = (r_1(x), r_2(x)y)$ is a point in $E(\overline{K})$, so we have

$$r_2(x)^2 y^2 = r_1(x)^3 + Ar_1(x) + B.$$

This gives

$$\frac{(x^3+Ax+B)s(x)^2}{t(x)^2} = \frac{u(x)}{q(x)^3} \implies (x^3+Ax+B)s(x)^2q(x)^3 = u(x)t(x)^2.$$

where

$$u(x) = p(x)^3 + Ap(x)q(x)^2 + Bq(x)^3.$$

Since $p(x)$ and $q(x)$ have no common factor, so do $u(x)$ and $q(x)$.
Now assume that $t(x_0) = 0$. Then, $s(x_0) \neq 0$ since $s(x)$ and $t(x)$ have no common factor. Since x_0 is a multiple root of $t(x)^2$, and the cubic x^3+Ax+B has distinct roots (as E is an elliptic curve), we must have $q(x_0) = 0$.

We will use the result below to check whether a map $\phi : E(\overline{K}) \to E(\overline{K})$ is a homomorphism.

Theorem 6.1.1 Let $\phi : E(\overline{K}) \to E(\overline{K})$ be a map given by rationals functions. Then ϕ is an endomorphism if and only if $\phi(0) = 0$.

Example 6.1.1.1 Let m be a non-zero integer. Then as in Example 6.1.0.2, one can show that the map

$$[m] : E(\overline{K}) \to E(\overline{K})$$

$$P \mapsto [m]P := \begin{cases} \underbrace{P+\cdots+P}_{m\text{times}} & \text{if } m > 0 \\ \underbrace{(-P)+\cdots+(-P)}_{m\text{times}} & \text{if } m < 0. \end{cases}$$

is an endomorphism.

Definition 6.2 The set of all endomorphisms of E, denoted by $\mathrm{End}(E)$, is a ring under the following addition and multiplication laws. For all $\phi, \psi \in \mathrm{End}(E)$, define $\phi + \psi$ and $\phi\psi$ by

- $(\phi + \psi)(P) = \phi(P) + \psi(P)$,
- $(\phi\psi)(P) = \phi(\psi(P))$,

for all $P \in E(\overline{K})$. We call $\mathrm{End}(E)$ the **endomorphism ring** of E. (We allow the zero map $\phi \equiv 0$ given by $\phi(P) = 0, \forall P$.)

Definition 6.3 Let $\phi \in \mathrm{End}(E)$ be given by $(r_1(x), r_2(x)y)$, where $r_1(x) = p(x)/q(x)$ with $p(x)$ and $q(x)$ having no common factor. We define the **degree**, of ϕ to be 0 if ϕ is identically zero and $\max\{\deg(p), \deg(q)\}$, otherwise. We denote it by $\deg(\phi)$.

Example 6.1.1.2 In Example 6.1.0.2, we saw that the map $[2]P = 2P$ is given by two rational functions R_1, R_2 where

$$R_1(x,y) = \left(\frac{3x^2+A}{2y}\right)^2 - 2x.$$

By replacing y^2 by x^3+Ax+B, we get

$$r_1(x) = \frac{(3x^2+A)^2 - 8x(x^3+Ax+B)}{4(x^3+Ax+B)} = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3+Ax+B)}.$$

Therefore, by definition, $\deg([2]) = 4$.

Definition 6.4 Let $\phi \in \mathrm{End}(E)$ be non-zero. We say that ϕ is **separable** if $r_1'(x)$ is not identically zero, i.e. if $p'(x)$ and $q'(x)$ are not both identically zero. Otherwise, we say that it is **inseparable**.

Example 6.1.1.3 In Example 6.1.1.2, the derivative of the denominator $q(x)$ is $q'(x) = 4(3x^2+A)$. This is non identically zero (even in characteristic 3, since in that case $A \neq 0$: indeed, E is an elliptic curve, so $\Delta = -4A^3 - 27B^2 \equiv -4A^3 \bmod 3$ is non-zero). Therefore, the multiplication by 2 map is separable, when $\mathrm{char}(K) \neq 2$.

Example 6.1.1.4 Let K be a field of characteristic $\mathrm{char}(K) = 2$, and let E be an elliptic curve over K given by

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

In that case, one can show that the map $[2]P = 2P$ is given by

$$[2]P = (r_1(x), R_2(x,y)),$$

where $r_1(x) = (x^4 + a_6)/x^2 = p(x)/q(x)$. We see that $p'(x) = 4x^3 = 0$ and $q'(x) = 2x = 0$ identically. Therefore, the map $[2]$ is inseparable.

6.2 Separable endomorphisms

In this section, we study separable endomorphisms. Among other things, we will show that a non-zero separable endomorphism is surjective. We start with a review of the basic properties of separable polynomials.

Definition 6.5 Let $g(x) \in K[x]$ be a polynomial. We say that $g(x)$ is **separable** if $g'(x)$ is not identically zero.

It follows that

(a) If $g(x)$ is a *separable irreducible* polynomial, then $g(x)$ has *distinct* roots.

(b) When $\mathrm{char}(K) = 0$, then every polynomial is separable, since the only polynomials whose derivatives are identically zero are the constant ones.

When $\mathrm{char}(K) = p$, we have the following lemma.

Lemma 6.2.1 Let K be a field of characteristic $p > 0$, and $g(x) \in K[x]$. Then $g(x)$ is inseparable if and only if it is of the form $g(x) = h(x^p)$ with $h(x) \in K[x]$.

Proof. Let $g(x) = \sum_{i=0}^{n} a_i x^i$; then $g'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. Therefore, $g'(x) \equiv 0$ if and only if $ia_i = 0$

for all $1 \leq i \leq n$. Hence, if and only if $p \mid i$ for all i such that $a_i \neq 0$. Therefore,

$$g(x) = \sum_{k=0}^{m} a_{kp} x^{kp} = \left(\sum_{k=0}^{m} a_{kp} (x^p)^k \right) = h(x^p).$$

■

By induction, using the above lemma, we see that a polynomial $g(x)$ is inseparable if and only if there is a separable polynomial $t(x) \in K[x]$ such that $g(x) = t(x^{p^k})$ for some positive integer k. We then define the **separable degree** of $g(x)$ by $\deg_s(g(x)) = \deg(t(x))$, and its **inseparable degree** by $\deg_i(g(x)) = p^k$.

Lemma 6.2.2 Let $g(x), h(x) \in K[x]$. Then, we have

(a) $\deg(g(x)) = \deg_s(g(x)) \deg_i(g(x))$.

(b) $\deg_s(g(h(x)) = \deg_s(g(x)) \deg_s(h(x))$ and $\deg_i(g(h(x)) = \deg_i(g(x)) \deg_i(h(x))$.

In particular $g(h(x))$ is separable if and only if $g(x)$ and $h(x)$ are both separable.

Proof. Immediate from definitions. ■

Let $\phi \in \mathrm{End}(E)$ be given by $(r_1(x), r_2(x)y)$, where $r_1(x) = p(x)/q(x)$ with $p(x)$ and $q(x)$ having no common factor. Definition 6.4 says that ϕ is separable if and only if either $p(x)$ or $q(x)$ is separable. From this, we immediately get the following corollary.

Corollary 6.2.3 Let $\phi, \psi \in \mathrm{End}(E)$ then

(i) $\deg(\phi\psi) = \deg(\phi)\deg(\psi)$.

(ii) $\deg_s(\phi\psi) = \deg_s(\phi)\deg_s(\psi)$.

(iii) $\deg_i(\phi\psi) = \deg_i(\phi)\deg_i(\psi)$.

In particular, $\phi\psi$ is separable if and only if both ϕ and ψ are separable.

The following result gives an important property of non-zero separable endomorphisms. Namely, that if $\phi \in \mathrm{End}(E)$ is separable, then the size of $\phi^{-1}(P)$ is $\deg(\phi)$ for all $P \in E(\overline{K})$.

Theorem 6.2.4 Let E be an elliptic curve over a field K, and $\phi \in \mathrm{End}(E)$ be non-zero. Then

(i) $\phi : E(\overline{K}) \to E(\overline{K})$ is surjective.

(ii) For all $Q \in E(\overline{K})$, let $\phi^{-1}(Q) := \{P \in E(\overline{K}) : \phi(P) = Q\}$. Then, we have

$$\#\phi^{-1}(Q) = \#\ker(\phi).$$

(iii) If ϕ is separable, then $\#\ker(\phi) = \deg(\phi)$.
Otherwise, $\#\ker(\phi) = \deg_s(\phi) < \deg(\phi)$.

Proof. Let $Q \in E(\overline{K})$. Assume that

$$\phi^{-1}(Q) = \{P \in E(\overline{K}) : \phi(P) = Q\}$$

is non-empty, and choose $P_0 \in \phi^{-1}(Q)$. Since ϕ is a group homomorphism, the map

$$\begin{aligned} \ker(\phi) &\to \phi^{-1}(Q) \\ P &\mapsto P + P_0 \end{aligned}$$

is a bijection. Thus every non-empty *fiber* $\phi^{-1}(Q)$ has the same cardinality as $\ker(\phi) = \phi^{-1}(0)$. So it is enough to prove that ϕ is surjective.

Strategy. Assume that ϕ is separable of $\deg(\phi) = m$. We write it as

$$\phi(x,y) = (r_1(x), r_2(x)y) = \left(\frac{a(x)}{c(x)}, \frac{b(x)}{d(x)}y\right),$$

where $a(x), b(x), c(x), d(x) \in \overline{K}[x]$ and $\gcd(a,c) = \gcd(b,d) = 1$, and we recall that by definition $\deg(\phi) = m = \max\{\deg(a), \deg(c)\}$.

Let $Q = (u,v) \in E(\overline{K})$. Then by definition, we have

$$\begin{aligned} \phi^{-1}(Q) &= \left\{(x,y) \in E(\overline{K}) : (r_1(x), r_2(x)y) = (u,v)\right\} \\ &= \left\{(x,y) \in E(\overline{K}) : \frac{a(x)}{c(x)} = u \text{ and } r_2(x)y = v\right\} \\ &= \left\{(x,y) \in E(\overline{K}) : uc(x) - a(x) = 0 \text{ and } y = \frac{v}{r_2(x)}\right\}. \end{aligned}$$

The later equality makes sense provided $r_2(x) \neq 0$. We will show that there is a *finite* and *explicit* set $S \subset E(\overline{K})$ such that, for all $Q \in E(\overline{K}) \setminus S$, the fiber $\phi^{-1}(Q)$ is given as above and that $\#\phi^{-1}(Q) = \deg(\phi)$. Namely, we will show, for $Q = (u,v) \notin S$, the polynomial $uc(x) - a(x)$ has m distinct roots. To this end, we consider the three sets:

$$\begin{aligned} S_1 &:= \left\{Q = (u,v) \in E(\overline{K}) : u = 0 \text{or} \deg(c(x)u - a(x)) < \deg(\phi)\right\}, \\ S_2 &:= \left\{Q = (u,v) \in E(\overline{K}) : \exists x \in \overline{K} \text{with} u = r_1(x) \text{and} r_1'(x) = 0\right\}, \\ S_3 &:= \left\{Q = (u,v) \in E(\overline{K}) : \exists x \in \overline{K} \text{with} u = r_1(x) \text{and} r_2(x) = 0\right\}. \end{aligned}$$

It is not hard to see that both S_1 and S_3 are finite. Also, since ϕ is separable, $r_1'(x)$ is not identically zero; and so S_2 is finite as well.

Let $S := S_1 \cup S_2 \cup S_3$ and take $Q = (u,v) \in E(\overline{K}) \setminus S$. Then $uc(x) - a(x)$ is separable of degree $\deg(\phi)$, and so has distinct roots. Indeed, if x_0 is a multiple root, then

$$\left.\begin{aligned} uc(x_0) - a(x_0) &= 0 \\ uc'(x_0) - a'(x_0) &= 0 \end{aligned}\right\} \Rightarrow u(ac' - a'c)(x_0) = 0,$$

which implies that $(ac' - a'c)(x_0) = 0$. But $ac' - a'c$ is the numerator of $r_1'(x)$, hence is not identically 0. So $ac' - a'c$ has finitely many roots giving the points in S_2, which we already excluded. So $uc(x) - a(x)$ has $\deg(\phi)$ distinct roots $x_1, \ldots, x_m$. Since $(u,v) \notin S_3$, $r_2(x_i) \neq 0$, and we can solve for $y_i = v/r_2(x_i)$ for all $i = 1, \ldots, m$. Thus Q has exactly $\deg(\phi)$ preimages.

Since we know that each

$$\#\phi^{-1}(Q) = \begin{cases} 0, & \text{if } Q \notin \operatorname{im}(\phi) \\ \#\ker(\phi), & \text{if } Q \in \operatorname{im}(\phi), \end{cases}$$

and that *almost* all $\phi^{-1}(Q)$ have cardinality $\deg(\phi)$, it follows that

$$\#\phi^{-1}(Q) = \deg(\phi), \forall Q.$$

(Note that since $E(\overline{K})$ is an infinite abelian group, the complement of $\mathrm{im}(\phi)$ would be infinite if ϕ were not surjective.)
If ϕ is not separable, then the number of distinct roots of $uc(x) - a(x)$ is $\deg_s(\phi)$ (away from a finite set). The argument then proceeds as before. ■

We now apply this result to multiplication maps.

Proposition 6.2.5 The map $\mathbb{Z} \to \mathrm{End}(E)$, $m \mapsto [m]$, is an injective ring homomorphism.

Proof. From the definition, we see that, for $m, n \in \mathbb{Z}$,

$$[m+n] = [m] + [n]$$
$$[mn] = [m][n].$$

So the map is a homomorphism.
For the injectivity, we need to show that $m \neq 0 \Rightarrow [m] \neq 0$. It is enough to show that $[-1] \neq 0$, $[2] \neq 0$ and $[m] \neq 0$ when $m > 1$ is odd.
By definition $[-1] : (x, y) \mapsto (x, -y)$ so $\deg([-1]) = 1$. Also, from Example 6.1.1.2, we know that $\deg([2]) = 4$, so both $[-1]$ and $[2]$ are non-zero. Finally, let $m = 2k+1$ be odd, and assume that $\mathrm{char}(K) \neq 2$. Let $P \in E(\overline{K})$ be such that $2P = 0$ but $P \neq 0$ (i.e. $0 \neq P \in \ker([2])$). (There are 3 such points since $[2]$ is separable.) Then,

$$mP = (2k+1)P = P \neq 0.$$

0 Hence $[m] \neq 0$. ■

R The above proposition implies that the endomorphism ring $\mathrm{End}(E)$ of an elliptic curve is a **characteristic zero** ring.

Separability criterion

We will now give a very useful criterion for an endomorphism to be separable. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve, with $a, b \in K$ (recall that $\mathrm{char}(K) \neq 2, 3$). We can do implicit differentiation on E; thus

$$2yy' = 2y\frac{dy}{dx} = 3x^2 + a \text{ and } y' = \frac{dy}{dx} = \frac{3x^2+a}{2y}.$$

We can also differentiate any rational function $R(x, y)$ on E:

$$\frac{d}{dx}R(x,y) = \frac{\partial}{\partial x}R(x,y) + \frac{\partial}{\partial y}R(x,y)\frac{dy}{dx}.$$

Lemma 6.2.6 Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E. Set $P_3 = (x_3, y_3) = P_1 + P_2$. If we view x_3, y_3 as rational functions in (the indeterminates) x_1, x_2, y_1, y_2, then

$$\frac{\partial x_3}{\partial x_1} = \frac{y_3}{y_1} \text{ and } \frac{\partial x_3}{\partial x_2} = \frac{y_3}{y_2}.$$

Proof. This is a long but straightforward calculation, which uses the addition law formulas: for example if $x_1 \neq x_2$:

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2$$
$$y_3 = -y_1 - \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_3 - x_1).$$

■

Definition 6.6 Let E be an elliptic curve given by a long Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. The **invariant differential form** ω_E is the differential form given by:

$$\omega_E = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 - a_1y + 2a_2x + a_4}.$$

If E is given by a medium or a short Weierstrass equation then

$$\omega_E = \frac{dx}{2y}.$$

The following theorem provides a very useful criterion of separability and characterize the invariant differential.

Theorem 6.2.7 Let $E : y^2 = x^3 + ax + b$ over a field K with $\mathrm{char}(K) \neq 2, 3$. Then, we have the followings.

(i) If $P_3 = P_1 + P_2$, where $P_i = (x_i, y_i)$, then

$$\frac{\partial x_3}{\partial x_1} = \frac{y_3}{y_1} \text{ and } \frac{\partial x_3}{\partial x_2} = \frac{y_3}{y_2}.$$

(ii) If $Q = [m]P$ with $P = (x, y)$ and $Q = (x_m, y_m)$ then

$$\frac{dx_m}{dx} = m\frac{y_m}{y}.$$

(iii) More generally, if $\alpha \in \mathrm{End}(E)$ and $\alpha(P) = (x_\alpha, y_\alpha)$, then there exists a constant $c_\alpha \in \overline{K}$ such that

$$\frac{dx_\alpha}{dx} = c_\alpha\frac{y_\alpha}{y}.$$

(iv) The map $\mathrm{End}(E) \to \overline{K}$ given by $\alpha \mapsto c_\alpha$ is a ring homomorphism.

(v) $c_\alpha = 0 \Leftrightarrow \alpha$ is inseparable. In particular, for all non zero $m \in \mathbb{Z}$, the multiplication by m map $[m]$ is always separable in characteristic 0, and it is separable in characteristic p if and only if $p \nmid m$.

Proof. (i) is a tedious calculation (see the lemma above and assignment); (ii) follows by induction on $m \geq 1$. We will not prove (iii) but only observe that the right formulation of this statement is in terms of the invariant differential form. Consider the differential form

$\omega_E = \frac{dx}{2y}$ on E. Then (i) simply means that ω_E is translation invariant, whereas (iii) implies that $\omega_E \circ \alpha = c_\alpha \omega_E$, where $c_\alpha \in \overline{K}$.
To prove (iv), we first observe that

- If α is the zero endomorphism in $\mathrm{End}(E)$ then $c_\alpha = 0$.
- If $\alpha = 1$ is the identity map in $\mathrm{End}(E)$ then $c_\alpha = 1$.

Next, let $\beta \in \mathrm{End}(E)$ be another endomorphism. By writing

$$(\alpha+\beta)(x,y) = (x_{\alpha+\beta}, y_{\alpha+\beta}),$$

and using (iii), we get

$$\frac{dx_{\alpha+\beta}}{dx} = c_{\alpha+\beta}\frac{y_{\alpha+\beta}}{y}.$$

The addition law on $\mathrm{End}(E)$ means that

$$(\alpha+\beta)(x,y) = \alpha(x,y) + \beta(x,y),$$

which implies that

$$(x_{\alpha+\beta}, y_{\alpha+\beta}) = (x_\alpha, y_\alpha) + (x_\beta, y_\beta).$$

By applying (i) to this, we get

$$\frac{\partial x_{\alpha+\beta}}{\partial x_\alpha} = \frac{y_{\alpha+\beta}}{y_\alpha} \text{ and } \frac{\partial x_{\alpha+\beta}}{\partial x_\beta} = \frac{y_{\alpha+\beta}}{y_\beta}.$$

By using the chain rule and the property (iii), we see that

$$\frac{dx_{\alpha+\beta}}{dx} = \frac{\partial x_{\alpha+\beta}}{\partial x_\alpha}\frac{dx_\alpha}{dx} + \frac{\partial x_{\alpha+\beta}}{\partial x_\beta}\frac{dx_\beta}{dx} = \frac{y_{\alpha+\beta}}{y_\alpha}c_\alpha\frac{y_\alpha}{y} + \frac{y_{\alpha+\beta}}{y_\beta}c_\beta\frac{y_\beta}{y} = (c_\alpha + c_\beta)\frac{y_{\alpha+\beta}}{y}.$$

Combining this with the first identity, we get $c_{\alpha+\beta} = c_\alpha + c_\beta$.
For the composition of endomorphisms, we have

$$\begin{aligned}\alpha\beta(x,y) &= (x_{\alpha\beta}, y_{\alpha\beta}) = \alpha(x_\beta, y_\beta) \\ &= \left(x_\alpha(x_\beta), y_\alpha(x_\beta, y_\beta)\right).\end{aligned}$$

This gives

$$x_{\alpha\beta} = x_\alpha(x_\beta) \text{ and } y_{\alpha\beta} = y_\alpha(x_\beta, y_\beta).$$

Applying (iii) to $(x_{\alpha\beta}, y_{\alpha\beta})$ yields

$$\frac{dx_{\alpha\beta}}{dx} = c_{\alpha\beta}\frac{y_{\alpha\beta}}{y} = c_{\alpha\beta}\frac{y_\alpha(x_\beta,y_\beta)}{y} = c_{\alpha\beta}\frac{y_\alpha(x_\beta,y_\beta)}{y_\beta}\frac{y_\beta}{y}.$$

Multiplying through by $c_\alpha c_\beta$ and rearranging, we get

$$c_\alpha c_\beta \frac{dx_{\alpha\beta}}{dx} = c_{\alpha\beta}\left(c_\alpha\frac{y_\alpha(x_\beta,y_\beta)}{y_\beta}\right)\left(c_\beta\frac{y_\beta}{y}\right) = c_{\alpha\beta}x'_\alpha(x_\beta)\frac{dx_\beta}{dx},$$

where the latter equality uses (iii). From this, we conclude that

$$c_{\alpha\beta} = c_\alpha c_\beta,$$

since by the chain rule

$$\frac{dx_{\alpha\beta}}{dx} = x'_\alpha(x_\beta)\frac{dx_\beta}{dx}.$$

Finally, we only need to prove (v) when $\mathrm{char}(K) = p > 0$, since every endomorphism is separable in characteristic 0 by definition. To this end, write

$$\alpha(x,y) = (x_\alpha, y_\alpha) = (r_1(x), r_2(x)y).$$

Then,

$$\alpha \text{ is inseparable } \Leftrightarrow r'_1(x) \equiv 0 \Leftrightarrow x'_\alpha \equiv 0.$$

But

$$x'_\alpha(x) = \frac{dx_\alpha}{dx} = c_\alpha\frac{y_\alpha}{y} \Rightarrow c_\alpha = \frac{x'_\alpha(x)}{y_\alpha/y}.$$

Thus $c_\alpha = 0 \Leftrightarrow x'_\alpha(x) \equiv 0$. ■

Corollary 6.2.8 If $\mathrm{char}(K) = 0$, then the map $\alpha \mapsto c_\alpha$ is an embedding $\mathrm{End}(E) \hookrightarrow \overline{K}$. In particular, $\mathrm{End}(E)$ is **commutative**.

Proof. The kernel of this map is

$$\ker(\alpha \mapsto c_\alpha) := \{\alpha \in \mathrm{End}(E) : c_\alpha = 0\} = \{0\}$$

since the only inseparable endomorphism in characteristic zero is the zero map. ■

6.3 The parallelogram identity and the degree map

Theorem 6.3.1 — Parallelogram Identity. Let $\alpha, \beta \in \mathrm{End}(E)$. Then

$$\deg(\alpha+\beta) + \deg(\alpha-\beta) = 2\deg(\alpha) + 2\deg(\beta).$$

Proof. Since $\deg(0) = 0$, $\deg([-1]) = 1$ and $\deg([2]) = 4$, the statement is clear when:

- $\beta = 0$
- $\alpha = 0$ since $\deg(-\beta) = \deg([-1])\deg(\beta)$
- $\alpha = \beta$ since $\deg(2\alpha) = \deg([2])\deg(\alpha) = 4\deg(\alpha)$
- $\alpha = -\beta$ for the same reasons as above.

Claim. It is enough to show that

$$\deg(\alpha+\beta) + \deg(\alpha-\beta) \leq 2\deg(\alpha) + 2\deg(\beta)\ \forall \alpha, \beta \in \mathrm{End}(E). \tag{6.2}$$

Applying this to both $\alpha \pm \beta$ (in place of α, β), we get

$$\deg((\alpha+\beta)+(\alpha-\beta)) + \deg((\alpha+\beta)-(\alpha-\beta)) \leq 2\deg(\alpha+\beta) + 2\deg(\alpha-\beta)$$

which is the same as

$$\deg(2\alpha) + \deg(2\beta) \leq 2\deg(\alpha+\beta) + 2\deg(\alpha-\beta).$$

This gives the reverse inequality

$$2\deg(\alpha)+2\deg(\beta)\leq \deg(\alpha+\beta)+\deg(\alpha-\beta).$$

To prove (6.2), let $P=(x,y)\in E(\overline{K})$, and set

$$\begin{aligned}
P_1 &= \alpha(x,y)=(x_1,y_1)\\
P_2 &= \beta(x,y)=(x_2,y_2)\\
P_3 &= (\alpha+\beta)(P)=P_1+P_2=(x_3,y_3)\\
P_4 &= (\alpha-\beta)(P)=P_1-P_2=(x_4,y_4).
\end{aligned}$$

The x_i are all rational functions in x. Write each $x_i=\frac{a_i(x)}{b_i(x)}$, where $a_i(x)$ and $b_i(x)$ have no common factor, and let $d_i=\max\{\deg(a_i(x)),\deg(b_i(x))\}$. Then we need to prove that

$$d_3+d_4\leq 2d_1+2d_2.$$

The following identity holds:

$$(x_1-x_2)^2x_3=(x_1x_2+A)(x_1+x_2)-2y_1y_2+2B. \tag{6.3}$$

Applying this to the point P_4, where we recall that

$$P_4=P_1-P_2=P_1+(-P_2)\Leftrightarrow (x_4,y_4)=(x_1,y_1)+(x_2,-y_2),$$

we get

$$(x_1-x_2)^2x_4=(x_1x_2+A)(x_1+x_2)+2y_1y_2+2B. \tag{6.4}$$

This gives the two identities

$$\begin{aligned}
(x_1-x_2)^2(x_3+x_4) &= 2(x_1x_2+A)(x_1+x_2)+4B\\
(x_1-x_2)^2x_3x_4 &= (x_1x_2-A)^2-4B(x_1+x_2),
\end{aligned}$$

where the first one follows by adding (6.3) and (6.4), and the second one by multiplying them. Interpreting these two identities in projective coordinates yields

$$\begin{aligned}
[1:x_3+x_4:x_3x_4] &= [(x_1-x_2)^2:(x_1-x_2)^2(x_3+x_4):(x_1-x_2)^2x_3x_4]\\
&= [(x_1-x_2)^2:2(x_1x_2+A)(x_1+x_2)+4B:(x_1x_2-A)^2-4B(x_1+x_2)].
\end{aligned} \tag{6.5}$$

We homogenize each x_i by writing

$$X_i=\frac{Z^{d_i}a_i(X/Z)}{Z^{d_i}b_i(X/Z)}=\frac{U_i(X,Z)}{V_i(X,Z)}.$$

The U_i,V_i are homogeneous polynomial of degree d_i in the variables X,Z, with no common factor. By replacing this into (6.5) and clearing denominators, we get

$$[V_3V_4:U_3V_4+U_4V_3:U_3U_4]=[F:G:H],$$

where

$$\begin{aligned}
F &:= (U_1V_2-U_2V_1)^2,\\
G &:= 2(U_1U_2+AV_1V_2)(U_1V_2+U_2V_1)+4BV_1^2V_2^2,\\
H &:= (U_1U_2-AV_1V_2)^2-4B(U_1V_1+U_2V_2)V_1V_2.
\end{aligned}$$

Every term on the left hand side has degree d_3+d_4, and every term on the right hand side has degree $2d_1+2d_2$. The polynomials on the left hand side are coprime. Suppose W is an irreducible polynomial such that $W \mid V_3V_4$ and $W \mid U_3U_4$. Then

$$\begin{cases} W \mid V_3 \text{ or } W \mid V_4 \\ W \mid U_3 \text{ or } W \mid U_4 \end{cases}$$

So either W divides both V_3 and U_4 or W divides both V_4 and U_3. But

$$W \text{ divides } V_3, U_4 \Rightarrow W \nmid U_3 \text{ and } W \nmid V_4.$$

Hence $W \nmid (U_3V_4+U_4V_3)$.
Let W be the greatest common divisor of F, G and H. Then we have

$$[V_3V_4 : U_3V_4+U_4V_3 : U_3U_4] = [WF_1 : WG_1 : WH_1] = [F_1 : G_1 : H_1],$$

where $\gcd(F_1, G_1, H_1) = 1$. It then follows that

$$d_3+d_4 = 2d_1+2d_2-\deg(W) \leq 2d_1+2d_2.$$

■

We can now determine the degree of the multiplication-by-m, for $m \in \mathbb{Z}$, as the first application of the Parallelogram Identity.

Corollary 6.3.2 Let $m \in \mathbb{Z}$, then the degree of the multiplication by m map is $\deg([m]) = m^2$.

Proof. This is true for $m = 0, \pm 1, 2$. It is enough to prove this for $m > 0$ since we have

$$\deg([-m]) = \deg([-1][m]) = \deg([-1])\deg([m]) = \deg([m]).$$

We do this by induction. Assume that $\deg([n]) = n^2$ for all $1 \leq n \leq m$, then

$$\deg([m+1])+\deg([m-1]) = 2\deg([m])+2\deg([1]),$$

and so

$$\deg([m+1]) = 2m^2+2-(m-1)^2 = (m+1)^2.$$

■

Lemma 6.3.3 Let A be an abelian group, and F a field such that $\text{char}(F) \neq 2$. Let $Q : A \to F$ be a map such that

$$Q(x+y)+Q(x-y) = 2Q(x)+2Q(y),$$

and put

$$B(x,y) = \frac{1}{2}(Q(x+y)-Q(x)-Q(y)) \ \forall x,y \in A.$$

Then B is a symmetric bilinear form from A to F, i.e. it satisfies the conditions:

(a) $B(0,0) = 0$.

(b) $B(x+x',y) = B(x,y)+B(x'y), \ \forall x,x',y \in A$.

(c) $B(x,y) = B(y,x), \ \forall x,y \in A$.

Proof. To prove (a), we observe that $Q(0) = 0$. Indeed,

$$Q(0) + Q(0) = 2Q(0) + 2Q(0) \Rightarrow 2Q(0) = 0 \Rightarrow Q(0) = 0.$$

The symmetry condition (c) follows from the definition and the fact that A is abelian. We only need to prove (b), but we leave this as an exercise. ■

Next, for $\alpha, \beta \in \mathrm{End}(E)$, we define

$$\langle \alpha, \beta \rangle := \frac{1}{2} \left(\deg(\alpha + \beta) - \deg(\alpha) - \deg(\beta) \right).$$

Proposition 6.3.4 The map

$$\begin{aligned} \mathrm{End}(E) \times \mathrm{End}(E) &\to \mathbb{Q} \\ (\alpha, \beta) &\mapsto \langle \alpha, \beta \rangle \end{aligned}$$

is a positive definite symmetric bilinear form, *i.e.*, $\langle \alpha, \alpha \rangle \geq 0$, and $\langle \alpha, \alpha \rangle = 0 \Leftrightarrow \alpha = 0$.

Proof. The form $\langle \, , \, \rangle$ is symmetric bilinear by Lemma 6.3.3 and the properties of the degree map. It is positive definite because $\deg(\alpha) \geq 0$ for all $\alpha \in \mathrm{End}(E)$. ■

Proposition 6.3.5 Let $\alpha, \beta \in \mathrm{End}(E)$. Then, for all $m, n \in \mathbb{Z}$, we have

$$\deg(m\alpha + n\beta) = m^2 \deg(\alpha) + 2mn\langle \alpha, \beta \rangle + n^2 \deg(\beta).$$

Proof. This follows from the easy calculation

$$\deg(m\alpha + n\beta) = \langle m\alpha + n\beta, m\alpha + n\beta \rangle = m^2 \deg(\alpha) + 2mn\langle \alpha, \beta \rangle + n^2 \deg(\beta).$$

■

Corollary 6.3.6 — Cauchy-Schwartz. Let $\alpha, \beta \in \mathrm{End}(E)$, then

$$\langle \alpha, \beta \rangle^2 \leq \deg(\alpha) \deg(\beta).$$

Proof. For $\alpha = 0$ or $\beta = 0$, both sides of the equality are zero. Otherwise, consider the map

$$\begin{aligned} \mathbb{Z} \times \mathbb{Z} &\to \mathbb{Q} \\ (m, n) &\mapsto \deg(m\alpha + n\beta) = m^2 \deg(\alpha) + 2mn\langle \alpha, \beta \rangle + n^2 \deg(\beta). \end{aligned}$$

By Proposition 6.3.4, this is a symmetric positive definite bilinear form given by the matrix

$$M := \begin{pmatrix} \deg(\alpha) & \langle \alpha, \beta \rangle \\ \langle \alpha, \beta \rangle & \deg(\beta) \end{pmatrix}.$$

It is not hard to see that this form is positive definite if and only if the form

$$\begin{aligned} \mathbb{Q} \times \mathbb{Q} &\to \mathbb{Q} \\ (x, y) &\mapsto (x, y) M (x, y)^T \end{aligned}$$

is positive definite. Therefore, its discriminant must be positive, i.e.

$$\langle \alpha, \beta \rangle^2 \leq \deg(\alpha) \deg(\beta).$$

■

6.4 The endomorphism ring

In this section , we use the degree map to derive further properties of the endomorphism ring $\mathrm{End}(E)$.

Proposition 6.4.1 Let $\alpha \in \mathrm{End}(E)$. Then α satisfies the quadratic equation $\alpha^2 - t\alpha + d = 0$, where $t = 2\langle\alpha, 1\rangle$ and $d = \deg(\alpha)$.

Proof. It is enough to show that $\deg(\alpha^2 - t\alpha + d) = 0$. But

$$\begin{aligned}
\deg(\alpha^2 - t\alpha + d) &= \langle \alpha^2 - t\alpha + d, \alpha^2 - t\alpha + d\rangle \\
&= \langle \alpha^2, \alpha^2\rangle + t^2\langle\alpha,\alpha\rangle + d^2 - 2t\langle\alpha^2,\alpha\rangle + 2d\langle\alpha^2,1\rangle - 2td\langle\alpha,1\rangle \\
&= \deg(\alpha^2) + t^2\deg(\alpha) + d^2 - 2t\langle\alpha^2,\alpha\rangle + 2d\langle\alpha^2,1\rangle - 2td\langle\alpha,1\rangle \\
&= \deg(\alpha)^2 + t^2\deg(\alpha) + d^2 - 2t\langle\alpha^2,\alpha\rangle + 2d\langle\alpha^2,1\rangle - 2td\langle\alpha,1\rangle \\
&= d^2 + t^2 d + d^2 - 2t\langle\alpha^2,\alpha\rangle + 2d\langle\alpha^2,1\rangle - t^2 d \\
&= 2d^2 - 2t\langle\alpha^2,\alpha\rangle + 2d\langle\alpha^2,1\rangle \\
&= 2d^2 - 2t\langle\alpha^2,\alpha\rangle - 2d\langle\alpha^2,-1\rangle.
\end{aligned}$$

It is not hard to see that

$$\begin{aligned}
\langle\alpha\beta,\beta\rangle &= \frac{1}{2}\left(\deg(\alpha\beta+\beta) - \deg(\alpha\beta) - \deg(\beta)\right) \\
&= \frac{1}{2}\left(\deg(\beta)\deg(\alpha+1) - \deg(\alpha)\deg(\beta) - \deg(\beta)\right) \\
&= \frac{1}{2}\deg(\beta)\left(\deg(\alpha+1) - \deg(\alpha) - 1\right) \\
&= \deg(\beta)\langle\alpha,1\rangle.
\end{aligned}$$

In particular,

$$2\langle\alpha^2,\alpha\rangle = 2\deg(\alpha)\langle\alpha,1\rangle = td.$$

Next,

$$\begin{aligned}
2\langle\alpha^2,-1\rangle &= \deg(\alpha^2-1) - \deg(\alpha^2) - 1 = \deg((\alpha+1)(\alpha-1)) - \deg(\alpha^2) - 1 \\
&= \deg(\alpha+1)\deg(\alpha-1) - \deg(\alpha)^2 - 1 \\
&= \left(\deg(\alpha) + 2\langle\alpha,1\rangle + 1\right)\left(\deg(\alpha) - 2\langle\alpha,1\rangle + 1\right) - d^2 - 1 \\
&= (d+t+1)(d-t+1) - d^2 - 1 = ((d+1)^2 - t^2) - d^2 - 1 \\
&= 2d - t^2.
\end{aligned}$$

Replacing this back, we get

$$\deg(\alpha^2 - t\alpha + d) = 2d^2 - t(td) - d(2d - t^2) = 0$$

■

We can now summarize what we have learned about endomorphism rings of elliptic curves. We already showed the followings:

- $\mathrm{End}(E)$ is a characteristic zero ring since $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$.
- The map $(\mathrm{End}(E) \to \overline{K}, \alpha \mapsto c_\alpha)$ is an injection when $\mathrm{char}(K) = 0$.

- $\mathrm{End}(E)$ has no zero-divisors, i.e. $\alpha,\beta \in \mathrm{End}(E)$ and $\alpha\beta = 0 \implies \alpha = 0$ or $\beta = 0$. Indeed, $\deg(\alpha\beta) = \deg(\alpha)\deg(\beta)$ and $\deg(\alpha) = 0 \iff \alpha = 0$.
- Every $\alpha \in \mathrm{End}(E)$ is at worst quadratic over $\mathbb{Z}$.

When $\mathrm{char}(K) = 0$ this forces $\mathrm{End}(E)$ to be isomorphic to

- $\mathbb{Z}$ (typical case), or
- an *order* $\mathscr{O}$ in an imaginary quadratic field, i.e. $\mathscr{O} = \mathbb{Z}[\alpha] \subset \mathbb{Q}(\sqrt{-D})$, where D is a positive integer, and α satisfies a monic polynomial with integer coefficients. (E.g. $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-5}]$.) This is called the CM case or **complex multiplication**.

Example 6.4.1.1 Let $K = \mathbb{Q}(i)$, where $i^2 = -1$, and let E be the curve given by $y^2 = x^3 + x$. Then, the map $\alpha : (x,y) \mapsto (-x, iy)$ is an endomorphism such that $\alpha^2 = -1$ since

$$\alpha^2(x,y) = (x,-y) = [-1](x,y).$$

One can show that $\mathrm{End}(E) \cong \mathbb{Z}[i]$.

6.5 Automorphisms of elliptic curves

We now turn to the special case of the isomorphisms of a given elliptic curve onto itself.

Definition 6.7 Let $E : y^2 = x^3 + Ax + B$, with $A, B \in K$, be an elliptic curve. An **automorphism** of E is an isomorphism of E onto itself. The set of automorphisms of E form a group, which we denote by $\mathrm{Aut}(E)$.

The following theorem show that $\mathrm{Aut}(E)$ is rather small (let us remark that K is of characteristic different from 2 and 3).

Theorem 6.5.1 Let $E : y^2 = x^3 Ax + B$, with $A, B \in K$, be an elliptic curve. Then we have

(i) $\mathrm{Aut}(E) \simeq \mathbb{Z}/2\mathbb{Z}$ if $j(E) \neq 0, 1728$.

(ii) $\mathrm{Aut}(E)$ is a cyclic group of order 6 if $j(E) = 0$.

(iii) $\mathrm{Aut}(E)$ is a cyclic group of order 4 if $j(E) = 1728$.

For any elliptic curve E, not necessarily in short Weierstrass equation and in any characteristic (hence, also in characteristic 2), an automorphism α is an endomorphism of degree 1 which has an inverse, i.e. an isomorphism of the elliptic curve onto itself. In general, an automorphism is a map of the form

$$\alpha(x,y) = (ax + b, cy + dx + e)$$

for all $(x,y) \in E(\overline{K})$ where $a,b,c,d,e \in \overline{K}$ which is invertible: this gives restrictions on the coefficients a,b,c,d,e. The inverse map is given by

$$(x,y) \to \left(\frac{x+b}{a}, \frac{y + \frac{dx}{a} + \frac{db}{a} + e}{c} \right),$$

so in particular α is an automorphism if and only if $a, c \neq 0$. If E is given in short Weierstrass equation and the characteristic of K is not 2 or 3 then we can express α as an isomorphism, like in Chapter 4.

j-**invariant characteristic** 2 **and** 3
Elliptic curves in characteristic 2
The j-invariant in characteristic 3

Isomorphism classes

The Frobenius endomorphism

Hasse's Inequality

Endomorphism ring

7. Elliptic Curves over finite fields

In this chapter we will focus on elliptic curves over finite fields and prove one of the most important results in this theory: the Hasse-Weil inequality. In order to do so, we will study the Frobenius endomorphism which is the simplest example of an inseparable endomorphism.
We will also complete the definition of j-invariant in the cases excluded in Chapter 3, that is when the field K has characteristic 2 or characteristic 3.

7.1 j-invariant characteristic 2 and 3

7.1.1 Elliptic curves in characteristic 2

In the previous chapters we have been mostly using elliptic curves E over K given by short Weierstrass equations instead of long Weierstrass equations: when the field K has characteristic different from 2 and 3, we have shown that there exists a change of coordinates from a long Weierstrass equation to a short Weierstrass equation. If the field K has characteristic 2, the formulas given do not apply. In this section we sketch what happens in this case.

For the remaining of this section we will assume $\mathrm{char}(K) = 2$.

First let us observe that the short Weierstrass equation gives a singular curve. Let C be the curve $y^2 = x^3 + Ax + B$ defined over K and let $g(x,y) = y^2 - x^3 - Ax - B$, then $\frac{\partial g}{\partial y} = 2y \equiv 0$ and $\frac{\partial g}{\partial x} = -3x^2 - A \equiv x^2 + A$. For any $x_0 \in K$ such that $x^2 + A = 0$, let y_0 be the square root of $x_0^3 + Ax_0 + B$. The point (x_0, y_0) lies on the curve C and it is a singular point since $\frac{\partial g}{\partial y}(y_0) = \frac{\partial g}{\partial x}(x_0) = 0$.

Let E be an elliptic curve over K given by a long Weierstrass equation:

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

with $a_1, a_2, a_3, a_4, a_6 \in K$. There are two cases we will consider, depending on the coefficient a_1.

Case 1. Let us suppose that a_1 is not zero, then the change of coordinates:

$$\begin{cases} x = a_1^2x_1 + \frac{a_3}{a_1} \\ y = a_1^3y_1 + a_1^{-3}(a_1^2a_4 + a_3^2). \end{cases}$$

gives the following equation: $y_1^2 + x_1y_1 = x_1^3 + a_2'x_1^2 + a_6'$ with $a_2', a_6' \in K$. This equation is non-singular if and only if $a_6' \neq 0$. In this case we set

$$j(E) := \frac{1}{a_6'}.$$

Case 2. Let us suppose that $a_1 = 0$, then the change of coordinates:

$$\begin{cases} x = x_1 + a_2 \\ y = y_1. \end{cases}$$

gives the equation: $y_1^2 + a_3'y_1 = x_1^3 + a_4'x_1 + a_6'$ with a_3', a_4' and $a_6' \in K$. This equation is non-singular if and only if $a_3' \neq 0$. In this case we set

$$j(E) := 0.$$

The group law on an elliptic curve E over a field K of characteristic 2 is defined as we did in Chapter 2, through chord and tangent process. Let us notice that the inverse of a point $P = (x,y) \in E(\overline{K})$ is the point $-P = (x, -a_1x - a_3 - y) \in E(\overline{K})$ (the usual formula for the inverse of a point for an elliptic curve given by a long Weierstrass equation).

Let us describe the duplication law in characteristic 2. One of the expressions we will derive has been already used in Example 6.1.1.4. As before there are two cases, depending on the equation of the elliptic curve or, equivalently, depending on the j-invariant being zero or not.

Let $P = (x_0, y_0) \in E(\overline{K})$.

If the elliptic curve E is given by $y^2 + xy = x^3 + a_2x^2 + a_6$ with $a_2, a_6 \in K$ (hence, $a_6 \neq 0$) then by implicit differentiation we have:

$$x\frac{dy}{dx} + (y + x^2) = 0$$

since $2y + x \equiv x$ and $y + 3x^2 + 2a_2x \equiv y + x^2$. If $x_0 = 0$ the point $P = -P$ hence $2P = 0$. Otherwise, the slope of the tangent line L thought P is $m = \frac{y_0 + x_0^2}{x_0}$. So the equation of the line is given by:

$$L : y = m(x - x_0) + y_0,$$

and the intersection $L \cap E = \{P, -2P\}$ contains the point $-2P = (x_1, y_1)$ where

$$x_1 = m^2 + m + a_2 = \frac{x^4 + a_6}{x^2} \qquad y_1 = m(x_1 - x_0) + y_0.$$

Hence, $2P = (x_2, y_2)$ where $x_2 = \frac{x_0^4 + a_6}{x_0^2}$ and $y_2 = x_1 + y_1$.

Similarly, if the elliptic curve E is given by $y^2 + a_3y = x^3 + a_4x + a_6$ with a_3, a_4 and $a_6 \in K$, and $a_3 \neq 0$, by implicit differentiation:

$$a_3\frac{dy}{dx} + (a_4 + x^2) = 0$$

so the equation of the tangent line at the point P is

$$L : y = \frac{x_0^2 + a_4}{a_3}(x - x_0) + y_0.$$

As before, an easy computation shows that $2P = (x_2, y_2)$ where $x_2 = \frac{x_0^4 + a_4^2}{a_3^2}$ and $y_2 = a_3 + y_1$.

7.1.2 The j-invariant in characteristic 3

Let E be an elliptic curve over a field K with $\mathrm{char}(K) = 3$. Then, after a suitable change of coordinates, E is given by a medium Weierstrass equation:

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

with $a_2, a_4, a_6 \in K$. The j-invariant of E is defined as:

$$j(E) = \frac{a_2^6}{a_2^2a_4^2 - a_2^3a_6 - a_4^3} = \frac{a_2^6}{\Delta_f},$$

where Δ_f is the discriminant of $f(x) = x^3 + a_2x^2 + a_4x + a_6$ (this formula is false if the characteristic is not 3).

7.2 Isomorphism classes

Let $p \geq 5$ be a prime, and $K = \mathbb{F}_p (= \mathbb{Z}/p\mathbb{Z})$. The group $\mathbb{F}_p^\times$ is a cyclic group. Let ζ be a *primitive root* modulo p, i.e. a cyclic generator of $\mathbb{F}_p^\times$. Let $(\mathbb{F}_p^\times)^2$ denote the subgroup of elements in $\mathbb{F}_p^\times$ that are square. We can write

$$\begin{aligned} \mathbb{F}_p^\times &= \{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\} \\ (\mathbb{F}_p^\times)^2 &= \{1, \zeta^2, \zeta^4, \ldots, \zeta^{p-3}\}. \end{aligned}$$

We see that the cardinality of $(\mathbb{F}_p^\times)^2$ is $\frac{p-1}{2}$, i.e. half of that of $\mathbb{F}_p^\times$. In other words, half of the non-zero elements of $\mathbb{F}_p$ are squares, and the other half are non-squares. So the quotient $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2$ is a group of order 2 with representatives 1 and ζ.
Let $E : y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{F}_p^\times$, be an elliptic curve. The condition $A, B \neq 0$ implies that $j = j(E) \neq 0, 1728$. For every $g \in \mathbb{F}_p^\times$, let

$$E^{(g)} : y^2 = x^3 + g^2Ax + g^3B.$$

Then $E^{(g)}$ is also an elliptic curve, and we have $j(E) = j(E^{(g)})$. If g is not a square in $\mathbb{F}_p$ then $E \ncong E^{(g)}$ over $\mathbb{F}_p$, but $E \cong E^{(g^2)}$ over $\mathbb{F}_p$. In general, $E \cong E^{(g)}$ over $\mathbb{F}_p$ when g is a non-zero square, and $E \ncong E^{(g)}$ over $\mathbb{F}_p$ when g is a non-square.
Hence, for each $j \neq 0, 1728$, there are **two** isomorphism classes of elliptic curves $E/\mathbb{F}_p$ with $j(E) = j$. The calculations for $j = 0$ and $j = 1728$ depend on the order of $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^4$ and of $\mathbb{F}_p^\times/(\mathbb{F}_p^\times)^6$ respectively.

7.3 The Frobenius endomorphism

The Frobenius map is the simplest example of an inseparable map which plays an important role in the study of elliptic curves over finite fields.
Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^s$ for some prime p. We recall that, as a subfield of the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, $\mathbb{F}_q$ is characterised by

$$\mathbb{F}_q = \{x \in \overline{\mathbb{F}}_p : x^q = x\}.$$

Indeed, the zero element of $\mathbb{F}_q$ clearly satisfies the identity $x^q - x = 0$. Since $\mathbb{F}_q$ is a field, $\mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$ is a group with $(q-1)$ elements. Thus each $x \in \mathbb{F}_q^\times$ satisfies the polynomial $x^{q-1} - 1 = 0$, which is separable in $\mathbb{F}_q[x]$ since $(x^{q-1} - 1)' = -x^{q-2} \neq 0$. Thus the roots of this polynomial are the $(q-1)$ distinct elements of $\mathbb{F}_q^\times$.

Definition 7.1 Let E be an elliptic curve over $\mathbb{F}_q$. The **Frobenius map** of E is given by

$$\begin{aligned}\phi_q : E(\overline{\mathbb{F}}_q) &\to E(\overline{\mathbb{F}}_q)\\ (x,y) &\mapsto (x^q, y^q).\end{aligned}$$

It is easy to see that this is indeed a map: if $P = (x,y) \in E(\overline{\mathbb{F}}_q)$, then we have

$$(y^q)^2 = (y^2)^q = (x^3 + Ax + B)^q = x^{3q} + A^q x^q + B^q = (x^q)^3 + Ax^q + B = f(x^q).$$

(Note that this uses the fact that E is defined over $\mathbb{F}_q$.) Hence, $\phi_q(P) = (x^q, y^q) \in E(\overline{\mathbb{F}}_q)$.

Corollary 7.3.1 (a) The map ϕ_q is a (purely) inseparable endomorphism.
(b) For every integer $m,n \in \mathbb{Z}$, the map $m\phi_q + n$ is separable if and only if $p \nmid n$.

Proof. The map ϕ_q is clearly given by rational functions; since $\phi_q(0) = 0$, it is an endomorphism by Theorem 6.1.1. Furthermore, ϕ_q is inseparable since the derivative of the first coordinate is $qx^{q-1} \equiv 0$. In fact, we can see that

$$\deg_i(\phi_q) = q \text{ and } \deg_s(\phi_q) = 1.$$

Thus ϕ_q is purely inseparable (in particular, $c_{\phi_q} = 0$). This proves (a).
For (b), we observe that, by Theorem 6.2.7 (ii) and (iv),

$$c_{m\phi_q+n} = mc_{\phi_q} + n = n.$$

This implies that $c_{m\phi_q+n} \neq 0 \Leftrightarrow p \nmid n$. By Theorem 6.2.7 (v), this means that $m\phi_q + n$ is separable if and only if $p \nmid n$. ■

Corollary 7.3.2 Let E be an elliptic curve over a finite field $\mathbb{F}_q$. Then, we have

$$\#E(\mathbb{F}_q) = \deg(\phi_q - 1).$$

Proof. Let $P = (x,y) \in E(\overline{\mathbb{F}}_q)$; we see that

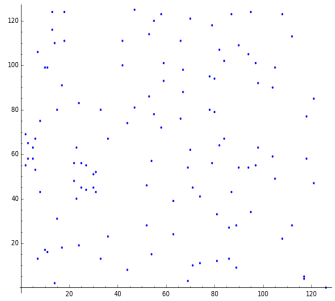
$$P \in E(\mathbb{F}_q) \Leftrightarrow (x^q, y^q) = (x,y) \Leftrightarrow \phi_q(P) = P \Leftrightarrow (\phi_q - 1)(P) = 0 \Leftrightarrow P \in \ker(\phi_q - 1)$$

Hence, $E(\mathbb{F}_q) = \ker(\phi_q - 1)$. By Corollary 7.3.1, we know that $(\phi_q - 1)$ is separable. So it follows from Theorem 6.2.4 (iii) that $\#E(\mathbb{F}_q) = \#\ker(\phi_q - 1) = \deg(\phi_q - 1)$. ■

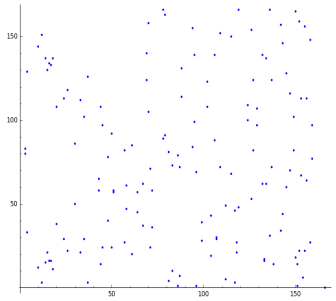
7.4 Hasse's Inequality

Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Estimates for the size of the group $E(\mathbb{F}_q)$ are important for cryptographic applications.

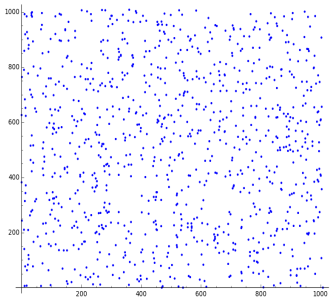
For example, let E be the elliptic curve $y^2 + xy + y = x^3 + x^2 + x + 1$: then we have that $\#E(\mathbb{F}_{127}) = 120, \#E(\mathbb{F}_{163}) = 152$ and $\#E(\mathbb{F}_{1009}) = 980$.



(a) $\#E(\mathbb{F}_{127}) = 120$,



(b) $\#E(\mathbb{F}_{163}) = 152$,



(c) $\#E(\mathbb{F}_{1009}) = 980$.

We can now prove the following important result:

Theorem 7.4.1 — Hasse's Inequality. Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. Let E be an elliptic curve defined over $\mathbb{F}_q$. Then, we have

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

Proof. We recall the Frobenius endomorphism

$$\begin{aligned} \phi_q : E(\overline{\mathbb{F}}_q) &\to E(\overline{\mathbb{F}}_q) \\ (x,y) &\mapsto (x^q, y^q). \end{aligned}$$

It has degree $\deg(\phi_q) = q$. We showed in Corollary 7.3.2 that $\#E(\mathbb{F}_q) = \deg(\phi_q - 1)$, hence:

$$\#E(\mathbb{F}_q) = \deg(\phi_q - 1) = \deg(\phi_q) - 2\langle \phi_q, 1\rangle + 1 = q + 1 - 2\langle \phi_q, 1\rangle.$$

Hence

$$\#E(\mathbb{F}_q) - (q+1) = -2\langle \phi_q, 1\rangle.$$

By the Cauchy-Schwartz inequality, we see that

$$|\#E(\mathbb{F}_q) - (q+1)| = 2|\langle \phi_q, 1\rangle| \leq 2\sqrt{q}.$$

■

Example 7.4.1.1 Let $q = 7$, and E an elliptic curve over $\mathbb{F}_7$. Then, the Hasse Inequality implies that

$$|\#E(\mathbb{F}_7) - (7+1)| \leq 2\sqrt{7} = \sqrt{28} \Rightarrow |\#E(\mathbb{F}_7) - 8| \leq 5.$$

So

$$3 \leq \#E(\mathbb{F}_7) \leq 13.$$

R For an elliptic curve E over $\mathbb{F}_q$, the finite field with q elements, the Hasse Inequality gives a very good estimate of the size of the group of $\mathbb{F}_q$-rational points on E:

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

Corollary 7.4.2 Let E be an elliptic curve over $\mathbb{F}_q$. Let $a_q = q+1-\#E(\mathbb{F}_q)$. Then, the Frobenius endomorphism ϕ_q satisfies the polynomial $x^2 - a_q x + q$.

Proof. In the proof of Theorem 7.4.1, we showed that

$$a_q = q+1-\#E(\mathbb{F}_q) = 2\langle \phi_q, 1\rangle.$$

Since $\deg(\phi_q) = q$, Proposition 6.4.1 implies that ϕ_q satisfies the equation $x^2 - a_q x + q = 0$. We can reinterpret the Hasse Inequality as the statement that

$$-2\sqrt{q} \leq a_q \leq 2\sqrt{q}.$$

■

R The statements of this section and the previous do also hold in characteristic 2 and 3.

Let E be an elliptic curve defined over $\mathbb{F}_q$, then $\#E(\mathbb{F}_q) = q+1-a_q$. The Frobenius endomorphism ϕ_q satisfies: $x^2 - a_q x + q = 0$. Let α, β be the roots of $x^2 - a_q x + q = 0$, therefore,

$$x^2 - a_q x + q = (x-\alpha)(x-\beta) = 0$$

where $\alpha + \beta = a_q$, $\alpha\beta = q$.
Let n be a positive integer, it is possible to prove the following recursive relation to compute the number of points of E over the finite field of cardinality q^n:

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - a_{q^n} = q^n + 1 - \alpha^n - \beta^n.$$

7.5 Endomorphism ring

Analogously with the characteristic zero case, when $\mathrm{char}(K) = p > 0$ is prime, there are two cases. In positive characteristic, the endomorphism ring is a characteristic zero ring but it has not to be commutative. Here the two cases:

- the elliptic curve is said to be *ordinary* if $\mathrm{End}(E)$ has rank 2, this is the "usual case";
- the elliptic curve is said to be *supersingular* if $\mathrm{End}(E)$ has rank 4, this is the "unusual case". In that case, $\mathrm{End}(E)$ is non-commutative, and is isomorphic to an order in a quaternion algebra.

Points of finite order

Division polynomials

Galois representations

8. Points of finite order

In this chapter, we will show that for an elliptic curve E defined over a field K, with $\mathrm{char}(K) = 0$, and a positive integer n the torsion subgroup

$$E[n] = \{P \in E(\overline{K}) : nP = 0\} \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

We will also describe the torsion subgroup when the field K has positive characteristic.

At the end of the chapter, we will briefly explain the construction of Galois representations attached to elliptic curves from torsion subgroups. Galois representations are some of the most important objects in modern number theory: for example, they play a crucial role in the proof of the Fermat Last Theorem.

8.1 Points of finite order

Let K be a field, and E an elliptic curve defined over K. Let $n \in \mathbb{Z}$ be non-zero. Then, by Theorem 6.2.4 (i), we know that the multiplication-by-n is surjective.

Definition 8.1 A point $P \in E(\overline{K})$ has **finite order** if there exists a positive integer n such that $nP = 0$. The smallest of such n is called the **order** of the point and we denote it by $\mathrm{ord}(P)$. We define the **n-torsion subgroup** of E to be

$$E[n] := \ker([n]) = \{P \in E(\overline{K}) : nP = 0\} = \{P \in E(\overline{K}) : \mathrm{ord}(P) \mid n\}.$$

By Theorem 6.2.4 (i), (iii) and Corollary 6.3.2, we know that

$$\#E[n] = \deg_s([n]) \leq \deg([n]) = n^2.$$

We need the following theorem for characterise the n-torsion subgroup:

Theorem 8.1.1 — Structure Theorem for finite abelian groups. Let A be a finite non-trivial abelian group. Then, there exists a sequence of integers $1 < n_1 \leq n_2 \leq \cdots \leq n_k$ such

that $n_i \mid n_{i+1}$, for $1 \leq i < k$, and

$$A \cong (\mathbb{Z}/n_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}).$$

The integers (n_i) are uniquely determined.

Proposition 8.1.2 If $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p$ and $p \nmid n$, then

$$E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}).$$

Proof. The conditions on $\mathrm{char}(K)$ ensure that the multiplication-by-n is separable; hence $\#E[n] = n^2$. By Theorem 8.1.1, we can write

$$E[n] \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/n_k\mathbb{Z}),$$

where $n_i > 0$ and $n_i \mid n_{i+1}$, $0 < i < k$. This implies that $E[n_1] \subset E[n]$ has order n_1^k. But we just proved that $\#E[n_1] = n_1^2$, so $k = 2$. Since multiplication by n annihilates

$$E[n] \cong (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z}),$$

we must have $n_2 \mid n$. This combined with $n_1 n_2 = n^2$ implies that $n_1 = n_2 = n$. ■

Example 8.1.2.1 Assume $\mathrm{char}(K) \neq 2$, and E be given by an equation

$$y^2 = (x - e_1)(x - e_2)(x - e_3),\ e_i \in \overline{K}.$$

Then, the above proposition implies that

$$E[2] = \{0, (e_1, 0), (e_2, 0), (e_3, 0)\}.$$

Let $T_i = (e_i, 0)$, $i = 1, 2, 3$; then $T_3 = T_1 + T_2$.
If $\mathrm{char}(K) = 2$, as we have seen before $[2]$ is inseparable, so $\#E[2] < 4$. In fact $\#E[2] = 1$ or 2 as the Theorem 8.1.5 shows.

Example 8.1.2.2 Assume that $\mathrm{char}(K) \neq 2, 3$, and $E : y^2 = x^3 + Ax + B$. Let $P = (x, y) \in E(\overline{K})$. Then, we see that

$$\begin{aligned} P \text{ has order } 3 &\Leftrightarrow 2P = -P \\ &\Rightarrow x(2P) = x(P) = x \\ &\Rightarrow 3x^4 + 6Ax^2 + 12Bx - A^2 = 0, \end{aligned}$$

which clearly has a non-zero discriminant. Therefore $\#E[3] = 9$ (each root of this polynomial gives two opposite points in $E(\overline{K})$, plus the zero element).

R In Definition 8.1, we work with the algebraic closure $\overline{K}$ of K. Otherwise, $[n]$ would no longer be surjective, and the conclusion of Proposition 8.1.2 would be wrong.

For $K \subset K' \subset \overline{K}$, we will write $E(K')[n]$ for the subset of $E[n]$ consisting of the n-torsion points with coordinates in K'. By definition, $E(K')[n]$ is a subgroup of $E[n]$.

Example 8.1.2.3 (a) The curve $E_1 : y^2 = x^3 - 2$ has no 2-torsion point defined over $\mathbb{Q}$ since $x^3 = 2$ has no rational solutions, i.e. $E_1(\mathbb{Q})[2] = \{0\}$.

(b) For the curve $E_2 : y^2 = x(x^2+1)$, we have $E_2(\mathbb{Q})[2] = \{0,(0,0)\}$, but

$$E(\mathbb{Q}(i))[2] = \{0,(0,0),(\pm i,0)\}.$$

(c) All the 2-torsion points of the congruence curve $E_n : y^2 = x(x^2 - n^2)$ are defined over $\mathbb{Q}$:

$$E(\mathbb{Q})[2] = \{0,(0,0),(\pm n,0)\}.$$

Proposition 8.1.3 Let $\mathrm{char}(K) = p$ (prime). Then, either

1. $E[p^e] = \{0\}$ for all $e \geq 1$ (when E is supersingular), or
2. $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ for all $e \geq 1$ (when E is ordinary).

Proof. First assume that $e = 1$. Since $[p]$ is inseparable, either

1. $\deg_s([p]) = 1$ and $\deg_i([p]) = p^2$, which implies that $E[p] = \{0\}$, or
2. $\deg_s([p]) = p = \deg_i([p])$, in which case $E[p] \cong \mathbb{Z}/p\mathbb{Z}$.

We observe that for a general e, Case (1) implies that $[p]$ is purely inseparable; hence $[p^e] = [p]^e$ is purely inseparable. Thus $E[p^e] = \{0\}$. In Case (2), $\deg_s([p]) = p$ implies that $\deg_s([p^e]) = \deg_s([p]^e) = p^e$; hence $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$. ∎

Let us recall the following result about abelian groups:

Lemma 8.1.4 If A is an abelian group and m,n are coprime positive integers, then

$$A[mn] \cong A[m] \times A[n].$$

Combining Lemma 8.1.4 and Propositions 8.1.2 and 8.1.3 we obtain the following result:

Theorem 8.1.5 Let E be an elliptic curve defined over a field K. For all $n \geq 1$,

(i) If $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) = p \nmid n$ then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

(ii) If $\mathrm{char}(K) = p \mid n$ then either

(a) $E[n] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$; or
(b) $E[n] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$,

where we write $n = p^e m$ with $p \nmid m$ (so $e \geq 1$).

Definition 8.2 Let E be an elliptic curve defined over a field K. The **torsion subgroup** of E is defined as

$$E_{\mathrm{tors}} := \bigcup_{n \geq 1} E[n].$$

This is the subgroup of $E(\overline{K})$ consisting of all points of finite order. It is **infinite** abelian.

8.2 Division polynomials

Let K be a field, and E an elliptic curve defined over K. Let $n \in \mathbb{Z}$ be non-zero. The n-torsion subgroup of E can be described through the zero locus of polynomials. In this section we will explain shortly how it is possible to do this.

Definition 8.3 Let E be an elliptic curve over the field K, given by a short Weierstrass equation: $y^2 = x^3 + Ax + B$. Let n be an integer greater or equal to zero, the **n-th division polynomial** ψ_n on E is defined using the following recursive formulas:

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 2\\
\psi_{2m} &= (2y)^{-1}(\psi_m)(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \geq 2.
\end{aligned}$$

If the elliptic curve is given by a long Weierstrass equation, similar formulas are available, anyway, we will only define these polynomials for elliptic curves given by short Weierstrass equations.
For any positive integer m, define the polynomials:

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1}, \qquad \omega_m = (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2).$$

Using these polynomials we can express the multiplication by n endomorphism:

Theorem 8.2.1 Let $P = (x,y)$ be a $\overline{K}$-point of the elliptic curve $y^2 = x^3 + Ax + B$ over a field K of characteristic different from 2, and let n be a positive integer. Then

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right).$$

where $\phi_n(x), \psi_n^2(x)$ are the polynomials obtained from $\phi_n(x,y), \psi_n^2(x,y)$ through the equation $y^2 = x^3 + Ax + B$.

The proof of this theorem goes through the Weierstrass $\wp$-function if the characteristic of K is zero, and elements of algebraic geometry otherwise, hence we omit it. Anyway, let us remark that it is possible to show that $\phi_n(x)$ and $\psi_n^2(x)$ have no common factor and that the degree of $\phi_n(x)$ is n^2. Therefore, it is possible to obtain again that the multiplication by n has degree n^2 without using the parallelogram identity.
Moreover, a point $P = (x,y) \in E(\overline{K})$ is a point of n-torsion if and only if $\psi_n^2(x) = 0$, by definition of endomorphism.

8.3 Galois representations

For the rest of section, we let that $K = \mathbb{Q}$. We recall that the Galois group of $\overline{\mathbb{Q}}$ over $\mathbb{Q}$ is defined by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \mathrm{Aut}(\overline{\mathbb{Q}})$. Let us denote its action on $\overline{\mathbb{Q}}$ by $x \mapsto \sigma(x)$, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Let $n \geq 2$ be an integer, and set

$$\mu_n := \left\{ x \in \overline{Q}^\times : x^n = 1 \right\}.$$

This is an abelian group under multiplication. For any $\zeta' \in \mu_n$, we say that ζ' is *primitive* if $\zeta'^m = 1$ implies that $n \mid m$. Let $\zeta = e^{\frac{2\pi i}{n}}$; then ζ is a primitive root. Every other primitive root is of the form $\zeta' = \zeta^m$ with $\gcd(m,n) = 1$. In fact, μ_n is a *cyclic* group in which every primitive root is a *generator*, and we have a natural bijection

$$\begin{aligned} &\mu_n \to \mathbb{Z}/n\mathbb{Z} \\ &\zeta^m \mapsto \overline{m} := m \bmod n, \end{aligned}$$

which sends the set of primitive roots to $(\mathbb{Z}/n\mathbb{Z})^\times$.
The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\overline{\mathbb{Q}}$ preserves μ_n since $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $\zeta' \in \mu_n$ implies that

$$\sigma(\zeta')^n = \sigma(\zeta'^n) = \sigma(1) = 1.$$

Moreover, since every $\sigma \in \mathrm{Gal}(\overline{Q}/\mathbb{Q})$ is an automorphism, its also preserves orders; and so, $\sigma(\zeta')$ is primitive if and only ζ' is primitive. So, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, there exists an integer m_σ such that $\gcd(m_\sigma, n) = 1$ and $\sigma(\zeta) = \zeta^{m_\sigma}$. It is not hard to see that the map

$$\begin{aligned} \bar{\varepsilon}_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma &\mapsto m_\sigma \bmod n \end{aligned}$$

is a well-defined group homomorphism. It is called a $\bmod n$ *cyclotomic character*.

Example 8.3.0.1 Let $p \geq 3$ be prime. Then $x^p - 1 = (x-1)\Phi_p(x)$, where

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible. The primitive root $\zeta = e^{\frac{2\pi i}{p}}$ clearly satisfies $\Phi_p(x)$. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; since σ is $\mathbb{Q}$-linear, and is a ring homomorphism, we see that

$$\Phi_p(\sigma(\zeta)) = \Phi_p(\zeta) = 0.$$

Hence, $\sigma(\zeta)$ is also a primitive root of 1. In this case, we get the $\bmod p$ cyclotomic character

$$\begin{aligned} \bar{\varepsilon}_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) &\to \mathbb{F}_p^\times \\ \sigma &\mapsto \bar{\varepsilon}_p(\sigma). \end{aligned}$$

This is a one dimensional $\bmod p$ *Galois representation*.

Now, we let $E : Y^2 = X^3 + AX + B$ be an elliptic curve, with $A, B \in \mathbb{Q}$. For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $P = (x,y) \in E(\overline{\mathbb{Q}})$, set

$$\sigma(P) = (\sigma(x), \sigma(y)).$$

Since $\sigma : \overline{Q} \to \overline{Q}$ is a ring homomorphism (hence it is $\mathbb{Q}$-linear), we see that

$$P \in E(\overline{\mathbb{Q}}) \implies \sigma(P) \in E(\overline{\mathbb{Q}}).$$

Moreover,

$$(\tau\sigma)(P) = \tau(\sigma(P)) \ \forall \tau, \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

So, this defines an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E(\overline{\mathbb{Q}})$. Furthermore, we see that this action sends lines to lines. So it is compatible with the group structure of $E(\overline{\mathbb{Q}})$. In particular, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ preserves the subgroup $E[n]$. Next, let us choose a $(\mathbb{Z}/n\mathbb{Z})$-basis of $E[n]$, that is equivalent to giving an isomorphism $E[n] \cong (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$. We note that $E[n]$ is a $(\mathbb{Z}/n\mathbb{Z})$-module, i.e.

$$[a]P + [b]Q \in E[n], \forall P, Q \in E[n] \text{ and } a, b \in \mathbb{Z}/n\mathbb{Z}.$$

Then, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ gives rise to a group homomorphism

$$\bar{\rho}_n : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

From now on, assume that p is a prime. In that case,

$$E[p] \cong (\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z}) = \mathbb{F}_p \times \mathbb{F}_p.$$

Definition 8.4 The mod p **Galois representation** attached to E is defined by

$$\bar{\rho}_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p).$$

Theorem 8.3.1 Let $\bar{\rho}_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ be the mod p representation attached to an elliptic curve E. Then, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\det(\bar{\rho}_p(\sigma)) = \bar{\varepsilon}_p(\sigma)$.

Galois representations are some of the most important objects in modern number theory. For example, they play a crucial role in the proof of the Fermat Last Theorem.

Example 8.3.1.1 Let $p \geq 5$, and consider the Fermat equation $a^p + b^p = c^p$ (see Section 1). Assume that there is $(a,b,c) \in \mathbb{Z}^3$ such that $abc \neq 0$ and $\gcd(a,b,c) = 1$. WLOG, we can assume that $a \equiv -1 \pmod 4$ and $b \equiv 0 \pmod 2$. Consider the elliptic curve

$$E : y^2 = x(x - a^p)(x + b^p).$$

This is called the *Frey curve* associated to the solution (a,b,c). It has discriminant

$$\Delta = [(0 - (-a^p))(0 - b^p)(-a^p - b^p)]^2 = (abc)^{2p}.$$

The above construction says that there is a mod p Galois representation

$$\bar{\rho}_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p),$$

associated to this curve, and hence to the solution (a,b,c). Hence, to show that (a,b,c) doesn't exist, it is enough to show that $\bar{\rho}_p$ cannot exist. This can be done by relating $\bar{\rho}_p$ to Galois representations attached to *modular forms*. A deep and careful study of the latter reveals that $\bar{\rho}_p$ cannot exist.

Valuations

Integral models

Torsion subgroup: The Lutz-Nagell Theorem

Reduction mod p

9. Elliptic curves over $\mathbb{Q}$: torsion

In this chapter and the next, we will study the structure of the abelian group $E(\mathbb{Q})$, when E is an elliptic curve over $\mathbb{Q}$. Namely, we will prove the following theorem.

Theorem 9.0.2 — Mordell-Weil. Let $E/\mathbb{Q}$ be an elliptic curve defined over $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ is **finitely generated**, i.e.

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T,$$

where $r \geq 0$ is the **rank** of $E(\mathbb{Q})$, and T is a finite group. This means that there exist $r \geq 0$ points $P_1, \ldots, P_r \in E(\mathbb{Q})$ such that every point $P \in E(\mathbb{Q})$ can be **uniquely** expressed as

$$P = P_0 + n_1 P_1 + \cdots n_r P_r, \text{ with } n_i \in \mathbb{Z}, \;\; P_0 \in T = E(\mathbb{Q})_{\text{tors}}.$$

We will first see that, for most primes p, we can reduce the curve E modulo p and obtain a curve $\overline{E}_p$ over $\mathbb{F}_p$, the field of integers mod p. The information gathered in this process will be used to determine $E(\mathbb{Q})_{\text{tors}}$. Then, we will proved that $E(\mathbb{Q})$ has finite rank.

9.1 Valuations

Let p be a prime, $x \in \mathbb{Q}^\times$; then we can write

$$x = p^e \frac{a}{b},$$

where $a, b \in \mathbb{Z}$, $p \nmid ab$ and $\gcd(a,b) = 1$. We set

$$v_p(x) = \text{ord}_p(x) = e.$$

We see that

- $v_p(x) > 0$ if and only if p divides only the numerator of x.
- $v_p(x) = 0$ if and only if p divides neither the numerator nor the denominator of x.
- $v_p(x) < 0$ if and only if p divides only the denominator of x.

Definition 9.1 Let p be a prime. The map

$$\begin{aligned} v_p : \mathbb{Q} &\to \mathbb{Z} \cup \{\infty\} \\ 0 &\mapsto \infty \\ x &\mapsto v_p(x), x \neq 0, \end{aligned}$$

is called a p-**adic valuation**.

Lemma 9.1.1 Let p be a prime. Then

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x+y) \geq \min\{v_p(x), v_p(y)\}$, with equality if $v_p(x) \neq v_p(y)$.

Proof. Exercise. ■

Example 9.1.1.1 $v_2(4 \cdot 4) = v_2(16) = 4 = v_2(4) + v_2(4)$, on the other hand, $v_2(4+4) = v_2(8) = 3 > 2 = \min\{v_2(4), v_2(4)\}$.

Definition 9.2 Let p be a prime and $x \in \mathbb{Q}^\times$. We say that x is

- p-**integral** if $v_p(x) \geq 0$,
- a p-**unit** if $v_p(x) = 0$,

Definition 9.3 Let p be a prime. The p-**adic norm** (or **absolute value**) associated to v_p is the map $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ defined by

$$|x|_p := \begin{cases} 0, & x = 0 \\ p^{-v_p(x)}, & x \neq 0 \end{cases}$$

From Lemma 9.1.1, it immediately follows that

1. $|xy|_p = |x|_p |y|_p$;
2. $|x+y|_p \leq \max\{|x|_p, |y|_p\}$, with equality if $|x|_p \neq |y|_p$.

R The p-adic valuation v_p and norm $|\cdot|_p$ are designed to encode divisibility properties by p. Indeed, the higher the power of p that divides an integer x is, that is $v_p(x)$, the smaller is its norm $|x|_p = p^{-v_p(x)}$. The completions $\mathbb{Z}_p$ and $\mathbb{Q}_p$ of $\mathbb{Z}$ and $\mathbb{Q}$ with respect to $|\cdot|_p$ are called the *p-adic integers* and *p-adic numbers*, respectively. We have

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}.$$

R Let $x \in \mathbb{Q}$, then $v_p(x) \geq 0 \forall p$ if and only if $x \in \mathbb{Z}$. In other words,

$$\mathbb{Z} = \{x \in \mathbb{Q} : v_p(x) \geq 0 \forall p \text{ prime}\}.$$

9.2 Integral models

Let $E : Y^2 = X^3 + AX + B$, with $A, B \in \mathbb{Q}$, be an elliptic curve. Recall that we may replace (A, B) by $(\mu^4 A, \mu^6 B)$, for any $\mu \in \mathbb{Q}^\times$, to obtain a curve which is isomorphic to E. By using a suitable μ we arrive at an equation in which

1. the coefficients $A, B \in \mathbb{Z}$: *integrality condition*, any equation satisfying this is an **integral model** of E,
2. if $d^4 \mid A$ and $d^6 \mid B$ then $|d| = 1$: *minimality condition*, any equation satisfying this is a **minimal model** of E.

This process will not affect the group structure of $E(\mathbb{Q})$ since $(x, y) \mapsto (\mu^2 x, \mu^3 y)$ is a group isomorphism over $\mathbb{Q}$ since $\mu \in \mathbb{Q}^\times$.

Example 9.2.0.2 The curve $E : y^2 = x^3 + 2x - 3$ is a minimal integral model for the curve

$$E' : y^2 = x^3 + \frac{2592}{625}x - \frac{139968}{15625}.$$

To see this, simply take $\mu = \frac{5}{6}$.

R The curve $E : Y^2 = X^3 + AX + B$ is integral and minimal if and only if for all prime p:

$$\min\left\{\left[\frac{v_p(A)}{4}\right], \left[\frac{v_p(B)}{6}\right]\right\} = 0.$$

Why are we interested in integral equation? The reason is that we can reduce them and consider equations over finite fields.
Let E be an elliptic curve given by an integral short Weierstrass equation $Y^2 = X^3 + AX + B$, then we may reduce E modulo p to get a curve

$$\overline{E} : Y^2 = X^3 + \bar{A}X + \bar{B},$$

where $\bar{A}, \bar{B} \in \mathbb{F}_p$ are the reductions of A, B mod p. This may be a singular curve. Fortunately, the next lemma implies that this only happens finitely many times.

Lemma 9.2.1 Let $E/\mathbb{Q}$ be an elliptic curve given by an **integral** equation $Y^2 = X^3 + AX + B$. Then for all but finitely many primes p, the reduced curve $\overline{E}$ is an elliptic curve over $\mathbb{F}_p$.

Proof. The discriminant $\Delta = -(4A^3 + 27B^2) \in \mathbb{Z}$ is non-zero. The discriminant of $\overline{E}$ is $\bar{\Delta}$ which is $0 \in \mathbb{F}_p$ if and only if $p \mid \Delta$. But Δ only has a finite number of prime divisors. ■

Definition 9.4 Let $E/\mathbb{Q}$ be an elliptic curve given by an integral equation $Y^2 = X^3 + AX + B$, and p an odd prime. Then E has **good reduction** at p if $p \nmid \Delta$. If $E/\mathbb{Q}$ is given by an integral minimal equation and it has not good reduction at p, then it has **bad reduction** at p.

If an elliptic curve has bad reduction modulo a prime, then its reduction is a singular cubic. Therefore, we classify the reduction type according to the singular curve: additive (the singular point is a cusp) or multiplicative (the singular point is a node) split or non-split.
We will omit the prime 2 from the discussion (a different definition of discriminant would be needed to study the reduction modulo 2).

Example 9.2.1.1 (1) Let $n \geq 1$ be an integer, and $E_n : Y^2 = X^3 - n^2X$ the congruent number curve associated to n. The discriminant of E_n is $\Delta = 4n^6$. Therefore E has good reduction at p for all prime $p \nmid 2n$.
(2) The curve $E : Y^2 = X^3 + c$, with $c \in \mathbb{Z}$ has discriminant $\Delta = -27c^2$. So it has good reduction at p if $p \nmid 6c$.

Lemma 9.2.2 Let $E : Y^2 = X^3 + AX + B$, $A, B \in \mathbb{Z}$, be given by an integral equation, and let $p \nmid 2\Delta$. Then, there is a well-defined map $r_p : E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$, called the **reduction map**.

Proof. Let $P := [x : y : z] \in \mathbf{P}^2(\mathbb{Q})$, where we choose $x, y, z \in \mathbb{Z}$ such that $\gcd(x, y, z) = 1$ (see Assignment 1), then $\min\{v_p(x), v_p(y), v_p(z)\} = 0$. So one of the coordinates is a p-unit, and its image in $\mathbb{F}_p$ is non-zero, hence $[\bar{x} : \bar{y} : \bar{z}] \in \mathbf{P}^2(\mathbb{F}_p)$. Let $x', y', z' \in \mathbb{Z}$ be such that $\gcd(x', y', z') = 1$ and $[x' : y' : z'] = [x : y : z]$. Then, we must have $x' = ux$, $y' = uy$ and $z' = uz$, with $u = \pm 1$, so $r_p(P) := [\bar{x} : \bar{y} : \bar{z}]$ is well-defined.

$$\begin{array}{ccc} \mathbf{P}^2(\mathbb{Q}) & \xrightarrow{r_p} & \mathbf{P}^2(\mathbb{F}_p) \\ \uparrow & & \uparrow \\ E(\mathbb{Q}) & \xrightarrow{r_p} & \overline{E}(\mathbb{F}_p) \end{array}$$

Let $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ in homogeneous coordinates, and $\overline{E} : Y^2Z = X^3 + \bar{A}XZ^2 + \bar{B}Z^3$ its reduction modulo p. Then we see that $[x : y : z] \in E(\mathbb{Q})$ implies $r_p([x : y : z]) \in \overline{E}(\mathbb{F}_p)$. ■

R Let E be an elliptic curve over $\mathbb{Q}$, then there exists a prime p such that E has bad reduction modulo p: this is a theorem of Tate.

We will go back to study the reduction map in details at the end of this chapter.

9.3 Torsion subgroup: The Lutz-Nagell Theorem

Let E be given by an integral short Weierstrass equation. We will see that points of finite order are **integral**. The Bachet-Mordell equation $Y^2 = X^3 - 2$ shows that the converse is false since $P = (3, 5)$ has infinite order.

Example 9.3.0.1 Let $E : Y^2 = X^3 - 2$, and $P = (3, 5)$. Then, we see that

$$\begin{aligned} 2P &= \left(\frac{3 \cdot 43}{2^2 \cdot 5^2}, -\frac{383}{2^3 \cdot 5^3} \right), \\ 3P &= \left(\frac{73 \cdot 2251}{3^4 \cdot 19^2}, -\frac{5 \cdot 43 \cdot 71 \cdot 4339}{3^6 \cdot 19^3} \right), \\ 4P &= \left(\frac{3 \cdot 11 \cdot 43 \cdot 59 \cdot 27961}{2^4 \cdot 5^2 \cdot 383^2}, \frac{23 \cdot 911 \cdot 48383 \cdot 111721}{2^6 \cdot 5^3 \cdot 383^3} \right), \\ 5P &= \left(\frac{3 \cdot 241 \cdot 49681 \cdot 8556001}{29^2 \cdot 211^2 \cdot 2069^2}, \frac{5^2 \cdot 179 \cdot 269 \cdot 39239 \cdot 63901 \cdot 1510679}{29^3 \cdot 211^3 \cdot 2069^3} \right). \end{aligned}$$

The number of primes appearing in the the denominators and their powers are increasing more and more through the multiple of P.

It it possible to characterize the $\mathbb{Q}$-rational points of an elliptic curve given by an integral short Weierstrass equation:

Proposition 9.3.1 Let $E/\mathbb{Q}$ be an elliptic curve given by an integral equation $Y^2 = X^3 + AX + B$. Let $P = (x,y) \in E(\mathbb{Q})$. Then

$$x = \frac{a}{c^2}, \qquad y = \frac{b}{c^3},$$

where $a,b,c \in \mathbb{Z}$, $c > 0$, $\gcd(a,c) = \gcd(b,c) = 1$.

Proof. Write $P = (x,y)$ with $x,y \in \mathbb{Q}$. It suffices to show that for all primes p,

$$v_p(x) < 0 \Leftrightarrow v_p(y) < 0 \Leftrightarrow v_p(x) = -2r, \quad v_p(y) = -3r \qquad (r > 0).$$

If $v_p(x) = -k < 0$ then $v_p(x^3) = -3k$, $v_p(Ax) = v_p(A) + v_p(x) \geq -k$ and $v_p(B) \geq 0$ (using integrality of A,B). So $v_p(x^3 + Ax + B) = -3k$, but this also equals $v_p(y^2) = 2v_p(y)$ so is even, hence $k = 2r$ with $r \in \mathbb{Z}$ positive and $v_p(x) = -2r$, $v_p(y) = -3k/2 = -3r$. Conversely if $v_p(x) \geq 0$ then $v_p(x^3 + Ax + B) \geq 0$ so $v_p(y) \geq 0$. ∎

Main idea: If $P = (x,y)$ is not p-integral (so $v_p(x) = -2k$ and $v_p(y) = -3k$ for some $k \geq 1$), then $2P, 3P, 4P, \ldots$ have denominators more and more highly divisible by p.

Let us make this observation rigorous. Fix a prime p, and for each $k \geq 1$ define a subset of $E(\mathbb{Q})$ by

$$E_k := \{P = (x,y) \in E(\mathbb{Q}) : v_p(x) \leq -2k, v_p(y) \leq -3k\} \cup \{0\}.$$

Then $P \in E_k$ if and only if p^{2k} divides the denominator of x_P. Therefore,

$$E(\mathbb{Q}) \supset E_1 \supset E_2 \supset \cdots \supset \{0\}.$$

The sequence $(E_k)_k$ is called a (decreasing) **p-adic filtration** on $E(\mathbb{Q})$.
We will show that E_{k+1} has finite index in E_k (for all $k \geq 1$), where the index is a power of p, and E_1 has no elements of finite order except 0.
In order to work with positive valuations, keeping the notations as above, we will introduce new coordinates as follows. By dividing the defining equation of E through by Y^3, we get

$$\frac{1}{Y} = \left(\frac{X}{Y}\right)^3 + A\left(\frac{X}{Y}\right)\left(\frac{1}{Y}\right)^2 + B\left(\frac{1}{Y}\right)^3.$$

Setting $U = X/Y$ and $V = 1/Y$, we get the curve

$$\tilde{E} : V = U^3 + AUV^2 + BV^3.$$

We can express this change of coordinates projectively as

$$(X,Y) \rightsquigarrow [X : Y : 1] = \left[\frac{X}{Y} : 1 : \frac{1}{Y}\right] = [U : 1 : V].$$

For $P = (x,y) \in E(\mathbb{Q})$, we will denote the image of P under the change of coordinates by

$$\tilde{P} = \left(\frac{x}{y}, \frac{1}{y}\right) = (u,v) \in \tilde{E}(\mathbb{Q}).$$

We see that

$$\begin{aligned} E(\mathbb{Q}) \ni 0 &\longleftrightarrow (0,0) = \mathscr{O} \in \tilde{E}(\mathbb{Q}) \\ P = (x,y) &\longleftrightarrow (u,v) = \tilde{P} \\ -P = (x,-y) &\longleftrightarrow (-u,-v) = -\tilde{P}. \end{aligned}$$

The points of order 2 on E become point of infinite order on $\tilde{E}$. Under this change of variables (which is a projective transformation), there is a correspondence

$$E_k \leftrightarrow \tilde{E}_k := \left\{ \tilde{P} \in \tilde{E}(\mathbb{Q}) : \mathrm{ord}_p(u) \geq k, \mathrm{ord}_p(v) \geq 3k \right\},$$

where $(\tilde{E}_k)$ is now an *increasing* filtration.

Lemma 9.3.2 Let $\tilde{P}_i = (u_i, v_i) \in \tilde{E}_k(\mathbb{Q})$ for $i = 1,2$, where $k \geq 1$. Set

$$\tilde{P}_3 = \tilde{P}_1 + \tilde{P}_2 = (u_3, v_3).$$

Then, we have $u_3 \equiv u_1 + u_2 (\bmod\ p^{5k})$ (equivalently $v_p(u_1 + u_2 - u_3) \geq 5k$).

Proof. We have

$$\begin{aligned} v_1 &= u_1^3 + Au_1v_1^2 + Bv_1^3 \\ v_2 &= u_2^3 + Au_2v_2^2 + Bv_2^3, \end{aligned}$$

which gives

$$\begin{aligned} v_1 - v_2 &= u_1^3 - u_2^3 + A(u_1v_1^2 - u_2v_2^2) + B(v_1^3 - v_2^3) \\ &= u_1^3 - u_2^3 + A[(u_1v_1^2 - u_1v_2^2) + (u_1v_2^2 - u_2v_2^2)] + B(v_1^3 - v_2^3) \\ &= (u_1 - u_2)(u_1^2 + u_1u_2 + u_2^2) + Av_2^2(u_1 - u_2) + Au_1(v_1^2 - v_2^2) \\ &\quad + B(v_1 - v_2)(v_1^2 + v_1v_2 + v_2^2) \\ &= (u_1 - u_2)(u_1^2 + u_1u_2 + u_2^2) + Av_2^2(u_1 - u_2) + Au_1(v_1 - v_2)(v_1 + v_2) \\ &\quad + B(v_1 - v_2)(v_1^2 + v_1v_2 + v_2^2). \end{aligned}$$

From this, we obtain

$$(v_1 - v_2)\left[1 - Au_1(v_1 + v_2) - B(v_1^2 + v_1v_2 + v_2^2)\right] = (u_1 - u_2)\left[u_1^2 + u_1u_2 + u_2^2 + Av_2^2\right].$$

We rewrite this as

$$(v_1 - v_2)\alpha = (u_1 - u_2)\beta,$$

where

$$\begin{aligned} \alpha &= 1 - Au_1(v_1 + v_2) - B(v_1^2 + v_1v_2 + v_2^2) \\ \beta &= u_1^2 + u_1u_2 + u_2^2 + Av_2^2. \end{aligned}$$

We observe that, since $v_p(u_1), v_p(u_2) \geq k$ and $v_p(v_1), v_p(v_2) \geq 3k$, we have

- $\alpha = 1 - Au_1(v_1 + v_2) - B(v_1^2 + v_1v_2 + v_2^2) \equiv 1 (\bmod\ p^{4k})$, so $v_p(\alpha) = 0$ and $\alpha \neq 0$.
- $\beta = u_1^2 + u_1u_2 + u_2^2 + Av_2^2$ so $v_p(\beta) \geq 2k$.

If $u_1 = u_2$ then $v_1 = v_2$ since $\alpha \neq 0$. In this case, $\tilde{P}_1 = \tilde{P}_2$. So, the line $\tilde{P}_1\tilde{P}_2$ has slope

$$m = \begin{cases} \frac{v_2 - v_1}{u_2 - u_1} = \frac{\beta}{\alpha} & \text{if} \quad \tilde{P}_1 \neq \tilde{P}_2 \\ \\ \frac{3u_1^2 + Av_1^2}{1 - 2Au_1v_1 - 3Bv_1^2} & \text{if} \quad \tilde{P}_1 = \tilde{P}_2 \end{cases}$$

where in the second case, we use implicit differentiation on $\tilde{E} : V = U^3 + AUV^2 + BV^3$ to get

$$dV = 3U^2dU + AV^2dU + 2AUVdV + 3BV^2dV,$$

and

$$(1 - 2AUV - 3BV^2)dV = (3U^2 + AV^2)dU.$$

Now, $v_p(m) \geq 2k$ (in both cases). The equation of the line $\tilde{P}_1\tilde{P}_2$ is $V = mU + c$, where

$$c = v_1 - mu_1 \Rightarrow v_p(c) \geq 3k.$$

This line intersects $\tilde{E}$ where

$$mU + c = U^3 + AU(mU + c)^2 + B(mU + c)^3,$$

with roots $u_1, u_2, -u_3$. By expanding this equality and rearranging it terms, we see that

$$(1 + Am^2 + Bm^3)U^3 + (2Amc + 3Bm^2c)U^2 + \text{lower terms} = 0.$$

Hence

$$u_1 + u_2 - u_3 = -\frac{2Amc + 3Bm^2c}{1 + Am^2 + Bm^3},$$

and

$$v_p(u_1 + u_2 - u_3) \geq 5k.$$

■

Corollary 9.3.3 For every $k \geq 1$, there is an injective group homomorphism

$$\begin{aligned} E_k/E_{5k} &\to \mathbb{Z}/p^{4k}\mathbb{Z} \\ (x, y) &\mapsto p^{-k}\frac{x}{y} (\text{mod } p^{4k}). \end{aligned}$$

Hence E_k has finite index (a power of p) in E_1.

We can now derive the following important theorem on torsion points.

Theorem 9.3.4 — Lutz-Nagell. Let E be an elliptic curve defined over $\mathbb{Q}$ by an **integral** short Weierstrass equation

$$Y^2 = X^3 + AX + B.$$

If $P = (x, y) \in E(\mathbb{Q})$ has finite order, then

1. the coordinates $x, y \in \mathbb{Z}$, and
2. either $y = 0$ or $y^2 \mid \Delta$ (where $\Delta = -4A^3 - 27B^2$).

Proof. Suppose that P has order $n \geq 2$. If $x \notin \mathbb{Z}$ then, there exists prime p such that $\mathrm{ord}_p(x) = v_p(x) < 0$, which implies that $\mathrm{ord}_p(x) = v_p(x) = -2k$ for some $k \geq 1$. So, in the p-adic filtration

$$E(\mathbb{Q}) \supset E_1 \supset E_2 \supset \cdots \supset \{0\},$$

we have $P \in E_k \setminus E_{k+1}$. This means that $v_p(u) = k$, where $\tilde{P} = (u,v)$.

Case 1: $p \nmid n$. Then, we have

$$nP = 0 \Rightarrow \widetilde{nP} = \mathscr{O} = (0,0) \Rightarrow u(\widetilde{nP}) = 0.$$

By Lemma 9.3.2, this means that

$$0 = u(\widetilde{nP}) \equiv n \cdot u(\tilde{P}) (\bmod\ p^{5k}) \equiv nu (\bmod\ p^{5k}),$$

which implies that $v_p(nu) \geq 5k$. But, we have

$$v_p(nu) = v_p(n) + v_p(u) = 0 + k,$$

so $k \geq 5k$, which is a contradiction.

Case 2: $p \mid n$. We replace P by the point $Q = (n/p)P$, which has order p. As before, we have that

$$v_p(pu) = 1 + k \geq 5k,$$

which is again a contradiction. This proves (1).
To prove (2), assume that $P = (x,y)$, with $x,y \in \mathbb{Z}$, has finite order n. If $n = 2$ then $y = 0$. Otherwise $n \geq 3$ and $2P \neq 0$. Now $2P$ also has finite order, so has integral coordinates by (1). This implies that

$$x(2P) = \frac{(x^2 - A)^2 - 8Bx}{4y^2} \in \mathbb{Z},$$

hence $y^2 \mid (x^2 - A)^2 - 8Bx$. But we also know that $y^2 \mid x^3 + Ax + B$. A straightforward calculation shows that

$$\Delta = -(4A^3 + 27B^2) = -(3x^2 + 4A)((x^2 - A)^2 - 8Bx) + (3x^3 - 5Ax - 27B)(x^3 + Ax + B).$$

Therefore, $y^2 \mid \Delta$. ■

Corollary 9.3.5 The torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is finite.

Example 9.3.5.1 (a) Let E be the curve given by $Y^2 = X^3 + 4$, with $\Delta = -27(4)^2 = -3(12)^2$. If $P = (x,y)$ has finite order then, either $y = 0$ or $|y| \mid 12$, i.e. $y \in \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12\}$.

$\lvert y\rvert$	0	1	2	3	4	6	12
y^2	0	1	4	9	16	36	144
$y^2 - 4$	-4	-3	0	5	12	32	140
x	–	–	0	–	–	–	–

So the only two possibilities are $P = (0,2)$ or $-P = (0,-2)$. In fact, $2P = -P$ so P has order 3 (the line $y = 2$ intersects E at P with multiplicity 3, so $P + P + P = 0$).

(b) Let E be given by $Y^2 = X^3 + 8$, with $\Delta = -27 \cdot 8^2 = -3(24)^2$. Then if $P = (x,y)$ has finite order then either $y = 0$ or $|y| \mid 24$. For $y = 0$, one gets $T = (-2,0)$ which has order 2. For $y = 3$, we obtain the point $P = (1,3)$. Since $2P = (-7/4, -13/8)$ is not integral, it must have infinite order. Therefore P also has infinite order. The value $y = 4$ yields

the point $Q = (2,4)$, which also has infinite order since $2Q = (-7/4, 13/8) = -2P$. In particular $P+Q = T$.

9.4 Reduction mod p

Let $E/\mathbb{Q}$ be an elliptic curve given by an integral equation $Y^2 = X^3 + AX + B$. If the discriminant of E has lots of prime factors, determining the $\mathbb{Q}$-torsion using only the Lutz-Nagell Theorem can be time-consuming: for each candidate y we need to solve a cubic equation. An alternative is the reduction modulo primes as we will see in this section.

Lemma 9.4.1 Let $E : Y^2 = X^3 + AX + B$, with $A, B \in \mathbb{Z}$, be an elliptic curve given by an integral equation, and let $p \nmid 2\Delta$. Let $r_p : E(\mathbb{Q}) \to \overline{E}(\mathbb{F}_p)$ be the reduction map, and let $P = (x,y) \in E(\mathbb{Q})$. Then $r_p(P) = 0$ if and only if $P \in E_1$.

Proof. By Proposition 9.3.1, we can write

$$P = [x : y : 1] = \left[\frac{a}{c^2} : \frac{b}{c^3} : 1\right] = [ac : b : c^3],$$

with $a, b, c \in \mathbb{Z}$, $c > 0$ and $\gcd(a,c) = \gcd(b,c) = 1$. (Note that the integers ac, b, c^3 are coprime.) Then, we see that

$$r_p(P) = \bar{P} = [\bar{a}\bar{c} : \bar{b} : \bar{c}^3].$$

So

$$P \in E_1 \Leftrightarrow p \mid c \Leftrightarrow \bar{P} = [0 : \bar{b} : 0] = [0 : 1 : 0].$$

■

Theorem 9.4.2 Let $E/\mathbb{Q}$ be an elliptic curve given by an integral equation $Y^2 = X^3 + AX + B$, and p a prime of good reduction for E ($p \nmid 2\Delta$). Then the map

$$\begin{aligned} r_p : E(\mathbb{Q}) &\to \overline{E}(\mathbb{F}_p) \\ P &\mapsto \bar{P} \end{aligned}$$

is a group homomorphism whose kernel is E_1:

$$E_1 := \{P = (x,y) \in E(\mathbb{Q}) : v_p(x) \leq -2, v_p(y) \leq -3\} \cup \{0\}.$$

Proof. We know that r_p is well-defined and that $\bar{P} = 0 \Leftrightarrow P \in E_1$. So we only have to prove that r_p is a group homomorphism.
Suppose that $L : aX + bY + cZ = 0$ is line in $\mathbf{P}^2(\mathbb{Q})$ which intersects $E(\mathbb{Q})$ in three points P_1, P_2, P_3 so that $P_1 + P_2 + P_3 = 0$. We need to show that L reduces to a line $\overline{L}$ in $\mathbf{P}^2(\mathbb{F}_p)$ which intersects $\overline{E}(\mathbb{F}_p)$ in $\bar{P}_1, \bar{P}_2, \bar{P}_3$ with the correct multiplicity; so that $\bar{P}_1 + \bar{P}_2 + \bar{P}_3 = 0$.
Without loss of generality, we can assume $a, b, c \in \mathbb{Z}$ with $\gcd(a,b,c) = 1$. Then, L reduces to the line $\overline{L} : \bar{a}X + \bar{b}Y + \bar{c}Z = 0$. Let $P = [x : y : z] \in \mathbf{P}^2(\mathbb{Q})$ be on L. Again, we can assume that $x, y, z \in \mathbb{Z}$ and $\gcd(x,y,z) = 1$. Then, we see that $\bar{P} = [\bar{x} : \bar{y} : \bar{z}] \in \overline{L}$ since $\bar{a}\bar{x} + \bar{b}\bar{y} + \bar{c}\bar{z} = 0$. This shows that $\bar{P}_1, \bar{P}_2, \bar{P}_3 \in \overline{E}(\mathbb{F}_p) \cap \overline{L}(\mathbb{F}_p)$.
To finish the proof, we only need to show that these are the only points in $\overline{E}(\mathbb{F}_p) \cap \overline{L}(\mathbb{F}_p)$. By Bezout's Theorem, it is enough to show that $\overline{E}$ does not contain the line $\overline{L}$ altogether. We can show that the Weierstrass cubic $ZY^2 = X^3 + \bar{A}XZ^2 + \bar{B}Z^3$ is always irreducible, i.e. never contains a line (even when it is singular). ■

Theorem 9.4.3 — Reduction Theorem. Let $p \geq 3$ be a prime of good reduction for an elliptic curve E over $\mathbb{Q}$ given by an integral short Weierstrass equation. Then, the reduction mod p map r_p is injective on the torsion subgroup, i.e.

$$\ker(r_p) \cap E(\mathbb{Q})_{\text{tors}} = \{0\}.$$

Proof. By Theorem 9.4.2, $\ker(r_p) = E_1$. Therefore, if $P \in \ker(r_p)$ then P is not integral. So by the Lutz-Nagell Theorem, P has infinite order. ■

By the above proposition, if we restrict r_p to $E(\mathbb{Q})_{\text{tors}}$, we get an injective group homomorphism

$$r_p : E(\mathbb{Q})_{\text{tors}} \hookrightarrow \overline{E}(\mathbb{F}_p).$$

By Lagrange Theorem then

Corollary 9.4.4 Let $p \geq 3$ be a prime of good reduction for an elliptic curve E over $\mathbb{Q}$ given by an integral short Weierstrass equation. Then,

$$\#E(\mathbb{Q})_{\text{tors}} \mid \#\overline{E}(\mathbb{F}_p).$$

Example 9.4.4.1 Let $E : Y^2 = X^3 + 4$, with $\Delta = -432$. Then E has good reduction at any prime $p \geq 5$. Reducing mod 5, we get the curve $\overline{E} : Y^2 = X^3 - 1$.

x	0	1	-1	2	-2
x^3	0	1	-1	-2	2
x^3-1	-1	0	-2	2	1
y	± 2	0	$-$	$-$	± 1

So, we have

$$\overline{E}(\mathbb{F}_5) = \{0, (1,0), (0,\pm 2), (-2,\pm 1)\}.$$

This gives $\#\overline{E}(\mathbb{F}_5) = 6$, and implies that $\#E(\mathbb{Q})_{\text{tors}} = 1, 2, 3$ or 6. Looking at $E(\mathbb{Q})$, we find that it has no point of order 2. But the point $P = (0,2)$ has order 3 (the line $Y = 2$ intersects E at P only). So $E(\mathbb{Q})_{\text{tors}}$ is a group of order 3 generated by P.

Example 9.4.4.2 Let $E : Y^2 = X^3 + 8$, with $\Delta = -27 \cdot 8^2$, it has good reduction at all prime $p \geq 5$. The point $T = (-2,0)$ is a 2-torsion point on E. For the prime $p = 5$, we find

$$\overline{E}_5(\mathbb{F}_5) = \{0, (1,\pm 2), (2,\pm 1), (-2,0)\}.$$

So $\#\overline{E}_5(\mathbb{F}_5) = 6$ and $\#E(\mathbb{Q})_{\text{tors}} \mid 6$. Since $\#E(\mathbb{Q})_{\text{tors}}$ is a multiple of 2, it must be 2 or 6. Looking at other primes, we find $\#\overline{E}_7(\mathbb{F}_7) = \#\overline{E}_{11}(\mathbb{F}_{11}) = 12$. However, for $p = 13$, we get $\#\overline{E}_{13}(\mathbb{F}_{13}) = 16$. This implies that $E(\mathbb{Q})_{\text{tors}} = \langle T \rangle$ has order 2.

Example 9.4.4.3 Let E be the curve given by $Y^2 = X^3 + 18X + 72$. It hast discriminant $\Delta = -4(18)^3 - 27(72)^2 = -163296 = -2^5 \cdot 3^3 \cdot 7$. Using Lutz-Nagell's Theorem to look for torsion points would require us to check 25 values of y. Instead, we use reduction mod 5 and 11. This gives $\#\overline{E}_5(\mathbb{F}_5) = 5$ and $\#\overline{E}_{11}(\mathbb{F}_{11}) = 8$, which implies that $E(\mathbb{Q})_{\text{tors}} = \{0\}$.

Let E be an elliptic curve over $\mathbb{Q}$. The torsion subgroup can be easily computed thanks to the following result, combined with the Lutz-Nagell Theorem and the Reduction Theorem,

Theorem 9.4.5 — Mazur. Let E be an elliptic curve over $\mathbb{Q}$, then

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} C_n \ (n = 1, \ldots, 10 \text{or } n = 12) \\ \\ C_2 \times C_{2n} \ (n = 1, 2, 3, 4). \end{cases}$$

Heights

Heights on elliptic curves

Isogenies and descent
Isogenies
2-isogenies and the descent map

The Weak Mordell-Weil Theorem

The Mordell-Weil Theorem

10. The Mordell–Weil Theorem

Let E be an elliptic curve over $\mathbb{Q}$, we will show that $E(\mathbb{Q})$ is finitely generated. We will proceed in two steps:

Step 1: We will prove that $E(\mathbb{Q})/2E(\mathbb{Q})$ is **finite**: **Weak Mordell-Weil Theorem**.

Step 2: We use the theory of **heights** of rational points to deduce the **Mordell-Weil Theorem** which asserts that $E(\mathbb{Q})$ is **finitely generated**.

This strategy goes back to Fermat, and is often called the 2-*descent method*. To illustrate this elegant and power method, consider the congruence number curve $E : Y^2 = X^3 - X$. Our proof of the Weak Mordell-Weil Theorem will show that there is a canonical isomorphism

$$E(\mathbb{Q})[2] \simeq E(\mathbb{Q})/2E(\mathbb{Q}),$$

where $E(\mathbb{Q})[2] = \{0,(0,0),(\pm 1,0)\}$ is the subgroup of the 2-torsion containing only points whose coordinates are rational. Consequently, given $P \in E(\mathbb{Q})$, there exists a point $T_1 \in E(\mathbb{Q})[2]$ and $P_1 \in E(\mathbb{Q})$ such that $P - T_1 = 2P_1$. By repeating this argument, there exist $T_2 \in E(\mathbb{Q})[2]$ and $P_2 \in E(\mathbb{Q})$ such that $P_1 - T_2 = 2P_2$, and $T_3 \in E(\mathbb{Q})[2]$, $P_3 \in E(\mathbb{Q})$ such that $P_2 - T_3 = 2P_3$, etc. We will use the notion of heights to show that the sequence $P, P_1, P_2, P_3, \ldots$ terminates; hence that $E(\mathbb{Q})$ is *finitely* generated.

We will develop the theory of heights, and use it to prove Step 2. We will do this in complete generality. However, we will only prove Step 1 for a curve $E/\mathbb{Q}$ with a 2-*torsion* point, i.e. of the form

$$E : Y^2 = (X - e)(X^2 + aX + b)$$

with $e, a, b \in \mathbb{Z}$. In fact, with the appropriate change of coordinates we move the 2-torsion point to $(0,0)$, and so we will assume that E is given by the equation

$$E : Y^2 = X(X^2 + AX + B), \qquad (*)$$

with $A, B \in \mathbb{Z}$ and discriminant $\Delta = B^2(A^2 - 4B) \neq 0$.

10.1 Heights

Let $n \geq 1$ be an integer, and $P \in \mathbf{P}^n(\mathbb{Q})$. Then we can choose representatives for the projective coordinates of P such that $P = [a_0 : \cdots : a_n]$ for $a_0, \ldots, a_n \in \mathbb{Z}$ with $\gcd(a_0, \ldots, a_n) = 1$. This representation is unique up to a sign. We define the **height** of P by

$$H(P) := \max\{|a_0|, \ldots, |a_n|\}.$$

Lemma 10.1.1 For all $c > 0$, the set $\{P \in \mathbf{P}^n(\mathbb{Q}) : H(x) \leq c\}$ is **finite**.

Proof. Choose a representative for $P \in \mathbf{P}^n(\mathbb{Q})$ such that $P = [a_0 : \cdots : a_n]$ for $a_0, \ldots, a_n \in \mathbb{Z}$ with $\gcd(a_0, \ldots, a_n) = 1$, for every positive c, we have that a_i is an integer with absolute value bounded by c in the set considered. Therefore the cardinality of the set $\{P \in \mathbf{P}^n(\mathbb{Q}) : H(x) \leq c\}$ is bounded by $(2(c+1))^{n+1}$. ■

We recall that, there is an injection

$$\mathbb{Q} \hookrightarrow \mathbf{P}^1(\mathbb{Q}), \qquad x \mapsto [x : 1],$$

so, identifying $\mathbb{Q}$ with its image under this map and, we define a height function on $\mathbb{Q}$ by

$$H(x) := H([x : 1]) \quad x \in \mathbb{Q}.$$

Equivalently, we can define the height of a rational number x by

$$H(x) = \max\{|a|, |b|\}, \text{ where } x = \frac{a}{b}, \text{ and } \gcd(a, b) = 1.$$

In particular, we have $H(0) = 1$, and it follows that

$$H(x) = H(-x) \quad \forall x \in \mathbb{Q}$$
$$H(x) = H(1/x) \quad \forall x \in \mathbb{Q}^\times.$$

Moreover, for all $c > 0$, the set $\{x \in \mathbb{Q} : H(x) \leq c\}$ is finite: this follows from Lemma 10.1.1.

The results that we are now going to present allow us to estimate the height of the image of a point under a map given by homogeneous polynomials. We will need them in order to understand the growth of the height function of an elliptic curve.

Let $f(x), g(x) \in \mathbb{Q}[x]$ be polynomials of degree m and n respectively, and let $R_{f,g}$ be their resultant. In Chapter 2, Lemma 2.2.1 and Theorem 2.2.2 we showed that

(i) There exist polynomials $u(x), v(x) \in \mathbb{Q}[x]$ of degree $\leq n-1$ and $m-1$ respectively, such that $vf + ug = R_{f,g}$, and that

(ii) f and g have a common factor which is non-constant if and only if $R_{f,g} = 0$.

Lemma 10.1.2 Let $F(X,Y), G(X,Y) \in \mathbb{Q}[X,Y]$ be two homogeneous polynomials of degree m and n respectively. Let f_1, g_1 (resp. f_2, g_2) be the dehomogenisation of F, G with respect to X (resp. Y). Then $R_{f_1,g_1} = R_{f_2,g_2}$. We call this quantity the **resultant** of F and G.

Proof. This follows from the definition, see Chapter 2. ■

Lemma 10.1.3 Let $F(X,Y), G(X,Y) \in \mathbb{Q}[X,Y]$ be two homogeneous polynomials of the same degree m. Let R be the resultant of F and G. Let

$$D(F,G) := \mathbf{P}^1(\mathbb{Q}) \setminus \{P : F(P) = G(P) = 0\}.$$

(i) The map

$$\begin{aligned} \phi : D(F,G) &\to \mathbf{P}^1(\mathbb{Q}) \\ P &\mapsto [F(P) : G(P)] \end{aligned}$$

is well-defined.

(ii) There exists $C > 0$ such that

$$H(\phi(P)) \leq CH(P)^m, \forall P \in D(F,G).$$

(iii) Assume that $R \neq 0$. Then, $D(F,G) = \mathbf{P}^1(\mathbb{Q})$, and there exists $C' > 0$ such that

$$H(\phi(P)) \geq C'H(P)^m, \forall P \in \mathbf{P}^1(\mathbb{Q}).$$

Proof. (i) We excluded all $P \in \mathbf{P}^1(\mathbb{Q})$ such that $F(P) = G(P) = 0$. Since both F and G are homogeneous of the same degree, we see that $\phi(P)$ is well-defined for all $P \in D(F,G)$.
(ii) Without loss of generality, we can assume that $F, G \in \mathbb{Z}[X,Y]$. Then, we can write

$$F(X,Y) = \sum_{i=0}^{m} c_i X^i Y^{m-i}, \; G(X,Y) = \sum_{i=0}^{m} c_i' X^i Y^{m-i}, \text{ with } c_i, c_i' \in \mathbb{Z}.$$

Let $P = [a : b] \in \mathbf{P}^1(\mathbb{Q})$, with $a, b \in \mathbb{Z}$ and $\gcd(a,b) = 1$. Then, we have

$$|F(a,b)| \leq \sum_{i=0}^{m} |c_i||a|^i|b|^{m-i} \leq \left(\sum_{i=0}^{m} |c_i| \right) \max\{|a|,|b|\}^m = C_1 H(P)^m.$$

Similarly, letting $C_2 = \sum_{i=0}^{m} |c_i'|$, we see that

$$|G(a,b)| \leq C_2 H(P)^m.$$

The constant $C = \max\{C_1, C_2\}$ clearly depends on F and G only, and we see that

$$H(\phi(P)) = \max\{|F(a,b)|, |G(a,b)|\} \leq CH(P)^m.$$

(iii) Since $R \neq 0$, both F and G never vanish at the same point; so $D(F,G) = \mathbf{P}^1(\mathbb{Q})$. Then, by Lemma 10.1.2, we can write

$$\begin{aligned} V_1(X,Y)F(X,Y) + U_1(X,Y)G(X,Y) &= RX^{2m-1}, \\ V_2(X,Y)F(X,Y) + U_2(X,Y)G(X,Y) &= RY^{2m-1}, \end{aligned}$$

where the $U_i, V_i \in \mathbb{Z}[X,Y]$ are homogeneous polynomials of degree $m-1$. By evaluating this at $P = [a : b]$, where $a, b \in \mathbb{Z}$ and $\gcd(a,b) = 1$, we see that

$$\begin{aligned} V_1(a,b)F(a,b) + U_1(a,b)G(a,b) &= Ra^{2m-1}, \\ V_2(a,b)F(a,b) + U_2(a,b)G(a,b) &= Rb^{2m-1}. \end{aligned}$$

Let $d = \gcd(F(a,b), G(a,b))$, then $d \mid R$. Writing $\phi(P) = [a' : b']$, where $a', b' \in \mathbb{Z}$ and $\gcd(a', b') = 1$, we see that

$$V_1(a,b)a' + U_1(a,b)b' = \frac{R}{d}a^{2m-1},$$
$$V_2(a,b)a' + U_2(a,b)b' = \frac{R}{d}b^{2m-1}.$$

From Part (ii), we know that there exists $C_1 > 0$ such that

$$|U_i(a,b)|, |V_i(a,b)| \leq C_1 H(P)^{m-1}.$$

This implies that

$$2C_1 H(P)^{m-1} H(\phi(P)) \geq \frac{|R|}{|d|} \max\left\{|a|^{2m-1}, |b|^{2m-1}\right\} = \frac{|R|}{|d|} H(P)^{2m-1}.$$

Dividing through by $2C_1 H(P)^{m-1}$, we get

$$H(\phi(P)) \geq \frac{|R|}{2|d|C_1} H(P)^m \geq \frac{1}{2C_1} H(P)^m.$$

So we can take $C' = \frac{1}{2C_1}$. ■

Lemma 10.1.4 Let $P_i = [a_i : b_i] \in \mathbf{P}^1(\mathbb{Q})$, $i = 1, 2$. Then $P_3 = [b_1 b_2 : a_1 b_2 + a_2 b_1 : a_1 a_2]$ is a point in $\mathbf{P}^2(\mathbb{Q})$, and we have

$$\frac{1}{2} H(P_1) H(P_2) \leq H(P_3) \leq 2H(P_1) H(P_2).$$

Proof. We can assume that $a_i, b_i \in \mathbb{Z}$ with $\gcd(a_i, b_i) = 1$. Then, it follows that $\gcd(b_1 b_2, a_1 b_2 + a_2 b_1, a_1 a_2) = 1$, so P_3 is a well-defined point in $\mathbf{P}^2(\mathbb{Q})$. By making use of the triangle inequality, we get

$$H(P_3) \leq 2H(P_1) H(P_2).$$

To prove the second inequality, we need to show that

$$H(P_1) H(P_2) \leq 2H(P_3),$$

which is the same as

$$\max\{|a_1|, |b_1|\} \cdot \max\{|a_2|, |b_2|\} \leq 2 \max\{|b_1 b_2|, |a_1 b_2 + a_2 b_1|, |a_1 a_2|\}.$$

Equivalently, we need to show that

$$|a_1 a_2|, |a_1 b_2|, |a_2 b_1|, |b_1 b_2| \leq 2 \max\{|b_1 b_2|, |a_1 b_2 + a_2 b_1|, |a_1 a_2|\}.$$

In fact, we only need to prove that

$$|a_1 b_2|, |a_2 b_1| \leq 2 \max\{|b_1 b_2|, |a_1 b_2 + a_2 b_1|, |a_1 a_2|\}.$$

By symmetry, it is enough to show that

$$|a_1 b_2| \leq 2 \max\{|b_1 b_2|, |a_1 b_2 + a_2 b_1|, |a_1 a_2|\}.$$

There is nothing to prove if $a_1b_2 = 0$; or either $2|b_1b_2| \geq |a_1b_2|$ or $2|a_1a_2| \geq |a_1b_2|$. So we assume that $a_1b_2 \neq 0$, and that $2|b_1b_2|, 2|a_1a_2| < |a_1b_2|$. In this case, we have $|b_1| < \frac{1}{2}|a_1|$ and $|a_2| < \frac{1}{2}|b_2|$. Then, by making use of the triangle inequality, we get

$$|a_1b_2| = |a_1b_2 + a_2b_1 - a_2b_1| \leq |a_1b_2 + a_2b_1| + |a_2b_1| < |a_1b_2 + a_2b_1| + \frac{1}{4}|a_1b_2|.$$

This implies that

$$\frac{3}{4}|a_1b_2| < |a_1b_2 + a_2b_1| \implies |a_1b_2| < 2|a_1b_2 + a_2b_1|.$$

This proves the second inequality. ■

10.2 Heights on elliptic curves

We now introduce the notion of heights on elliptic curves.

Definition 10.1 Let $x \in \mathbb{Q}$, we define the **logarithmic height** of x by

$$h(x) := \log H(x).$$

Definition 10.2 Let E be an elliptic curve over $\mathbb{Q}$. We define the **height** function on E by

$$h : E(\mathbb{Q}) \to \mathbb{R}, \quad h(P) := \begin{cases} \log H(x), & \text{if } P = (x,y) \neq 0, \\ 0, & \text{if } P = 0(\infty). \end{cases}$$

The height function on E is usually called h the **naive height**.

Lemma 10.2.1 For all $c > 0$ the set $\{P \in E(\mathbb{Q}) : h(P) \leq c\}$ is finite.

Proof. Considering the projective equation of E, it is clear that any $P = (x,y) \in E(\mathbb{Q})$ can be seen as a point in $\mathbf{P}^2(\mathbb{Q})$, then the result follows from Lemma 10.1.1. ■

Lemma 10.2.2 — Approximate Parallelogram Law. There exists $c_1 > 0$ depending on E only such that, for all $P, Q \in E(\mathbb{Q})$, we have

$$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)| < c_1.$$

This is a consequence of the following two lemmas.

Lemma 10.2.3 There exists $c_2 > 0$ such that, for all $P, Q \in E(\mathbb{Q})$,

$$h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + c_2.$$

Lemma 10.2.4 There exists $c_3 > 0$ such that, for all $P \in E(\mathbb{Q})$,

$$4h(P) \leq h(2P) + c_3.$$

Proof of Approximate Parallelogram Law. By Lemma 10.2.4, we have

$$4h(P) + 4h(Q) \leq h(2P) + h(2Q) + 2c_3.$$

Applying Lemma 10.2.3 to the pair $(P+Q, P-Q)$ we see that

$$h(2P) + h(2Q) \leq 2h(P+Q) + 2h(P-Q) + c_2,$$

hence

$$4h(P) + 4h(Q) \leq 2h(P+Q) + 2h(P-Q) + (2c_3 + c_2),$$

which implies that

$$2h(P) + 2h(Q) \leq h(P+Q) + h(P-Q) + c',$$

where $c' = c_3 + c_2/2$. This gives the Approximate Parallelogram Law with

$$c_1 = \max\{c_2, c_3 + c_2/2\}.$$

■

Proof of Lemma 10.2.3. Without loss of generality, we can assume that E is given by $Y^2 = X^3 + AX + B$, with $A, B \in \mathbb{Z}$. We write

$$x_1 = x(P) = \frac{a_1}{b_1}, \qquad x_2 = x(Q) = \frac{a_2}{b_2}, \qquad x_3 = x(P+Q) = \frac{a_3}{b_3}, \qquad x_4 = x(P-Q) = \frac{a_4}{b_4},$$

where $a_i, b_i \in \mathbb{Z}$ and $\gcd(a_i, b_i) = 1$. Let $H_i = H(x_i)$ and $h_i = h(x_i)$. We need to show that

$$h_3 + h_4 \leq 2h_1 + 2h_2 + c_2.$$

By making use of Equation 6.5, that is a relation we have computed proving the parallelogram law for degrees, we have

$$[1 : x_3 + x_4 : x_3x_4] = [(x_1 - x_2)^2 : 2(x_1x_2 + A)(x_1 + x_2) + 4B : (x_1x_2 - A)^2 - 4B(x_1 + x_2)].$$

By homogenisation, this gives

$$[b_3b_4 : a_3b_4 + a_4b_3 : a_3a_4] = [d_1 : d_2 : d_3],$$

where

$$\begin{aligned} d_1 &= (a_1b_2 - a_2b_1)^2, \\ d_2 &= 2(a_1a_2 + Ab_1b_2)(a_1b_2 + a_2b_1) + 4Bb_1^2b_2^2, \\ d_3 &= (a_1a_2 - Ab_1b_2)^2 - 4B(a_1b_2 + a_2b_1)b_1b_2. \end{aligned}$$

By Lemma 10.1.4, we have

$$H_3H_4 \leq 2\max\{|b_3b_4|, |a_3b_4 + a_4b_3|, |a_3a_4|\} \leq 2\max\{|d_1|, |d_2|, |d_3|\}.$$

The same argument as in the proof of Lemma 10.1.3 (ii) shows that there is a constant $C > 0$ such that

$$\max\{|d_1|, |d_2|, |d_3|\} \leq CH_1^2H_2^2.$$

Hence

$$H_3H_4 \leq 2CH_1^2H_2^2.$$

Taking logarithms, we obtain

$$h_3 + h_4 \leq 2h_1 + 2h_2 + c_2,$$

where $c_2 = \log(2C)$. ■

We now turn to the proof of Lemma 10.2.4.

Proof of Lemma 10.2.4. The duplication formula gives that

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = \frac{f(x)}{g(x)}.$$

Assume that $x = a/b$ in lowest terms, then we can write

$$x(2P) = \frac{f(a/b)}{g(a/b)} = \frac{F(a,b)}{G(a,b)},$$

where

$$F(X,Y) = X^4 - 2AX^2Y^2 - 8BXY^3 + A^2Y^4,$$
$$G(X,Y) = 4(X^3Y + AXY^3 + BY^4).$$

Now, let $u(x) = -(3x^2 + 4A)$ and $v(x) = (3x^3 - 5Ax - 27B)$. In Chapter 8, in the proof of the Lutz-Nagell Theorem, we showed that $vf + ug = \Delta \neq 0$. So the resultant $R_{f,g} = \Delta$ is non-zero. We apply Lemma 10.1.3 (iii) to the polynomials F and G, with $m = 4$. So there exists a constant $C_3 > 0$ such that

$$H(P)^4 \leq C_3 H(2P).$$

Taking logarithms then yields the desired inequalities. ■

We will replace the height function h by a function $\hat{h}$ which has slightly better properties, in particular the parallelogram law holds.

Definition 10.3 Let E be an elliptic curve over $\mathbb{Q}$. The **canonical height** on $E(\mathbb{Q})$ is defined by

$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$$
$$\hat{h}(P) := \lim_{n\to\infty} \frac{1}{4^n} h(2^n P).$$

Theorem 10.2.5 — Properties of the canonical height. Let E be an elliptic curve defined over $\mathbb{Q}$. Let $\hat{h}$ be the canonical height on $E(\mathbb{Q})$. Then, we have

1. $\hat{h}$ is well-defined and $\hat{h}(P) \geq 0$ for all $P \in E(\mathbb{Q})$.
2. There exists a constant $c_0 > 0$ such that

$$\forall P \in E(\mathbb{Q}),\ |h(P) - \hat{h}(P)| \leq c_0.$$

3. $\forall c > 0$, the set $\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq c\}$ is finite.
4. $\forall m \geq 1, \forall P \in E(\mathbb{Q})$, $\hat{h}(mP) = m^2\hat{h}(P)$.
5. Parallelogram Law: $\forall P, Q \in E(\mathbb{Q})$, $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$.
6. $\hat{h}(P) = 0 \iff P$ has finite order.

10.3 Isogenies and descent

In this section, we gather several results that will be needed for the proof of the main theorem of this chapter. Let K be a field, not necessarily $\mathbb{Q}$.

10.3.1 Isogenies

Definition 10.4 Let E_1 and E_2 be elliptic curves defined over a field K. An **isogeny** ϕ between E_1 and E_2 is a rational map $\phi : E_1(\overline{K}) \to E_2(\overline{K})$ that induces a group homomorphism from $E_1(\overline{K})$ to $E_2(\overline{K})$. Two elliptic curves are called **isogenous** if there is a non-constant isogeny between them.

A rational map between elliptic curves induces a group homomorphism if and only if it preserves the identity element:

Theorem 10.3.1 Let E_1 and E_2 be elliptic curves defined over a field K. Let $\phi : E_1(\overline{K}) \to E_2(\overline{K})$ be a map given by rationals functions. Then ϕ is an isogeny if and only if $\phi(0) = 0$.

Let E_1 and E_2 be elliptic curves defined over a field K, let $\alpha, \beta \in \mathrm{Hom}(E_1, E_2)$, the set of group homomorphism between $E_1(\overline{K})$ and $E_2(\overline{K})$. Point-wise addition $(\alpha+\beta)(P) = \alpha(P) + \beta(P)$ makes the set $\mathrm{Hom}(E_1, E_2)$ of isogenies from E_1 to E_2 into an additive abelian group. The map that sends every point on $E_1(\overline{K})$ to the point 0 on $E_2(\overline{K})$ is the zero isogeny. The zero isogeny is the identity element of this group. Composition of isogenies is possible only if the target of the first isogeny is equal to the starting elliptic curve for the other.

To complete our definition of isogeny we need to say exactly what we mean by a rational map. To do this we first introduce the function field of a curve, a concept that plays a key role in the general theory of algebraic curves. As this is an introductory course on elliptic curves, we will make only very limited use of function fields, just to have a more precise definition.

Definition 10.5 Let $\mathscr{C}$ be a projective curve defined over K by an irreducible homogeneous polynomial $f(x,y,z)$. The **function field** of $\mathscr{C}$ consists of rational functions g/h such that the following hold:

1. g and h are homogeneous elements of $K[x,y,z]$ of the same degree.
2. h does not lie in the ideal (f) (i.e. h is not constantly zero in $\mathscr{C}(\overline{K})$).
3. the functions g_1/h_1 and g_2/h_2 are considered equivalent whenever $g_1h_2 - g_2h_1 \in (f)$.

The function field of $\mathscr{C}$ is denoted $K(\mathscr{C})$. The fact that f is irreducible and $K[x,y,z]$ is a unique factorization domain (so every irreducible element is prime) makes it clear that $K(\mathscr{C})$ is, in fact, a field. The field $\overline{K}(\mathscr{C})$ is defined analogously, with $g, h \in \overline{K}[x,y,z]$.

Alternatively, if C is a plane curve defined over K by a polynomial equation $f(x,y) = 0$, one can define $K(C)$ as the fraction field of the ring $K[x,y]/(f)$.

Definition 10.6 Let $\mathscr{C}_1$ and $\mathscr{C}_2$ be projective curves defined over a field K. A **rational map** $\phi : \mathscr{C}_1 \to \mathscr{C}_2$ is given by $[\phi_x : \phi_y : \phi_z]$, with $\phi_x, \phi_y, \phi_z \in \overline{K}(\mathscr{C}_1)$, such that for every point $P \in \mathscr{C}_1(\overline{K})$ where ϕ_x, ϕ_y, and ϕ_z are all defined, the point $[\phi_x(P) : \phi_y(P) : \phi_z(P)]$ lies in $\mathscr{C}_2(\overline{K})$.

Note that $\phi = [\phi_x : \phi_y : \phi_z]$ is defined only up to scalar equivalence. There may be points $P \in \mathscr{C}_1(\overline{K})$ where one of ϕ_x, ϕ_y, and ϕ_z is not defined, but in this case it may still be possible to evaluate the map ϕ at P after rescaling by an element of $\overline{K}(\mathscr{C}_1)$.

All the definition given in Chapter 5 (degree, separable degree, inseparable degree, etc.) can be extended to isogenies: in particular, *endomorphism are isogenies* between the same elliptic curve.

Non constant isogenies are surjective (note that we are considering maps between $\overline{K}$-rational points of elliptic curves, if we do not work on the algebraic closure this is no longer true).

Let us remark that *isomorphisms are isogenies*: they are isogenies of degree one. It is possible to show that in any characteristic, an isomorphism τ between two elliptic curves E_1 and E_2 is a map $\tau : E_1(\overline{K}) \to E_2(\overline{K})$ of the form

$$\tau(x,y) = (ax+b, cy+dx+e)$$

for all $(x,y) \in E_1(\overline{K})$ with $a,b,c,d,e \in \overline{K}$, which is invertible, hence $a,c \neq 0$. In particular, if the elliptic curves are given by short Weierstrass equations, then an isomorphism is given exactly in the way described in Chapter 3.
An isogeny of degree n is usually called an n-isogeny. For the purposes of this course we will be mostly interested in 2-isogenies and in the next section we will see an example.

10.3.2 2-isogenies and the descent map

We will assume that $\mathrm{char}(K) \neq 2$, where K is our base field.

Lemma 10.3.2 Let E be a curve of the form $(*)$. Let $E' : Y^2 = X(X^2 + A'X + B')$, where $A' = -2A$ and $B' = A^2 - 4B$. Then, E' is an elliptic curve, and the map $\phi : E \to E'$ given by

$$\phi(P) := \begin{cases} \left(\frac{y^2}{x^2}, \frac{y(x^2-B)}{x^2}\right) & \text{if} \quad P = (x,y) \neq 0, (0,0) \\ 0 & \text{if} \quad P = 0 \,\text{or}\, (0,0), \end{cases}$$

is a 2-isogeny.

Proof. We want to show that ϕ is well defined. First, let $P = (x,y) \in E(\overline{K}) \setminus \{0,(0,0)\}$, and write $Q = \phi(P) = (x',y')$. We need to show that $Q \in E'(\overline{K})$. But, we see that

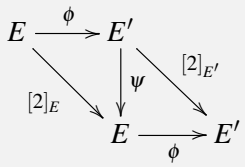
$$y'^2 = \frac{y^2(x^2-B)^2}{x^4} = \frac{y^2}{x^2}\frac{(x^4 - 2Bx^2 + B^2)}{x^2} = \frac{y^2}{x^2}\left(x^2 - 2B + \frac{B^2}{x^2}\right) = x'\left[\left(x + \frac{B}{x}\right)^2 - 4B\right].$$

By observing that

$$(x'-A)^2 = \left(\frac{y^2}{x^2} - A\right)^2 = \left(\frac{x^2 + Ax + B}{x} - A\right)^2 = \left(x + \frac{B}{x}\right)^2,$$

we obtain that $y'^2 = x'\left[(x'-A)^2 - 4B\right] = x'(x'^2 - 2Ax' + (A^2 - 4B))$. It remains to show that ϕ is a group homomorphism. We can do this by tedious computations. However, since ϕ is given by rational functions and $\phi(0) = 0$, we can use Theorem 10.3.1. ∎

Lemma 10.3.3 Let E be a curve of the form $(*)$, and E' as in Lemma 10.3.2. Then, there exists a homomorphism $\psi : E' \to E$ such that $\psi \circ \phi = [2]_E$ and $\phi \circ \psi = [2]_{E'}$; i.e. such that the following diagram commutes:



Proof. By applying Lemma 10.3.2 to E', we get the curve $E'' : Y^2 = X(X^2 + 4AX + 16B)$, and a homomorphism $\psi' : E' \to E''$. The curve E'' is isomorphic to E, it is a twist by $1/2$: the change of coordinates $(x,y) \mapsto (x/4, y/8)$ gives the isomorphism. By composing these morphisms, we get the map $\psi : E' \to E$ given by

$$\psi(P') := \begin{cases} \left(\frac{y'^2}{4x'^2}, \frac{y'(x'^2 - B')}{8x'^2}\right) & \text{if} \quad P' = (x',y') \neq 0, (0,0) \\ \\ 0 & \text{if} \quad P' = 0 \text{or} (0,0). \end{cases}$$

For $P = (x,y) \in E(\overline{K})$, let $Q = (x_Q, y_Q) = \psi(\phi(P))$. Then, by definition, we have

$$\begin{aligned} x_Q &= \left(\frac{y(x^2 - B)}{x^2}\right)^2 \times \frac{1}{4}\left(\frac{x^2}{y^2}\right)^2 = \frac{(x^2 - B)^2}{4y^2} \\ &= \left(\frac{3x^2 + 2Ax + B}{2y}\right)^2 + \frac{(x^2 - B)^2}{4y^2} - \left(\frac{3x^2 + 2Ax + B}{2y}\right)^2 \\ &= \left(\frac{3x^2 + 2Ax + B}{2y}\right)^2 + \frac{(x^2 - B)^2 - (3x^2 + 2Ax + B)^2}{4y^2} \\ &= \left(\frac{3x^2 + 2Ax + B}{2y}\right)^2 - \frac{(2x + A)x(x^2 + Ax + B)}{y^2} \\ &= \left(\frac{3x^2 + 2Ax + B}{2y}\right)^2 - A - 2x. \end{aligned}$$

This is precisely the x-coordinate of the point $2P$. Therefore, we must have $\psi(\phi(P)) = 2P$ or $\psi(\phi(P)) = -2P$. Replacing ψ by $-\psi$, if necessary, we see that $\psi \circ \phi = [2]_E$.
To show that $\phi \circ \psi = [2]_{E'}$, we first observe that ϕ and ψ are surjective on $\overline{K}$-points by construction. Now, from definitions, it follows that

$$(\phi \circ \psi) \circ \phi = \phi \circ (\psi \circ \phi) = \phi \circ [2]_E = [2]_{E'} \circ \phi.$$

Forgetting the intermediate equalities, this means that

$$(\phi \circ \psi) \circ \phi = [2]_{E'} \circ \phi.$$

Since ϕ is surjective, we conclude that $\phi \circ \psi = [2]_{E'}$. ■

R The result described in the previous lemma generalize: to any isogeny ϕ between two elliptic curves E_1 and E_2 it is possible to associate a **dual isogeny** $\hat{\phi} : E_2 \to E_1$, which is an isogeny of the same degree as ϕ such that $\hat{\phi} \circ \phi = [\deg(\phi)]_{E_1}$ and $\phi \circ \hat{\phi} = [\deg(\phi)]_{E_2}$. In the previous lemma $\psi = \hat{\phi}$.

Lemma 10.3.4 Let E, E', ϕ and ψ be as in Lemma 10.3.3; also, let $Q = (x', y') \in E'(K)$. Then, $Q \in \phi(E(K))$ if and only if $x' = 0$ and B' is a square in $K^\times$, or x' is a square in $K^\times$.

Proof. It is clear that, if $P = (x, y) \in E(K)$ and $Q = \phi(P) = (x', y')$, then x' is a square in K. Conversely, assume that $Q = (x', y') \in E'(K)$ and that x' is a square in $K^\times$. We recall that $\phi : E(\overline{K}) \to E'(\overline{K})$ is surjective. So, there exists $P = (x, y) \in E(\overline{K})$ such that $\phi(P) = Q$, and we only need to show that $P \in E(K)$. We recall that $y^2 = x(x^2 + Ax + B)$, and write

$$y' = \frac{y(x^2 - B)}{x^2} = \frac{y}{x} \times \frac{x^2 - B}{x},$$
$$x' = \frac{x^2 + Ax + B}{x} = \frac{x^2 - B}{x} + A + \frac{2B}{x}.$$

Since x' is a square in $K^\times$ and $y' \in K$, we see that $y/x, (x^2 - B)/x \in K$, and hence $x, y \in K$. (We leave the case $x' = 0$ as an exercise.) ■

Proposition 10.3.5 — The 2-descent map. Let E be an elliptic curves over K given by $Y^2 = X(X^2 + AX + B)$. Let $\delta : E(K) \to K^\times/(K^\times)^2$ be defined by

$$\delta(P) := \begin{cases} (K^\times)^2 & \text{if } P = 0, \\ B(K^\times)^2 & \text{if } P = (0,0), \\ x(K^\times)^2 & \text{if } P = (x,y) \neq (0,0). \end{cases}$$

Then, we have:

(i) δ is a group homomorphism.

(ii) $\ker(\delta) = \psi(E'(K))$.

Proof. By definition $\delta(0) = 1$, so to show that δ is a group homomorphism, we only need to show that if $P_1 + P_2 + P_3 = 0$ then $\delta(P_1)\delta(P_2)\delta(P_3) = 1$.
We first observe that, if all the $P_i = 0$ then there is nothing to prove. Also, if one of the $P_i = 0$, say P_1, then $P_2 = -P_3$ and

$$\delta(P_2)\delta(P_3) = \delta(P_2)\delta(-P_2) = \delta(P_2)^2 = 1,$$

since $\delta(P) = \delta(-P)$, $\forall\, P \in E(K)$, by definition. So we may assume that $P_i \neq 0$, $i = 1, 2, 3$. In that case, the $P_i = (x_i, y_i)$ are the intersections of E with a non-vertical line $L : Y = mX + c$.

Case 1: None of the P_i is equal to $T = (0,0)$. Then, we have

$$f(X) - (mX + c)^2 = (X - x_1)(X - x_2)(X - x_3).$$

Substituting $X = 0$ gives $f(0) = 0$, hence $x_1x_2x_3 = c^2$ is a non-zero square in K. This means that $\delta(P_1)\delta(P_2)\delta(P_3) = 1$.

Case 2: Exactly one of the P_i equals T, say $P_1 = T$. Then, x_2, x_3 are the roots of the polynomial $X^2 + (A - m^2)X + B = 0$. So $x_2x_3 = B$ and $\delta(P_1)\delta(P_2)\delta(P_3) = B^2(K^\times)^2 = 1$.

Case 3: Two of the P_i equal T, say $P_1 = P_2 = T$. In this case, we must have $P_3 = 0$. Hence, $\delta(P_1)\delta(P_2)\delta(P_3) = 1$. This proves (i).
The second part of the proposition follows from Lemma 10.3.4. ■

R Since $\ker(\delta) = \psi(E'(K))$, the First Isomorphism Theorem implies that the map δ induces an injection

$$E(K)/\psi(E'(K)) \hookrightarrow K^\times/(K^\times)^2,$$

which we will also denote by δ.

We conclude this section with the following lemma which we will need shortly.

Lemma 10.3.6 Let $\phi : A \to B$ and $\psi : B \to A$ be homomorphisms of abelian groups; and define the maps

$$\begin{aligned}\theta : A/\mathrm{im}(\psi\circ\phi) &\to A/\mathrm{im}(\psi)\\ x+\mathrm{im}(\psi\circ\phi) &\mapsto x+\mathrm{im}(\psi),\end{aligned}$$

and

$$\begin{aligned}\eta : B &\to A/\mathrm{im}(\psi\circ\phi)\\ x &\mapsto \psi(x)+\mathrm{im}(\psi\circ\phi).\end{aligned}$$

Then, they induce an exact sequence

$$0 \to B/(\ker(\psi)+\mathrm{im}(\phi)) \xrightarrow{\theta'} A/\mathrm{im}(\psi\circ\phi) \xrightarrow{\theta} A/\mathrm{im}(\psi) \to 0.$$

Hence, if $A/\mathrm{im}(\psi)$ and $B/\mathrm{im}(\phi)$ are finite, so is $A/\mathrm{im}(\psi\circ\phi)$.

Proof. To show that the sequence is exact, we only need to show that $\mathrm{im}(\eta) = \ker(\theta)$ and $\ker(\eta) = \ker(\psi)+\mathrm{im}(\phi)$. Then by the First Isomorphism Theorem, we will have that η induces an isomorphism

$$\theta' : B/(\ker(\psi)+\mathrm{im}(\phi)) \simeq \ker(\theta).$$

But the equality $\mathrm{Im}(\eta) = \ker(\theta)$ follows from the definition. So it remains to prove that $\ker(\eta) = \ker(\psi)+\mathrm{im}(\phi)$. But, we see that

$$\begin{aligned}x' \in \ker(\eta) &\iff \eta(x') = \psi(x')+\mathrm{im}(\psi\circ\phi) = \mathrm{im}(\psi\circ\phi)\\ &\iff \psi(x') = \psi(\phi(x)) \text{ for some } x\in A \iff \psi(x'-\phi(x)) = 0 \text{ for some } x\in A\\ &\iff x'-\phi(x) \in \ker(\psi) \text{ for some } x\in A \iff x' \in \ker(\psi)+\mathrm{im}(\phi).\end{aligned}$$

This means that $\ker(\eta) = \ker(\psi)+\mathrm{im}(\phi)$.
Finally, since $\mathrm{im}(\phi) \subset \ker(\psi)+\mathrm{im}(\phi)$, the canonical map $B/\mathrm{im}(\phi) \to B/(\ker(\psi)+\mathrm{im}(\phi))$ is surjective. Therefore, if $A/\mathrm{im}(\psi)$ and $B/\mathrm{im}(\phi)$ are finite, so is $A/\mathrm{im}(\psi\circ\phi)$. ■

R (a) We recall that, if $\phi : A \to B$ is a homomorphism of abelian groups, the *cokernel* of ϕ is defined by $\mathrm{coker}(\phi) = B/\mathrm{im}(\phi)$. So, Lemma 10.3.6 also gives the exact sequence

$$\mathrm{coker}(\phi) \xrightarrow{\theta'} \mathrm{coker}(\psi\circ\phi) \xrightarrow{\theta} \mathrm{coker}(\psi) \to 0.$$

(b) By the Second Isomorphism Theorem, we have

$$\frac{B}{\ker(\psi)+\mathrm{im}(\phi)} \simeq \frac{B/\mathrm{im}(\phi)}{(\ker(\psi)+\mathrm{im}(\phi))/\mathrm{im}(\phi)} \text{ and } \frac{\ker(\psi)+\mathrm{im}(\phi)}{\mathrm{im}(\phi)} \simeq \frac{\ker(\psi)}{\ker(\psi)\cap\mathrm{im}(\phi)}.$$

10.4 The Weak Mordell-Weil Theorem

In this section, we prove the finiteness of the quotient $E(\mathbb{Q})/2E(\mathbb{Q})$.

Let $(\mathbb{Q}^\times)^2$ be the subgroup of all squares in $\mathbb{Q}^\times$, and consider the quotient group

$$G := \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

Every coset is of the form $x(\mathbb{Q}^\times)^2$, where x is a non-zero *squarefree* integer.

Lemma 10.4.1 Let S be a finite set of primes, and set

$$\mathbb{Q}(S,2) := \left\{a(\mathbb{Q}^\times)^2 \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \middle|\ a \text{ is squarefree and a prime } p \mid a \iff p \in S\right\}.$$

This is a **finite** subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ of cardinality 2^{s+1}, where $s = \#S$.

Proof. We first observe that $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is a 2-group, i.e. every element $a(\mathbb{Q}^\times)^2$ has order at most 2 since

$$a(\mathbb{Q}^\times)^2 \cdot a(\mathbb{Q}^\times)^2 = a^2(\mathbb{Q}^\times)^2 = (\mathbb{Q}^\times)^2.$$

Let $a(\mathbb{Q}^\times)^2, b(\mathbb{Q}^\times)^2 \in \mathbb{Q}(S,2)$ be such that a and b are squarefree and only divisible by primes $p \in S$. Then, a prime $p \mid ab \iff p \in S$, and so

$$(ab)^{-1}(\mathbb{Q}^\times)^2 = ab(\mathbb{Q}^\times)^2 \in \mathbb{Q}(S,2).$$

Hence $\mathbb{Q}(S,2)$ is a subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$. Since, we have

$$\mathbb{Q}(S,2) = \left\{\pm(\textstyle\prod_{p\in S'} p)(\mathbb{Q}^\times)^2 \,|\, S' \subseteq S\right\},$$

it follows that $\#\mathbb{Q}(S,2) = 2^{s+1}$. ∎

Example 10.4.1.1 (a) For $S = \emptyset$, $\mathbb{Q}(S,2) = \left\{\pm(\mathbb{Q}^\times)^2\right\}$.

(b) For $S = \{2\}$, $\mathbb{Q}(S,2) = \left\{\pm(\mathbb{Q}^\times)^2, \pm 2(\mathbb{Q}^\times)^2\right\}$.

(c) For $S = \{2,5\}$, $\mathbb{Q}(S,2) = \left\{\pm(\mathbb{Q}^\times)^2, \pm 2(\mathbb{Q}^\times)^2, \pm 5(\mathbb{Q}^\times)^2, \pm 10(\mathbb{Q}^\times)^2\right\}$.

The following result together with Lemma 10.3.6 will be the key ingredients in the proof of the Weak Mordell-Weil Theorem.

Proposition 10.4.2 Let E be an elliptic curve over $\mathbb{Q}$ given by an integral equation

$$Y^2 = X(X^2 + AX + B),\ A, B \in \mathbb{Z}.$$

Let $S := \{p \text{ prime} : p \mid B\}$. Then $\mathrm{im}(\delta) \subset \mathbb{Q}(S,2)$; hence is **finite**.

Proof. Let p be a prime, and $P = (x,y) \in E(\mathbb{Q})$ with $x \neq 0$. If $v_p(x) < 0$, then $v_p(x)$ is even by Proposition 9.3.1. This means that, if $v_p(x)$ is odd, then $v_p(x) > 0$. We will show that $v_p(x)$ is odd only if $p \mid B$, which will imply that $\delta(P)$ belongs to $\mathbb{Q}(S,2)$.
Since E is integral, $v_p(x) \geq 0$ implies that $v_p(x^2 + Ax + B) \geq 0$. Furthermore, from

$$x(x^2 + Ax + B) = y^2,$$

we see that $v_p(x) + v_p(x^2 + Ax + B) = 2v_p(y)$ is even. Therefore, it follows that

$$v_p(x) \text{ is odd} \iff v_p(x^2 + Ax + B) \text{ is odd} \implies v_p(B) \geq 1.$$

Since $\delta(0), \delta(0,0) \in \mathbb{Q}(S,2)$ by definition, this concludes the proof of the proposition. ∎

The following result provides a method for computing $\mathrm{im}(\delta)$. We will need it when using the Weak Mordell-Weil Theorem in practice, as we will see shortly.

Corollary 10.4.3 The image of δ consists of the classes $b(\mathbb{Q}^\times)^2$ such that

(i) $b \mid B$ is squarefree, and

(ii) the equation

$$bl^4 + Al^2m^2 + (B/b)m^4 = n^2 \tag{10.1}$$

has a solution $(l,m,n) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$.

(Note that $\delta(0,0)$ is given by the squarefree part of B.)

Proof. Let $P = (x,y) \in E(\mathbb{Q})$, with $x \neq 0$; and write $x(\mathbb{Q}^\times)^2 = b(\mathbb{Q}^\times)^2$, where $b \in \mathbb{Z}$ is squarefree. Then, by Proposition 10.4.2, it follows that $b \mid B$. By combining Proposition 9.3.1 and Proposition 10.4.2, we can write

$$P = \left(\frac{bl^2}{m^2}, \frac{bln}{m^3}\right),$$

where $b,m,n,l \in \mathbb{Z}$, $m > 0$ and $\gcd(b,m) = \gcd(l,m) = \gcd(m,n) = 1$. By substituting this into $(*)$ and clearing denominators, we get

$$b^2l^2n^2 = bl^2(b^2l^4 + Abl^2m^2 + Bm^4) = b^2l^2(bl^4 + Al^2m^2 + (B/b)m^4).$$

Note that $bl \neq 0$ since $x \neq 0$. So by simplifying the above equality, we obtain

$$n^2 = bl^4 + Al^2m^2 + (B/b)m^4.$$

So each triple (l,m,n), which solves (10.1), corresponds to a class in $\mathrm{im}(\delta)$ and vice versa. ■

It is easy to show, using the corollary above that the following result holds:

Corollary 10.4.4 For $b \mid B$, define the quadratic form

$$Q_b(r,s) = br^2 + Ars + (B/b)s^2,\ r,s \in \mathbb{Z}.$$

(a) Equation (10.1) has a non-zero solution if and only if

$$\begin{cases} n^2 = Q_b(r,s) \\ l^2 = r \\ m^2 = s \end{cases}$$

has a non-zero solution.

(b) The followings are equivalent:

(i) $g(x) = x^2 + Ax + B$ is positive definite, i.e. $Q_1(r,s)$ is positive definite.

(ii) $Q_b(r,s)$ is positive definite for all $b > 0$.

(c) When g is definite, Equation (10.1) has no non-zero solution for $b < 0$.

Example 10.4.4.1 Let $E : Y^2 = X(X^2-1)$ be the congruence number curve for $n = 1$. Here, $S = \emptyset$ and $\mathbb{Q}(S,2) = \{\pm 1\}$ (modulo squares). In this case, $\mathrm{im}(\delta) = \mathbb{Q}(S,2)$.
The other curve is $E' : Y^2 = X(X^2+4)$. Here, $S' = \{2\}$ and $\mathbb{Q}(S',2) = \{\pm 1, \pm 2\}$ (modulo squares). We must determine which $b = -1, \pm 2$ are in $\mathrm{im}(\delta')$. Since X^2+4 is positive definite (see Corollary 10.4.4), we only need to determine whether $b = 2 \in \mathrm{im}(\delta')$. To this end, we must solve the equation $n^2 = 2l^4 + 2m^4$. We see immediately that this has the solution $(1,1,2)$. So $\mathrm{im}(\delta') = \{(\mathbb{Q}^\times)^2, 2(\mathbb{Q}^\times)^2\}$.

Example 10.4.4.2 Let $E : Y^2 = X(X^2-25)$ be the congruence number curve for $n = 5$. Then, Lemma 10.3.2 gives $E' : Y^2 = X(X^2+100)$. For the curve E, $S = \{5\}$ and $\mathbb{Q}(S,2) = \{\pm 1, \pm 5\}$ (modulo squares). By definition $\delta(0,0) = -1$. So, we only need to consider $b = \pm 5$. In fact, one of them suffices! For $b = -5$, we get the equation

$$n^2 = -5l^4 + 5m^4,$$

which has the solution $(1,1,0)$. So $\mathrm{im}(\delta) = \mathbb{Q}(S,2)$.
For the curve is E', $S' = \{2,5\}$ and $\mathbb{Q}(S',2) = \{\pm 1, \pm 2, \pm 5, \pm 10\}$ (modulo squares). Since $\delta'(0,0) = 1$ and X^2+100 is definite, we only need to consider $b = 2, 5$ which lead to

(i) $n^2 = 2l^4 + 50m^4$;

(ii) $n^2 = 5l^4 + 20m^4$.

We see that (i) is impossible modulo 5, while (ii) has the solution $(1,1,5)$. So $\mathrm{im}(\delta') = \{1,5\}$.

We can now prove the main theorem of this section.

Theorem 10.4.5 — Weak Mordell-Weil Theorem. Let E be an elliptic curve over $\mathbb{Q}$ as in $(*)$. Then, $E(\mathbb{Q})/2E(\mathbb{Q})$ is **finite**.

Proof. By Proposition 10.3.5 and the remark we made right after it, we have two injections

$$\delta : E(\mathbb{Q})/\psi(E'(\mathbb{Q})) \hookrightarrow \mathbb{Q}(S,2) \text{ and } \delta' : E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \hookrightarrow \mathbb{Q}(S',2)$$

whose images are finite by Proposition 10.4.2. By applying Lemma 10.3.6 with $A = E(\mathbb{Q})$ and $B = E'(\mathbb{Q})$, we see that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. ■

R In fact, Lemma 10.3.6 implies that

$$\#E(\mathbb{Q})/2E(\mathbb{Q}) \leq \#\mathrm{im}(\delta) \cdot \#\mathrm{im}(\delta').$$

Furthermore, we know that

$$\#\left(\frac{\ker(\psi)}{\ker(\psi) \cap \mathrm{im}(\phi)}\right) = \begin{cases} 1 & \text{if } B' \text{ is a square,} \\ 2 & \text{otherwise.} \end{cases}$$

Hence, by part (b) of the remark after Lemma 10.3.6, we have

$$\#E(\mathbb{Q})/2E(\mathbb{Q}) = \begin{cases} \#\mathrm{im}(\delta) \cdot \#\mathrm{im}(\delta') & \text{if } B' \text{ is a square,} \\ \dfrac{\#\mathrm{im}(\delta) \cdot \#\mathrm{im}(\delta')}{2} & \text{otherwise.} \end{cases}$$

Example 10.4.5.1 (a) In Example 10.4.4.1, $B' = 4$ is a square, so

$$\#E(\mathbb{Q})/2E(\mathbb{Q}) = \#\mathrm{im}(\delta)\cdot\#\mathrm{im}(\delta') = 2\cdot 2 = 4.$$

This means that all cosets in $E(\mathbb{Q})/2E(\mathbb{Q})$ are accounted for by the 2-torsion points

$$E(\mathbb{Q})[2] = \{0,(0,0),(\pm 1,0)\}.$$

In the next section, we will use this to show that $E(\mathbb{Q}) = E(\mathbb{Q})[2]$, i.e. the only $\mathbb{Q}$-rational points on E are the 2-torsion points. This will mean that $n = 1$ is **not** a congruence number.

(b) In Example 10.4.4.2, $B' = 100$ is a square, so

$$\#E(\mathbb{Q})/2E(\mathbb{Q}) = \#\mathrm{im}(\delta)\cdot\#\mathrm{im}(\delta') = 4\cdot 2 = 8.$$

In this case, a coset in $E(\mathbb{Q})/2E(\mathbb{Q})$ comes either from the point $P = (-4,6)$, or from the 2-torsion subgroup

$$E(\mathbb{Q})[2] = \{0,(0,0),(\pm 5,0)\}.$$

We will later see that $E(\mathbb{Q})$ has rank 1, i.e. $Q \in E(\mathbb{Q})$ if and only if

$$Q = nP + P_0,$$

with $n \in \mathbb{Z}$ and $P_0 \in E(\mathbb{Q})[2]$.

The weak Mordell-Weil Theorem hold for elliptic curves over $\mathbb{Q}$ with no restriction on the 2-torsion: in order to prove this statement in general we can first extend the base field in order to have $E[2]\cap E(\mathbb{Q}) \neq \{0\}$, and then proceed as before. In this way, using some theorems of algebraic number theory and Galois cohomology, it is possible to prove the general statement: clearly, this is out of the purposes of this course.

10.5 The Mordell-Weil Theorem

Theorem 10.5.1 — Mordell-Weil Theorem. Let E be an elliptic curve defined over $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ is finitely generated, i.e.

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

where $r \geq 0$ is the **rank** of $E(\mathbb{Q})$, and T is finite. This means that there exist $r \geq 0$ points $P_1,\dots,P_r \in E(\mathbb{Q})$ such that every point $P \in E(\mathbb{Q})$ can be uniquely expressed as

$$P = P_0 + n_1P_1 + \cdots n_rP_r, \text{ with } n_i \in \mathbb{Z},\ P_0 \in T = E(\mathbb{Q})_{\mathrm{tors}}.$$

Proof. By the weak Mordell-Weil Theorem (which we proved when $E[2]\cap E(\mathbb{Q}) \neq \{0\}$) we know that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. Let $R_1,R_2,\dots,R_n$ represent the cosets of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$. Set

$$c = \max\{\hat{h}(R_1),\dots,\hat{h}(R_n)\} > 0.$$

Let $Q_1,Q_2,\dots,Q_m$ $(m \geq n)$ be all the points $Q \in E(\mathbb{Q})$ such that $\hat{h}(Q) \leq c$ (use (3) of Theorem 10.2.5). Let A be the subgroup of $E(\mathbb{Q})$ generated by $Q_1,Q_2,\dots,Q_m$. We will show that $A = E(\mathbb{Q})$.

Suppose that $A \subsetneq E(\mathbb{Q})$. Then, there exists $P \in E(\mathbb{Q})\setminus A$. Of all such points, pick one for which $\hat{h}(P)$ is minimal. Then, there exists R_i such that $P - R_i \in 2E(\mathbb{Q})$. So $P - R_i = 2P_1$ for some

$P_1 \in E(\mathbb{Q})$. Write $R = R_i$, then $P - R = 2P_1$. Now

$$\begin{aligned} 4\hat{h}(P_1) = \hat{h}(2P_1) = \hat{h}(P-R) &= 2\hat{h}(P) + 2\hat{h}(R) - \hat{h}(P+R) \leq 2\hat{h}(P) + 2\hat{h}(R) \\ &\leq 2\hat{h}(P) + 2c < 2\hat{h}(P) + 2\hat{h}(P) = 4\hat{h}(P). \end{aligned}$$

So $\hat{h}(P_1) < \hat{h}(P)$. By minimality of $\hat{h}(P)$ we must have $P_1 \in A$. This implies that $P = R + 2P_1 \in A$ since both $R, P_1 \in A$, which is a contradiction. Hence $A = E(\mathbb{Q})$, so $E(\mathbb{Q})$ is finitely generated. ■

Example 10.5.1.1 Let E be defined by $Y^2 = X^3 - X$. In Example 10.4.5.1 (a), we saw that $\#E(\mathbb{Q})/2E(\mathbb{Q}) = 4$. By the Lutz-Nagell Theorem,

$$E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q})[2] = \{0, (0,0), (\pm 1, 0)\}.$$

By the Mordell-Weil Theorem, we can write

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}^r \times (\mathbb{Z}/2\mathbb{Z})^2.$$

Since the double of a point of infinite order is a point of infinite order, and the double of torsion point is a torsion point, we see that as a subgroup of $\mathbb{Z}^r \times (\mathbb{Z}/2\mathbb{Z})^2$

$$2E(\mathbb{Q}) \cong (2\mathbb{Z})^r \times 2E(\mathbb{Q})_{\text{tors}} = (2\mathbb{Z})^r \times \{0\}.$$

(We only have 2-torsion points.) Therefore, we have

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{Z}/2\mathbb{Z})^2 = (\mathbb{Z}/2\mathbb{Z})^2.$$

Thus, the rank of the curve E is $r = 0$, and

$$E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

Example 10.5.1.2 In Example 10.4.5.1 (b), for the curve $E : Y^2 = X^3 - 25X$, we saw that $\#E(\mathbb{Q})/2E(\mathbb{Q}) = 8$. We also saw that the cosets are given by $P = (-4, 6)$ and the 2-torsion points. Again, by the Lutz-Nagell Theorem,

$$E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q})[2] = \{0, (0,0), (\pm 5, 0)\}.$$

By the Mordell-Weil Theorem, we can write

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}^r \times (\mathbb{Z}/2\mathbb{Z})^2.$$

Therefore, we have

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{Z}/2\mathbb{Z})^2 = (\mathbb{Z}/2\mathbb{Z})^3.$$

Thus, the rank of the curve E is $r = 1$, and we have

$$E(\mathbb{Q}) \cong \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2.$$

Example 10.5.1.3 Consider the curve $E : Y^2 = X(X^2 - X + 4)$. Then, we have $S = \{2\}$ and $\mathbb{Q}(S,2) = \{\pm 1, \pm 2\}$ (modulo squares). Since $X^2 - X + 4$ is definite and $\delta(0,0) = 1$, we only need to consider $b = 2$ in order to find $\mathrm{im}(\delta)$. This gives the equation

$$2l^4 - m^2l^2 + 2m^4 = n^2.$$

This is the same as

$$2(l^2 + m^2)^2 - 5m^2l^2 = n^2,$$

which is impossible modulo 5. So, we have $\mathrm{im}(\delta) = \{1\}$.
The other curve to be considered is $E' : Y^2 = X(X^2 + 2X - 15)$. Here $S' = \{3,5\}$ and $\mathbb{Q}(S',2) = \{\pm 1, \pm 3, \pm 5, \pm 15\}$ (modulo squares). Since, $\delta'(0,0) = -15$, we only need to consider $b = -1$ and only one of $b = \pm 3$ or ± 5 to find $\mathrm{im}(\delta')$. For $b = -1$, we find the equation

$$-l^4 + 2m^2l^2 + 15m^4 = n^2.$$

This is the same as

$$-(l^2 - m^2)^2 + 16m^4 = n^2,$$

which has the solution $(1,1,4)$ corresponding to the point $(-1,4)$ on E'. For $b = 3$, we get the equation

$$3l^4 + 2m^2l^2 - 5m^4 = n^2,$$

which has the solution $(1,1,0)$ corresponding to $(3,0)$ on E'. Hence, we have $\mathrm{im}(\delta') = \mathbb{Q}(S',2)$. Since $B' = -15$ is a non-square, the Weak Mordell-Weil Theorem (and Remark 9.16) imply that $\#E(\mathbb{Q})/2E(\mathbb{Q}) = 8/2 = 4$. By the Lutz-Nagell Theorem, $E(\mathbb{Q})_{\mathrm{tors}} = \{0, (0,0)\}$. So, the Mordell-Weil Theorem (Theorem 10.5.1) implies that

$$E(\mathbb{Q})/2E(\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^{r+1} = (\mathbb{Z}/2\mathbb{Z})^2.$$

Hence, the curve E has rank $r = 1$. In fact, $E(\mathbb{Q}) = \langle (1,2) \rangle \times \langle (0,0) \rangle$.

Elliptic Curve Cryptography
Cryptography
Diffie-Hellman
ElGamal Cryptosystem
Elliptic Curve Discrete Logarithm Problem

Schoof's algorithm

11. Applications II

11.1 Elliptic Curve Cryptography

The idea to use elliptic curves in cryptography was independently proposed by Neil Koblitz and Victor Miller in the mid 1980s. Before describing two of the most known cryptosystem which use elliptic curves, let us recall some of the basic concepts and definitions in cryptography.

11.1.1 Cryptography

Cryptography is the process of writing using various methods, ciphers, to keep messages secret. Cryptography is used to hide information. It is not only use by spies but for phone, fax and e-mail communication, bank transactions, bank account security, PINs, passwords and credit card transactions on the web. It is also used for a variety of other information security issues including electronic signatures, which are used to prove who sent a message.
Cryptanalysis is the science of attacking ciphers, finding weaknesses, or even proving that a cipher is secure. **Cryptology** covers both; it's the complete science of secure communication.

A **plaintext message**, or simply a plaintext, P, is a message to be communicated. This is the original readable message (written in some standard language, like English, French, Cantonese, Italian, Spanish, Icelandic,...). A disguised version of a plaintext message is a **ciphertext message** or simply a ciphertext, C. This is the output of some **encryption scheme**: let E be the encryption function. We write, for example, $E(P) = C$ to mean that applying the encryption process E to the plaintext P produces the ciphertext C. The process of turning a ciphertext back into a plaintext is called **decryption**: the decryption function D is the function such that $D(C) = P$. Note $D(E(P)) = P$ and $E(D(C)) = C$. The **encryption key** is piece of data that allows the computation of E. Similarly we have the **decryption key**. These may or may not be the same. They also may not be secret.

A **cryptosystem** consists of an enciphering algorithm and a deciphering algorithm. A **symmetric key cryptosystem** requires a secret shared key. Two users must agree on a key ahead of time. In a **public key cryptosystem**, each user has an encrypting key which is published and a decrypting key which is not.

Today we use cryptography for a lot more than just sending secret messages:

- **Authentication**. Alice receives a ciphertext from Bob. How can she be sure that the message originated from Bob? How can she be sure that the message wasn't corrupted? How can Bob be sure Alice received it? How can Alice make sure that Bob can't deny having sent it?
- **Key exchange**. Over an insecure channel, Alice and Bob exchange two pieces of data that allow them to compute a common encryption/decryption key. But any attacker who intercepts the transmissions can't recover the key.
- **Zero-knowledge proofs**. Alice can unequivocally convince Bob that she has a certain piece of information, without revealing the exact piece of information to Bob.
- **Secret sharing**. Alice, Bob, Carol, ... each have a piece of information that is part of a commonly held secret S. If N or more of them meet and combine their knowledge, then S can be reconstructed. But if less than N get together, S cannot be reconstructed.

All of these protocols are in common usage in computer networks. They are also crucial in sensitive communication.

The fundamental ideas in cryptography are:

- Encryption and decryption should be easy for the proper users, Alice and Bob. Decryption should be hard for any eavesdropper, Eve.
- Must assume that the enemy will find out about the nature of a cryptosystem and will only be missing a key.

Example 11.1.0.4 (a) **Caesar cipher.** Encode letters by numbers:

$$A \to 0,\ B \to 1,\ C \to 2,\ \ldots, Z \to 25.$$

Choose a key t, which is a number between 0 and 25 (for Caesar t was always 3). For each letter P, E is defined by

$$E(P) = P + t,$$

that is, add t to the code for each letter to get a new letter code. Of course, you are counting modulo 25. For example, if we take $t = 17$, then encrypting the plaintext

ALLOFGAULISDIVIDEDINTOTHREEPARTS

yields the ciphertext

RCCFWXRLCZJUZMZUVUZEKFKYIVVGRIJK

Decryption is done by $D(C) = C - t$. This cryptosystem is horrendously insecure.

(b) **Affine cipher.** Choose a number a and define $E(P) = aP + t$.

(c) **Digraph affine cipher.** Choose numbers $a_1, a_2, b_1, b_2, t_1, t_2$, and then encrypt by transforming pairs of letters:

$$E(P_1, P_2) = (a_1P_1 + b_1P_2 + t_1, a_2P_1 + b_2P_2 + t_2).$$

These schemes are insecure, since natural languages have statistical biases (the "Wheel of Fortune phenomenon").

11.1.2 Diffie-Hellman

Suppose two communication parties, Alice and Bob, want to agree upon a key which will be later used for encrypted communication in conjunction with a private key cryptosystem. The Diffie-Hellman key exchange is a public key cryptosystem which provides them a way of doing this without revealing personal encryption keys.

Algorithm 11.1 — Diffie-Hellman key exchange.

Step 1: Bob and Alice choose a 200-digit integer p that is likely to be prime, and choose a number g with $1 < g < p$.

Step 2: Alice secretly chooses an integer n, computes $g^n \pmod{p}$ and tells Bob the result.

Step 3: Bob secretly chooses an integer m and tells Alice $g^m \pmod{p}$

Step 4: The shared secret key is then $s \equiv (g^n)^m \equiv (g^m)^n \equiv g^{nm} \pmod{p}$, which both Alice and Bob can compute.

Alice communicates with Bob by encrypting everything using their agreed upon secret key. In order to understand the conversation, the eavesdropper needs s, but it takes a long time to compute s given only p, g, g^n, and g^m. One way would be to compute n from knowledge of g and g^n; this is possible, but appears to be "computationally infeasible," in the sense that it would take too long to be practical.
Let a, b, and n be real numbers with $a, b > 0$ and $n \geq 0$. Recall that the "log to the base b" function is characterized by

$$\log_b(a) = n \qquad \text{if and only if} \qquad a = b^n.$$

Hence, the problem becomes: given a base b and a power a of b, find an exponent n such that $a = b^n$. That is, given $a = b^n$ and b, find n.
The discrete log problem is the analog of computing $\log_b(a)$ but where both b and a are elements of a finite group.

Discrete Log Problem: Let G be a finite group, for example, $G = \mathbb{F}_p^*$. Given $b \in G$ and a power a of b, find a positive integer n such that $b^n = a$.

As far as we know, finding discrete logarithms in $\mathbb{F}_p^*$ when p is large is "very difficult" in practice. Unfortunately, we have no formal proof that computing discrete logarithms on a classical computer is difficult. Also, Peter Shor showed that if one could build a sufficiently complicated quantum computer, it could solve the discrete logarithm problem in time bounded by a polynomial function of the number of digits of $\#G$. It is easy to give an inefficient algorithm that solves the discrete log problem. Simply try b^1, b^2, b^3, etc., until we find an exponent n such that $b^n = a$. When p is large, computing the discrete log this way soon becomes impractical, because increasing the number of digits of the modulus makes the computation take vastly longer.

The Diffie-Hellman key exchange works well on an elliptic curve with no serious modification. Alice and Bob agree on a secret key as follows:

Algorithm 11.2 — Diffie-Hellman key exchange with elliptic curves.

Step 1: Alice and Bob agree on a prime p, an elliptic curve E over $\mathbb{F}_p$, and a point $P \in E(\mathbb{F}_p)$.

Step 2: Alice secretly chooses a random m and sends mP.

Step 3: Bob secretly chooses a random n and sends nP.

Step 4: The secret key is nmP, which both Alice and Bob can compute.

Presumably, an adversary can not compute nmP without solving the discrete logarithm problem on elliptic curve, that we will describe later. For well-chosen E, P, and p, experience suggests that the discrete logarithm problem in $E(\mathbb{F}_p)$ is much more difficult than the discrete logarithm problem in $\mathbb{F}_p^*$.

11.1.3 ElGamal Cryptosystem

The ElGamal Cryptosystem allows one user to give a public key to use for encryption and still maintain a private encryption key. It is a public key cryptosystem.
The ElGamal cryptosystem produces a signature scheme: suppose Alice wants to send a signed message to Bob (here the message is not necessarily secret). What is important is for Bob to verify that it is signed by Alice.
To illustrate the ElGamal cryptosystem, we describe how Bob would set up an ElGamal cryptosystem that anyone could use to encrypt messages for him. Bob chooses a prime p, an elliptic curve E over $\mathbb{F}_p$, and a point $B \in E(\mathbb{F}_p)$, and publishes p, E, and B. He also chooses a random integer n, which he keeps secret, and publishes nB. His public key is the four-tuple

$$(p, E, B, nB).$$

Suppose Alice wishes to encrypt a message for Bob. If the message is encoded as an element $P \in E(\mathbb{F}_p)$, Alice computes a random integer r and the points rB and $P + r(nB)$ on $E(\mathbb{F}_p)$. The signature of Alice is rB. Then P is encrypted as the pair $(rB, P + r(nB))$. To decrypt the encrypted message, Bob multiplies rB by his secret key n to find $n(rB) = r(nB)$, then subtracts this from $P + r(nB)$ to obtain

$$P = P + r(nB) - r(nB).$$

Any other new message sent by Alice will be encrypted using rB: this will be Alice's signature and Alice in any further communication will encrypt any message P' as $P' + r(nB)$. If the decryption fails, Bob will not recognize the signature of Alice.
We do the above examples using the open-source mathematics software system Sage:

```
sage: p = 78596310237942882237669478944689739620749856895 1
sage: E = EllipticCurve(GF(p), \
... [31768908125132550347631747641382769327274695592 7,
... 79052896607878758718120572025718535432100651934])
sage: E.cardinality()
78596310237942882237669302488171495761268615742 9
sage: E.cardinality().is_prime()
True
sage: B = E([
... 77150721626264982617064826856557988990776925417 6,
```

```
... 39015751024655662852527945926651499556253319665 5])
sage: n=67080503113991051351752720769306045630021705 4473
sage: r=70674630913457179596452846564371866229568459543
sage: P = E([14489646124220757767,
... 66933778037328409627489513661819460446969683007 4])
sage: encrypt = (r*B, P + r*(n*B))
sage: encrypt[1] - n*encrypt[0] == P # decrypting works
True
```

11.1.4 Elliptic Curve Discrete Logarithm Problem

The two cryptosystems described depends on the difficulty to solve the following problem:

Elliptic Curve Discrete Log Problem: suppose E is an elliptic curve over $\mathbb{F}_p$ and $P \in E(\mathbb{F}_p)$. Given a multiple Q of P, the **elliptic curve discrete log problem** is to find $n \in \mathbb{Z}$ such that $nP = Q$.

For example, let E be the elliptic curve given by $y^2 = x^3 + x + 1$ over the field $\mathbb{F}_7$. We have

$$E(\mathbb{F}_7) = \{0, (2,2), (0,1), (0,6), (2,5)\}.$$

If $P = (2,2)$ and $Q = (0,6)$, then $3P = Q$, so $n = 3$ is a solution to the discrete logarithm problem.

If $E(\mathbb{F}_p)$ has order p or $p \pm 1$, or is a product of reasonably small primes, then there are some methods for attacking the discrete log problem on E, which are beyond the scope of this course. It is therefore important to be able to compute $\#E(\mathbb{F}_p)$ efficiently, in order to verify that the elliptic curve one wishes to use for a cryptosystem doesn't have any obvious vulnerabilities. The naive algorithm to compute $\#E(\mathbb{F}_p)$ is to try each value of $x \in \mathbb{F}_p$ and count how often $x^3 + ax + b$ is a perfect square mod p, but this is of no use when p is large enough to be useful for cryptography. Fortunately, there is an algorithm due to Schoof, Elkies, and Atkin for computing $\#E(\mathbb{F}_p)$ efficiently (polynomial time in the number of digits of p), but this algorithm is beyond the scope of this course: we will only present a basic version of the original algorithm by Schoof.

At present, it appears that given p, the discrete log problem in $E(\mathbb{F}_p)$ is much harder than the discrete log problem in the multiplicative group $\mathbb{F}_p^*$. This suggests that by using an elliptic curve-based cryptosystem instead of one based on $\mathbb{F}_p^*$, one gets equivalent security with much smaller numbers, which is one reason why building cryptosystems using elliptic curves is attractive to some cryptographers. For example, Certicom, a company that strongly supports elliptic curve cryptography, claims:

> "[Elliptic curve cryptography] devices require less storage, less power, less memory, and less bandwidth than other systems. This allows you to implement cryptography in platforms that are constrained, such as wireless devices, hand-held computers, smart cards, and thin-clients. It also provides a big win in situations where efficiency is important."

In April 2004, a specific cryptosystem based on an elliptic curve over $\mathbb{F}_p$, where p was chosen with 109 bits, was cracked. The first unsolved challenge problem involves an elliptic curve over $\mathbb{F}_p$, where p has 131 bits, and the next challenge after that is one in which p has 163 bits. Certicom claims that the 163-bit challenge problem is computationally infeasible.

11.2 Schoof's algorithm

When generating curves for elliptic curve cipher systems, the order of the group of points is important. The main method for generating these curves depends on the point counting problem. Usually, it is required, at least, for the group to be divisible by a large prime factor. By large we mean at least 160 bits in length.

Let E be an elliptic curve of the form $y^2 = x^3 + Ax + B$ over the finite field $\mathbb{F}_q$ where $q = p^n$ and $p \geq 3$ is an odd prime (there is a similar algorithm in characteristic 2 and 3, but for simplicity we are not going to discuss it here). By Hasse's Theorem, recall $\#E(\mathbb{F}_q) = q + 1 - a_q$ where $|a_q| \leq 2\sqrt{q}$. Let S be the set of primes,

$$S = \{2, 3, \ldots, L\}$$

such that the product of all its elements is larger than $4\sqrt{q}$, the length of the interval over which a lies in. We will also assume that the characteristic p of $\mathbb{F}_q$ is not an element in S.

The idea behind Schoof's algorithm is to find $a_q \bmod \ell$ for all $\ell \in S$, then use the Chinese Remainder Theorem to determine a_q.

For every $\ell \in S$ we do the following.

Step 1. Suppose $\ell = 2$. If $x^3 + Ax + B$ has a root $\alpha \in \mathbb{F}_q$, then $(\alpha, 0)$ is a point of order two. By Lagrange's Theorem, $E(\mathbb{F}_q)$ has even order, so $q + 1 - a_q \equiv 0 \bmod 2$, so $a_q \equiv 0 \bmod 2$.
To determine whether $x^3 + Ax + B$ has a root in $\mathbb{F}_q$, consider the equation $x^q - x = 0$. Recall that the elements of $\mathbb{F}_q$ are the elements of $\overline{\mathbb{F}}_q$ which satisfy $x^q - x = 0$. Thus, $x^3 + Ax + B$ has a root in $\mathbb{F}_q$ if and only if it has a root in common with $x^q - x$, i.e. $\gcd(x^3 + Ax + B, x^q - x) \neq 1$.
If $\gcd(x^3 + Ax + B, x^q - x) = 1$, then there is no common root, so $a_q \equiv 1 \bmod 2$.

Step 2. Suppose $\ell \neq 2$. Recall that the division polynomial ψ_ℓ is a function through which we characterize the ℓ-torsion: $(x, y) \in E[\ell]$ if and only if $\psi_\ell(x) = 0$.

1. Let $P = (x, y) \in E[\ell] \setminus \{0\}$, and let $k \equiv q \bmod \ell$ such that $|k| \leq \ell/2$. Let ϕ_q be the Frobenius endomorphism. Then $\phi_q^2 - a_q \phi_q + q = 0$. In other words,

$$(x^{q^2}, y^{q^2}) + [k](x, y) = [a_q](x^q, y^q).$$

2. Assume $\phi_q^2 P \neq [k]P$ for every $P \in E[\ell] \setminus \{0\}$ and denote $(x_n, y_n) := [n](x, y)$. We want to determine whether a j exists such that

$$(x^{q^2}, y^{q^2}) + (x_k, y_k) = (x_j^q, y_j^q)$$

for some $j \in \{1, 2, \ldots, \ell - 1\}$. This procedure tests if $\pm j$ is our required a_q, since the x-coordinates are the same for either sign and the y coordinates may differ by a constant. Since we will only evaluate the x coordinates, we only need to consider $j \in \{1, 2, \ldots, (\ell - 1)/2\}$ and $(x^{q^2}, y^{q^2}) + (x_k, y_k) = \pm(x_j^q, y_j^q)$.

The addition of points is an endomorphism. So $(x^{q^2}, y^{q^2}) + (x_k, y_k) = (G_1(x), yH_1(x))$ for rational functions G_1 and H_1. We also have $(x_j^q, y_j^q) = (G_2(x), yH_2(x))$ since this is just the

multiplication by j map. According to the group law,

$$\begin{aligned} G_1(x) &= \left(\frac{y^{q^2}-y_k}{x^{q^2}-x_k}\right)^2 - x^{q^2} - x_k = \\ &= y^2\left(\frac{y^{q^2-1}-r_{y,k}(x)}{x^{q^2}-x_k}\right)^2 - x^{q^2} - x_k = \\ &= (x^3+Ax+B)\left(\frac{(x^3+Ax+B)^{\frac{q^2-1}{2}}-r_{y,k}(x)}{x^{q^2}-x_k}\right)^2 - x^{q^2} - x_k, \end{aligned}$$

where $y_k = y\, r_{y,k}(x)$ and $r_{y,k}(x)$ is a rational function.

Now, $(G_1(x), yH_1(x)) = \pm(G_2(x), yH_2(x))$ if and only if $G_1(x) = G_2(x)$ for $(x,y) \in E[\ell]$. Recall ψ_ℓ has degree $(\ell^2-1)/2$, since this is a minimal polynomial whose roots are all the x-coordinates of elements in $E[\ell]$. Thus, for $(x,y) \in E[\ell]$, $\psi_\ell \mid G_1 - G_2$ if and only if $G_1(x) = G_2(x)$.

Suppose we found j such that $(G_1(x), yH_1(x)) = (G_2(x), \pm yH_2(x))$, i.e. $a_q \equiv \pm j \bmod \ell$. To determine the sign, one can make some easy computations with H_1 and H_2 and obtain, in a similar way as before, that if $H_1 - H_2 \cong 0 \bmod \psi_\ell$, then $a_q \equiv j \bmod \ell$, otherwise, $a_q \equiv -j \bmod \ell$.

3. Now suppose no such j works. Then there must exist a $P \in E[\ell] \setminus \{0\}$ such that $\phi_q^2(P) = \pm[k]P$. Let $w^2 \equiv q \bmod \ell$. If w does not exist, then $a_q \equiv 0 \bmod \ell$. Otherwise, the three following possibilities can occur:

   - $\gcd(\text{numerator}(x^q - x_w), \psi_\ell) = 1$, then $a_q \equiv 0 \bmod \ell$.
   - $\gcd(\text{numerator}((y^q - y_w)/y), \psi_\ell) \neq 1$, then $a_q \equiv 2w \bmod \ell$.
   - otherwise, $a_q \equiv -2w \bmod \ell$.

Now use Chinese Remainder theorem to compute $a_q \bmod \prod \ell$ and since a_q satisfies the Hasse's bound, we can determine a_q and so $\#E(\mathbb{F}_q)$.

12. Advanced topics

12.1 The Birch and Swinnerton-Dyer Conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$. The Mordell-Weil Theorem asserts that $E(\mathbb{Q})$ is finitely generated. More precisely, we showed that

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r,$$

where r is the rank of E.

Question: Does this mean that in practice we can determined $E(\mathbb{Q})$? By "determine" we mean find the abstract group structure, i.e. find the structure of $E(\mathbb{Q})_{\text{tors}}$ and r.

The torsion subgroup can be easily computed thanks to the following result, combined with the Lutz-Nagell Theorem.

Theorem 12.1.1 — Mazur. Let E be an elliptic curve over $\mathbb{Q}$, then

$$E(\mathbb{Q})_{\text{tors}} \cong \begin{cases} C_n \ (n = 1, \dots, 10 \text{ or } n = 12) \\ C_2 \times C_{2n} \ (n = 1, 2, 3, 4). \end{cases}$$

The rank r, however, remains highly mysterious. For example, it is unclear whether given a positive integer r there exists a curve E such that $\text{rank}(E) = r$. Although it is commonly believed that the rank can be arbitrarily large, the highest rank known to date belongs to a curve discovered by Elkies in 2006:

$$y^2 + xy + y = x^3 - x^2 - a_4 x + a_6$$

with

$$a_4 = 20067762415575526585033208209338542750930230312178956502,$$

$$a_6 = 3448161179503055646703298569039072037485594435931918036126600829629193944873224342 9,$$

whose rank is at least 28. Since the mid 60s, much effort has gone into understanding ranks of elliptic curves, leading to one of the most influential conjectures in number theory, namely the Birch and Swinnerton-Dyer Conjecture.

Let $E/\mathbb{Q}$ be as above; let Δ be its discriminant and p a prime. In Chapter 8, we described the reduction $\overline{E}_p$ of E modulo p. If p is a prime of *good* reduction, $\overline{E}_p$ is an elliptic curve over $\mathbb{F}_p$. In that case, we defined the trace of Frobenius on $\overline{E}_p$ by

$$a_p(E) = p + 1 - \#\overline{E}_p(\mathbb{F}_p).$$

We can extend the definition of a_p to the primes of *bad* reduction as follows: $\overline{E}_p$ is a singular curve, and we studied singular cubics in Chapter 2, so

$$a_p(E) := \begin{cases} 0 & \text{if } E \text{ has additive reduction at } p, \text{ i.e. } \overline{E}_p \text{ has a cusp,} \\ 1 & \text{if } E \text{ has split multiplicative reduction at } p, \text{ i.e. } \overline{E}_p \text{ has a node,} \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p, \text{ i.e. } \overline{E}_p \text{ has a node.} \end{cases}$$

Definition 12.1 Let E be an elliptic curve defined over $\mathbb{Q}$. The **L-series** attached to E is defined by

$$L(E,s) := \prod_{p|\Delta} \left(1 - a_p(E)p^{-s}\right)^{-1} \prod_{p\nmid\Delta} \left(1 - a_p(E)p^{-s} + p^{1-2s}\right)^{-1}. \tag{12.1}$$

One can show that the product (12.1) converges for $\Re(s) \geq 3/2$, and has a meromorphic continuation to the whole complex plane. (This product is called an *Euler product*.) Furthermore, one can show that

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s}.$$

The following is the weak version of the Birch and Swinnerton-Dyer Conjecture, which was formulated in the mid 60s based on numerical evidence gathered using EDSAC, one of the early computers available at Cambridge University.

Conjecture 12.1.2 — Birch-Swinnerton-Dyer. Let E be an elliptic curve defined over $\mathbb{Q}$, and let $r = \text{rank}(E)$. Then,

(i) $L(E,1) = 0$ if and only if $r > 0$.

(ii) If $L(E,1) = 0$, then $r = \text{ord}_{s=1}L(E,s)$, the order of vanishing of $L(E,s)$ at $s = 1$.

The central role played by this conjecture in the arithmetic theory of elliptic curve is highlighted by the fact that it is one of the Millennium Prize Problems of the Clay Mathematical Institute. Any proof of the (strong version of the) BSD Conjecture will lead to effective algorithms for computing ranks of elliptic curves.

Example 12.1.2.1 (a) We already saw that the congruence number curve $E : Y^2 = X^3 - X$ has rank $r = 0$. By evaluating the L-series of this curve to several digit precision using `Sage` or `Magma`, we see that

$$L(E,1) = 0.655514388573...,$$

which is consistent with the BSD Conjecture.
(b) Similarly, we saw that the rank of the curve $E : Y^2 = X^3 - 25X$ is 1. The L-series of this curve computed to several digit precision is

$$L(E,1) = 0.00000000000....$$

Example 12.1.2.2 (a) The discriminant of the curve $E : y^2 + y = x^3 - x^2 - 10x - 20$ is $\Delta = -11^5$. The evaluation of its L-series to several digit precision gives

$$L(E,1) = 0.25384186....$$

This curve has rank $r = 0$, which is consistent with BSD.

(b) The curve $E : y^2 + y = x^3 - x$ has discriminant $\Delta = 37$. One verifies that

$$L(E,1) = 0.000000000...,$$

and that $\text{rank}(E) = 1$. In fact the point $P = (0,0)$ generates $E(\mathbb{Q})$.

12.2 Modularity

Elliptic curves (over the rationals) are intrinsically related to modular forms; these are analytic objects, which have been studied since the 19th century. In the last two decades, some of the most spectacular results in number theory have come through this connection. The key insight that such a link exists is due mainly to Eicher, Shimura, Taniyama and Weil.
Let $\mathfrak{H}$ denote the Poincaré upper halfplane, i.e.

$$\mathfrak{H} := \{\tau \in \mathbb{C} : \text{Im}(\tau) > 0\}.$$

Definition 12.2 A **modular cusp form** of weight 2 and level N is an analytic function $f : \mathfrak{H} \to \mathbb{C}$ such that

(a) f is given by a power series

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, \text{ with } q = e^{2\pi i \tau}, \ \tau \in \mathfrak{H}.$$

(b) $f\left(\dfrac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 f(\tau)$, for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ with $N \mid c$.

(c) $f(z)$ tends rapidly to 0 as $z \to \alpha$ for all $\alpha \in \mathbb{Q}$ (vanishing at cusps).

The space of cusp forms of weight 2 and level N, which we denote by $S_2(N)$, is a *finite* dimensional complex vector space. It comes equipped with the action of a family of linear operators called *Hecke operators*, which are defined as follows. First, for each prime $p \nmid N$, one defines the Hecke operator T_p by

$$(T_p f)(\tau) := f(p\tau) + \sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right).$$

Analogously, one defines T_p for $p \mid N$. Finally, one extends the definition to all $n \in \mathbb{Z}_{\geq 1}$ by

$$\begin{array}{lcll} T_{p^r} & = & T_{p^{r-1}} T_p - p T_{p^{r-2}} & \text{if } r \geq 2 \text{ and } p \text{ is a prime not dividing } N; \\ T_{p^r} & = & T_p^r & \text{if } p \text{ is a prime dividing } N; \\ T_{mn} & = & T_m T_n & \text{if } (m,n) = 1. \end{array}$$

The T_n ($n \geq 1$) are *normal* operators which *commute*. So not only are they diagonalisable, but also they admit a common basis of eigenvectors.

Definition 12.3 Let $f(\tau) = \sum_{n=1}^{\infty} a_n q^n \in S_2(N)$. We say that f is a **normalised eigenform** if it is a common eigenvector for the Hecke operators and $a_1 = 1$.

Let f be a normalised eigenform. Shimura proved that each a_n is an algebraic number, and that

$$T_n f = a_n f, \text{ for all } n \geq 1.$$

We can define an equivalence relation on the set of normalised eigenforms as follows. Let

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n \text{ and } g(\tau) = \sum_{n=1}^{\infty} b_n q^n$$

be normalised eigenforms of level N and N' respectively. We say that f and g are equivalent, and write $f \sim g$, if $a_n = b_n$ for almost all n. It is not hard to see that this is indeed an equivalence relation. It can be shown that if $f \sim g$, then there exists a normalised eigenform $h \in S_2(M)$, where $M = \gcd(N, N')$, such that $f \sim g \sim h$.

Definition 12.4 Let f be a normalised eigenform of level N. We say that f is a **newform**, if f has the smallest level in its equivalence class.

It can be shown that every equivalence class under $\sim$ contains a *unique* newform. (This result is known as the *Multiplicity One Theorem*.) The *L-series attached to a newform* f is defined by

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

It can be shown that $L(f,s)$ is analytic, i.e. holomorphic on the whole complex plane, and admits an Euler product as in (12.1).
The first connection between elliptic curves and modular forms was observed by Eichler and Shimura. In the mid 60s, they proved the following result.

Theorem 12.2.1 — Eichler-Shimura. Let $f(\tau) = \sum_{n=1}^{\infty} a_n q^n \in S_2(N)$ be a newform such that all the coefficients a_n are **rational integers**. Then, there exists an elliptic curve E_f defined over $\mathbb{Q}$ such that

$$L(E_f, s) = L(f, s).$$

One of the most striking facts about the arithmetic theory of elliptic curves is that the converse to Theorem 12.2.1 is true.

Theorem 12.2.2 — Wiles, Breuil, Conrad, Diamond, Taylor. Let $E/\mathbb{Q}$ be an elliptic curve, and define $f_E : \mathfrak{H} \to \mathbb{C}$ by

$$f_E(\tau) := \sum_{n=1}^{\infty} a_n(E) q^n.$$

Then, f_E is a newform of weight 2. The level N of f_E is called the **conductor** of E.

Until the mid 90s, Theorem 12.2.2 was known as the Shimura-Tanyiama-Weil Conjecture. It proof uses some of the most sophisticated tools in modern mathematics: automorphic forms and representations; Galois representations; and arithmetic geometry, etc. The first major breakthrough came in 95, when Wiles proved Theorem 12.2.2 when the conductor of E is squarefree. His result was completed in 2001 by Breuil, Conrad, Diamond and Taylor.

Example 12.2.2.1 The newform attached to the curve $E : Y^2 = X^3 - X$ is

$$f_E = q - 2q^5 - 3q^9 + 6q^{13} + 2q^{17} - q^{25} - 10q^{29} - 2q^{37} + \cdots .$$

Its level is the integer $N = 32$.
The conductor of the curve $E : Y^2 = X^3 - 25X$ is $N = 800$, and the attached newform is

$$f_E = q - 3q^9 - 6q^{13} - 2q^{17} - 10q^{29} + 2q^{37} + 10q^{41} - 7q^{49} + \cdots .$$

Example 12.2.2.2 The curves in Example 12.1.2.2 have conductor 11 and 37 respectively, and the attached newforms are

$$f_{11} = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} + \cdots ,$$

$$f_{37} = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} - 5q^{11} + \cdots .$$

An immediate consequence of Theorem 12.2.2 is that $L(E,s) = L(f_E,s)$. This means that the L-series of an elliptic curve $E/\mathbb{Q}$ is an entire function.
Theorem 12.2.2 led to the resolution of a wide range of Diophantine equations, including Fermat's Last Theorem which was Wiles' initial motivation. It also enabled substantial progress towards the BSD Conjecture.

Theorem 12.2.3 — Kolyvagin. The BSD Conjecture is true for all elliptic curves $E/\mathbb{Q}$ such that $\mathrm{ord}_{s=1} L(E,s) \leq 1$.

Example 12.2.3.1 The BSD Conjecture is true for the curves in Examples 12.1.2.1 and 12.1.2.2.

Bibliography

[1] J. W. S Cassels. *Lectures on elliptic curves*. London Mathematical Society Student Texts, 24. Cambridge University Press, Cambridge, 1991.

[2] Dale Husemöller, *Elliptic curves*, Graduate Texts in Mathematics, 111, Springer-Verlag, New York, 2004.

[3] Anthony W. Knapp, *Elliptic curves*. Mathematical Notes, 40. Princeton University Press, Princeton, NJ, 1992.

[4] Joseph H. Silverman, *The arithmetic of elliptic curves*. Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.

[5] Notes from Peter Stevenhagen, Universiteit Leiden, avaliable at: `http://pub.math.leidenuniv.nl/~luijkrmvan/elliptic/2011/ec.pdf`

[6] Lawrence C. Washington, *Elliptic curves. Number theory and cryptography.* Second edition. Discrete Mathematics and its Applications. Chapman & Hall(2008).

Index

B-power smooth, 33
L-series, 118
mod *p* Galois representation, 78
j-invariant, 38
n-torsion subgroup, 73
p-adic filtration, 83
p-adic valuation, 80

algebraic closure of a field, 15
algebraic extension, 14
algebraic number, 14
algebraically closed field, 15

Bachet-Mordell equation, 12

canonical height, 97
congruent number, 13
congruent number curve, 13
cryptography, 109
cusp, 30

degree, 53
discriminant of a polynomial, 20
discriminant of an elliptic curve, 21
division polynomial, 76

Eisenstein series, 46
elliptic curve, 17
elliptic function, 43
endomorphism, 52
endomorphism ring, 53

Frobenius map, 70
fundamental parallelogram, 42

group law on an elliptic curve, 24

height in $\mathbf{P}^n(\mathbb{Q})$, 92
homogenisation, 9

inseparable, 54
inseparable degree, 55
integral model, 81
invariant differential form, 58
isogeny, 98

lattice, 41
Lenstra ECM, 35
logarithmic height, 95
long Weierstrass equation, 17

medium Weierstrass equation, 18
minimal model, 81
multiplicity of a point, 22

naive height, 95
node, 30
non-split node, 32

plane curve, 7
point at infinity, 17
point of finite order, 73
prime of bad reduction, 81
prime of good reduction, 81
projective space, 8

rational function, 51
rational point, 10
resultant, 18

separable, 54
separable degree, 55
short Weierstrass equation, 18
singular curve, 9
smooth curve, 9
split node, 32

torsion subgroup, 75
twist, 40

Weierstrass $\wp$-function, 43