1 Appendix on Elliptic curves

1.1 Rational elliptic curves

Consider the plane curves of equations

$$E_1\colon y^2 = x^3 + 17 \qquad E_2\colon y^2 = x^3 - x \qquad E_3\colon y^2 = x^3 - x + 1$$

They are all of the form $E\colon y^2 = P_3(x)$, where P_3 denotes a monic polynomial of degree three with rational coefficients. The task of finding pairs (x, y) on these curves could turn out to be complicated. We could for instance observe that the points $(-1, 4)$ and $(-2, 3)$ belong to E_1. On the other hand, we can get a few points on E_2 by using $y = 0$ and hence getting $(0, 0), (1, 0)$ and $(-1, 0)$. There are two main steps to find points on curves given by equations as above: we can draw a line passing through two points to find a third one, or, we can use a point (x, y) in the graph to obtain the point $(x, -y)$ using the symmetry with respect to x-axis. We want to combine these steps to consider the following operation:

(a) Find two points P, Q in $E(\mathbb{Q})$.

(b) Draw a line L passing by the points P and Q. That line intersects the curve E at a third point $R = (x_R, y_R)$.

(c) Compute the symmetric point $(x_R, -y_R)$ of the point R.

Theorem 1. *Suppose that the result of the above mentioned operation is denoted by $P + Q$ and we add the point $O = \infty$ to our curve E to make it compact. The point O will have the property that joining two symmetric points (x, y) and $(x, -y)$ passes through O and we obtain the following properties:*

1. *$P + Q + R = O$ if and only if there is a line passing by the points P, Q, R on E. In particular, for all points P in E:*

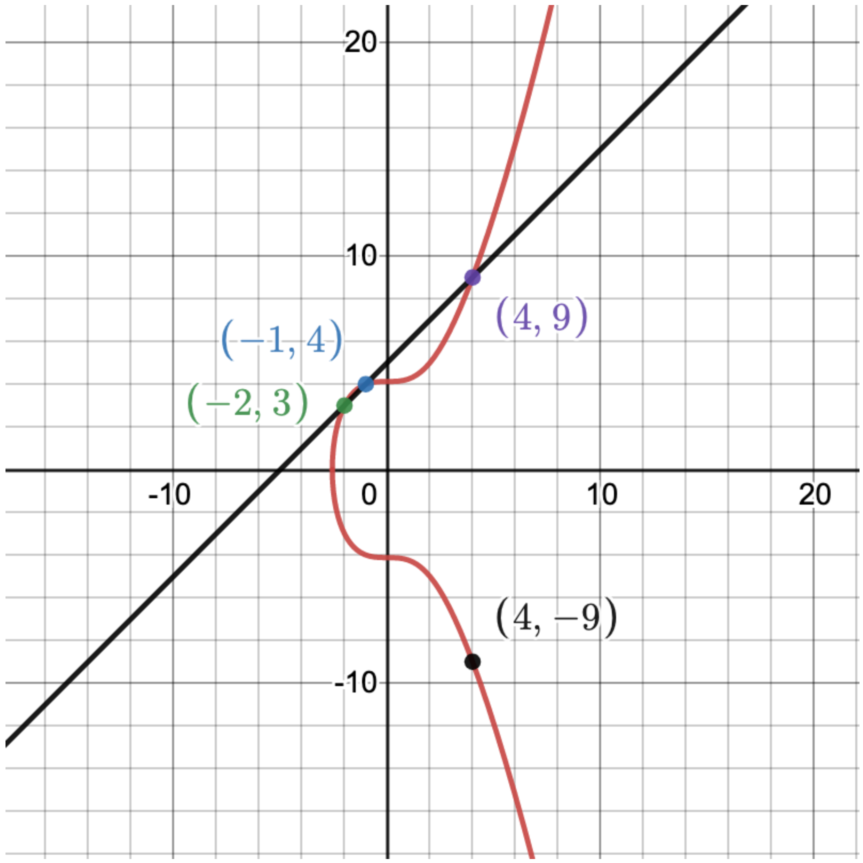
$$P + O = P.$$

2. *For $P = (x, y)$ the point $(-x, y)$ is denoted $-P$ and it satisfies $P+(-P)+O = O$ or*

$$P + (-P) = O.$$

3. *For any three points P, Q, R on the curve E, we will have*

$$(P + Q) + R = P + (Q + R).$$



Corollary 2. *The rational points of an elliptic curve with equation* $y^2 = P_3(x)$ *form a group* $(E, +, O)$ *with internal operation* $+$ *and with neutral element* O.

Theorem 3. *(Mordell, 1922) Let* $y^2 = p_3(x)$ *be an elliptic curve, such that the polynomial* p_3 *does not have repeated roots. Then, the group* $(E, +, O)$ *is finitely generated.*

Example 4. In $E_1\colon y^2 = x^3 + 17$ for example, the line joining the points $(-2, 3)$ and $(-1, 4)$ is the line of equation $L\colon y = x + 5$. The other point in the intersection $L \cap E_1$ is $(4, 9)$ and we have $(-2, 3) + (-1, 4) = (4, -9)$.

1.2 Complex elliptic curves

Consider elliptic curve $y^2 = p_3(x) = x^3 + ax + b$ where the polynomial p_3 has now in general complex coefficients $(a, b) \in \mathbb{C}$, and we are looking at pairs of complex numbers (x, y) satisfying the equation. In this case, the group law is the result of a natural addition on the complex plane mod out by a discrete subgroup. Consider two complex numbers ω_1 and ω_2 linearly independent over $\mathbb{R}$ and the subgroup Λ of $\mathbb{C}$ defined by

$$\Lambda = \{z \in \mathbb{C} \mid z = n\omega_1 + m\omega_2 \text{ where } n, m \in \mathbb{Z}\}.$$

A subgroup like Λ is called a lattice and the quotient group $\mathbb{T} = \mathbb{C}/\Lambda$ is called a torus with fundamental periods ω_1 and ω_2. A function on $\mathbb{T}$ is the same as a double periodic function $f(z+\omega_1) = f(z)$ and $f(z+\omega_2) = f(z)$ on $\mathbb{C}$.

Theorem 5. *There exist a function $\wp\colon \mathbb{T} \longrightarrow \mathbb{C}$ that together with its derivative $\wp'\colon \mathbb{T} \longrightarrow \mathbb{C}$ satisfies the equation $\wp'^2 = 4\wp^3 - g_2\wp - g_3$, providing us henceforth with a group isomorphism:*

$$[\wp, \wp'/2]\colon \mathbb{T} \longrightarrow (E, +, O),$$

where E is the elliptic curve of equation $E\colon y^2 = x^3 - g_2/4x - g_3/4$. The function $\wp$ is called the Weierstrass $\wp$-function associated to $\mathbb{T}$.