Chapter 2

Elliptic curves as cryptographic groups

The purpose of this chapter is to introduce elliptic curves as they are used in cryptography. Put simply, an elliptic curve is an abstract type of *group*.

Perhaps a newcomer will find this abstractness apparent immediately when we insist that to understand elliptic curve groups in cryptography, the reader should be familiar with the basics of *finite fields* $\mathbb{F}_q$. This is because, more generally, elliptic curves are groups which are defined on top of (over) fields. Even though elliptic curve groups permit only one binary operation (the so called *group law*), the operation itself is computed within the *underlying field*, which by definition permits two operations (and their inverses). For a general field K, the group elements of an elliptic curve E are *points* whose (x, y) coordinates come from $\overline{K}$ (the algebraic closure of K), and which satisfy the (affine) curve equation for E, given as

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

where $a_1, ..., a_6 \in \overline{K}$. Equation (2.1) is called the *general Weierstrass equation* for elliptic curves. Aside from all the $(x, y) \in \overline{K}$ solutions to the equation above, there is one extra point which can not be defined using the affine equation, but which must be included to complete the group definition. This point is called the *point at infinity*, which we denote by $\mathcal{O}$, and we will define it properly in a moment.

If $a_1, ..., a_6 \in K$, then we say E is *defined over* K, and write this as E/K (the same goes for any extension field L of K). Before we go any further, we make a convenient simplification of the general Weierstrass equation. If the field characteristic is not 2 or 3, then divisions by 2 and 3 in K permit the substitutions $y \mapsto (y - a_1x - a_3)/2$ to give $E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$, and then $(x, y) \mapsto \left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$, which (upon appropriate rescaling) yields the following simplified equation.

$$E : y^2 = x^3 + ax + b. \tag{2.2}$$

Equation (2.2) is called the *short Weierstrass equation* for elliptic curves, and will be used all the way through this text. Namely, we will always be working over large prime fields, where the short Weierstrass equation covers all possible isomorphism classes of elliptic curves, so the curves we use will always be an instance of (2.2).

Example 2.0.1 (Magma script). $E/\mathbb{Q} : y^2 = x^3-2$ is an elliptic curve. Along with the point at infinity $\mathcal{O}$ (which we are still yet to define), the set of points over $\mathbb{Q}$ is written as $E(\mathbb{Q})$, and is defined as $E(\mathbb{Q}) = \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : y^2 = x^3-2\} \cup \{\mathcal{O}\}$. The point $P = (x_P, y_P) = (3, 5)$ lies in $E(\mathbb{Q})$, as do $Q = (x_Q, y_Q) = \left(\frac{129}{100}, \frac{-383}{1000}\right)$ and $R = (x_R, y_R) = \left(\frac{164323}{29241}, \frac{-66234835}{5000211}\right)$, so we can write $P, Q, R \in E(\mathbb{Q})$. We usually write E to represent the group of points over the full algebraic closure, so for example, the point $S = (x_S, y_S) = \left(0, \sqrt{-2}\right) \in E = E(\overline{\mathbb{Q}})$, but $S \notin E(\mathbb{Q})$. Soon we will be defining the binary group operation $\oplus$ on E using rational formulas in the underlying field, so an active reader can return to this example with these formulas to verify that $R = P \oplus Q$, where x_R, y_R are computed from x_P, y_P, x_Q, y_Q using additions and multiplications (also subtractions and inversions) in $\mathbb{Q}$. Furthermore, it can also be verified that $Q = P \oplus P$, so that $R = P \oplus P \oplus P$; we usually write these as $Q = [2]P$ and $R = [3]P$, where $\underbrace{P \oplus P \cdots \oplus P}_{n} = [n]P$ in general. To finish this example, we remark that if $(x', y') \in E$, then $(x', -y') \in E$ (but is not distinct if $y' = 0$), which is true for any elliptic curve in short Weierstrass form.

Example 2.0.2 (Magma script). $E/\mathbb{F}_{11} : y^2 = x^3 + 4x + 3$ is an elliptic curve. $E(\mathbb{F}_{11})$ has 14 points: $(0, 5)$, $(0, 6)$, $(3, 3)$, $(3, 8)$, $(5, 4)$,$(5, 7)$, $(6, 1)$, $(6, 10)$, $(7, 0)$, $(9, 3)$, $(9, 8)$, $(10, 3)$, $(10, 8)$, not forgetting the point at infinity $\mathcal{O}$. Notice that all but two points come in pairs (x', y') and $(x', -y')$, the exceptions being $(x', y') = (7, 0)$ (since $y' = -y' = 0$) and $\mathcal{O}$. If we form the quadratic extension $\mathbb{F}_{q^2} = \mathbb{F}_q(i)$ with $i^2 + 1 = 0$, then considering E over $\mathbb{F}_{q^2}$ will allow many more solutions, and give many more points: namely, $\#E(\mathbb{F}_{q^2}) = 140$. In addition to the points in $E(\mathbb{F}_q)$, $E(\mathbb{F}_{q^2})$ will also contain those points with x-coordinates in $\mathbb{F}_q$ that did not give $x^3 + 4x + 3$ as a quadratic residue in $\mathbb{F}_q$ (but necessarily do in $\mathbb{F}_{q^2}$), and many more with both coordinates in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Examples of both such points are $(2, 5i)$ and $(2i + 10, 7i + 2)$ respectively. It is not a coincidence that $\#E(\mathbb{F}_q) \mid \#E(\mathbb{F}_{q^2})$, since $E(\mathbb{F}_q)$ is a subgroup of $E(\mathbb{F}_{q^2})$.

Not every tuple $(a, b) \in K \times K$ gives rise to the curve given by $f(x, y) = y^2 - (x^3 + ax + b) = 0$ being an elliptic curve. If there exists $P = (x_P, y_P)$ on f such that both partial derivatives $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ vanish simultaneously at P, then P is called a *singular* point and f is also deemed singular. Conversely, if no such point exists, f is called *non-singular*, or *smooth*, and is then an elliptic curve. It is easy enough to show that a singularity occurs if and only if $4a^3 + 27b^2 = 0$ (see [Sil09, Ch. III.1, Prop. 1.4]), so as long as $4a^3 + 27b^2 \neq 0$ in K, then $E/K : y^2 = x^3 + ax + b$ is an elliptic curve.

In cryptography we only ever instantiate elliptic curves defined over finite fields, but it is often conceptually helpful to view graphs of elliptic curves over $\mathbb{R}$. We illustrate the difference between singular and non-singular (smooth) elliptic curves in Figures 2.1-2.4.

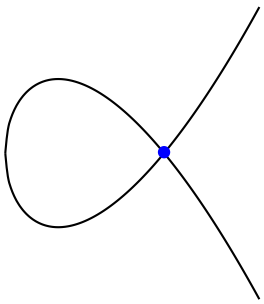

Figure 2.1: Singular curve $y^2 = x^3 - 3x + 2$ over $\mathbb{R}$.

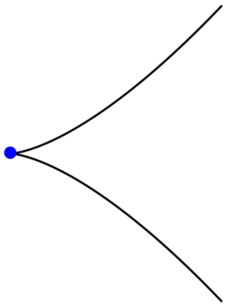

Figure 2.2: Singular curve $y^2 = x^3$ over $\mathbb{R}$.

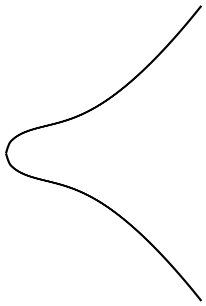

Figure 2.3: Smooth curve $y^2 = x^3 + x + 1$ over $\mathbb{R}$.

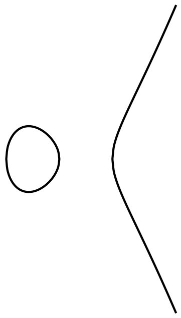

Figure 2.4: Smooth curve $y^2 = x^3 - x$ over $\mathbb{R}$.