1 Elliptic Curves

1.1 Geometry Intuition

Before we go on with more theoretical topics, let us examine another application of the quite abstract theory of algebra we have studied in the previous chapter, namely elliptic curves cryptography. It should be mentioned that linear algebra is by far not the only topic relevant in this context. In fact, important aspects of the theory of elliptic curves require the understanding of function analysis – where it actually comes from – but here we will focus on algebra and group theory.

Elliptic Curves (EC) provide the mathematical background for variants of public key cryptography. This kind of cryptography is being developed since the eighties, but it took a while until it was accepted by industry. It is the main public key cryptographic scheme today. Its acceptance was accelerated by the smartphone boom. In smartphones and other devices with restricited resources, classic cryptographic schemes are not very practical. Their drawback is the computational overhead resulting from key size. Many cryptoanalytical attacks on classic cryptography are known that force cryptographers to use huge keys. To achieve 128-bit security with RSA, we need keys with at least 3072 bits. The same level of security can be reached with EC cryptography, according to known attacks today, with 256 bits. A huge improvement!

EC cryptography is different from classic cryptography in various respects. First, it includes much more math. That is to say, it does not include theory from only one or two branches of mathematics like number theory in classic cryptography, but from many different branches. This has huge impact on cryptoanalysis. Hidden attacks may linger around in apparently remote fields of mathematics that we did not account for. However, the theory surrounding EC is very well understood today and, as said, it is the mainline cryptography today.

Second, the basic means, especially the group we need for public key cryptography, are much more "engineered" than in classic cryptography. Classic schemes are based mainly on modular arithmetic, which was well known centuries before anyone thought of cryptography. The groups found in modular arithmetic, in particular the multiplicative group, was then used to define cryptographic tools. In elliptic curves, there are no such groups "by nature". They are constructed on the curves with the purpose to use them in cryptography. Therefore, EC may sometimes feel a bit artificial. It is important to understand that the group we define on the curves is defined voluntarily according to

our purpose. When we speak of *point addition* in this context, one must not confuse this operation with the arithmetic operation of addition. It is something totally different.

Anyway, what are elliptic curves in the first place? Elliptic curves are polynomials that were intensively studied in the late 19^{th} century, especially by German mathematician Karl Weierstrass (1815 – 1897), who was of huge importance in the sound fundamentation of analysis. We will meet him again in the third part. He studied polynomials of the form

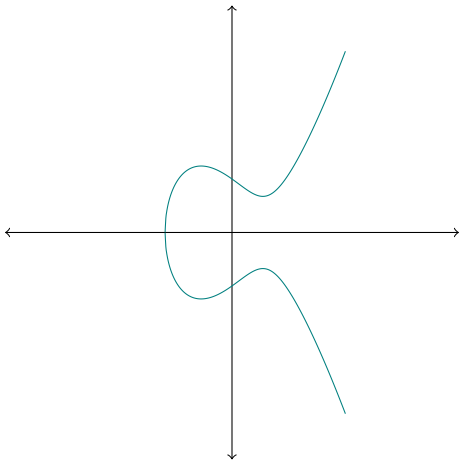
$$y^2 = x^3 + ax + b, \tag{1.1}$$

which is said to be in *Weierstrass form*. Obviously, we can easily transform this equation into a form that looks more like something that can be computed, namely:

$$y = \sqrt{x^3 + ax + b}. \tag{1.2}$$

But be careful! Weierstrass polynomials are not functions, at least not in $\mathbb{R}$, since there is not exactly one y for each x. When the expression $x^3 + ax + b$ becomes negative, there is, in the world of real numbers, no solution for the right-hand side of the equation. That is, there is no y for x that cause that expression to be negative.

This is quite obvious, when we look at the geometric interpretation of that polynomial. It looks – more or less – like in the following sketch:

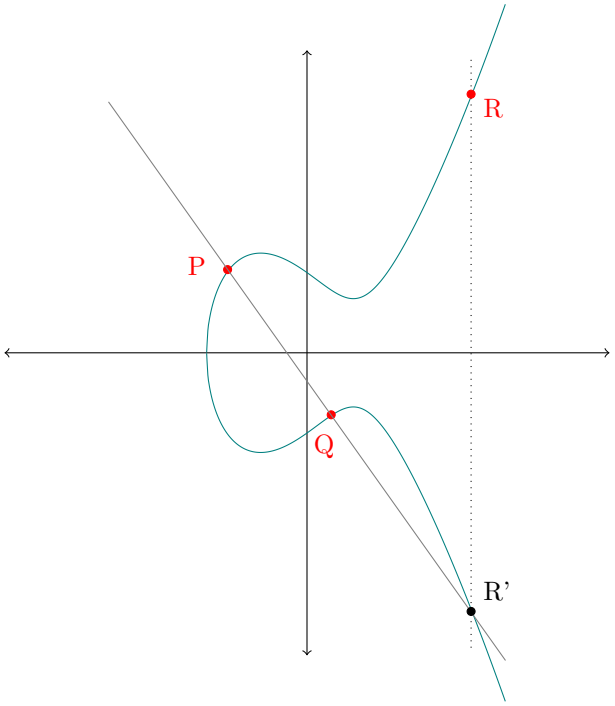


The exact shape depends on the coefficients a and b. The bubble on the left may sometimes be a circle or ellipse completely separated from the "tail" on the right; it may, in other cases, be less clearly distinguished from the tail on the right, forming just a tiny bulge in the tail.

Anyhow, the point is that the curve "ends" on the left-hand side for some $x < 0$. More precisely, it ends where x^3, for a negative value, becomes greater than $ax + b$, because, then, the whole expression becomes negative and there is no real square root for it anymore.

We will now start to construct a group on this kind of curves. We call it an *additional group*, but be aware that this is not addition in the sense of the arithmetic operation. It has nothing to do with that! Is a way to combine points with each other that can be captured in a – more or less – simple formula. We will start by giving a geometric interpretation of this operation. This will help getting an intuition. But, again, be aware that we are not dealing with geometry. We will soon deviate from geometry and talk about curves in a quite abstract way.

The following sketch shows an elliptic curve with three points P, Q and R, all coloured in red. These points are in the relation $P + Q = R$. The meaning of this operation is indicated by the lines:



When adding two points P and Q on an elliptic curve, we draw a straight line through them (the grey one). From the nature of the elliptic curve, it is obvious that the straight line will meet the curve once again. At that cross point, we draw a helper point, R'. Then we draw another line (the dotted one) that goes straight up crossing R'. This line will meet the curve again, namely at a point with the same x coordinate, but with the inverse of the y coordinate $-y$. That point is R, the result of $P + Q$.

You see that this operation has in fact nothing to do with arithmetic addition. It is an arbitrary construction to relate three different points.

The straight line is defined as:

$$l = mx + c, \tag{1.3}$$

where m is the slope and c the y-intercept.

$$m = \frac{y_Q - y_P}{x_Q - x_P} \tag{1.4}$$

$$c = y_P - mx_P \tag{1.5}$$

Now we set the two formulas equal:

$$(mx + c)^2 = x^3 + ax + b, \tag{1.6}$$

which is equivalent to

$$x^3 + ax + b - (mx + c)^2 = 0 \tag{1.7}$$

We know already that x_P and x_Q are intersections and, therefore, know that $x - x_P$ and $x - x_Q$ are factors of the polynomial above. We postulate that $x - x_R$ is also a factor and, hence, get

$$x^3 + ax + b - (mx + c)^2 = (x - x_P)(x - x_Q)(x - x_R), \tag{1.8}$$

which is the same as

$$x^3 + (x_P + x_Q + x_R)x^2 + (x_P x_Q + x_P x_R + x_Q x_R)x - x_P x_Q x_R.$$

We can derive

$$-m^2 = -x_P - x_Q - x_R \tag{1.9}$$

and, hence:

$$x_R = m^2 - x_P - x_Q. \tag{1.10}$$

1.2 Projective Geometry

1.3 EC modulo a Prime

1.4 EC Crypto Systems

1.5 Cryptoanalysis

1.6 Mr. Frobenius

1.7 Mr. Schoof

1.8 Mr. Elkies and Mr. Aktin

1.9 EC in Practice