Elliptic Curve Cryptography: A Gentle Introduction — Notes

Patrick Maedgen

September 2019

1 What is an Elliptic Curve?

An elliptic curve is defined as the set of points satisfying $y^2 = x^3 + ax + b$, known as the Weierstrass Normal Form. For the purposes of elliptic curve cryptography we want to exclude singular curves, where $4a^3 + 27b^2 \neq 0$. We also need to include a "point at infinity" denoted as 0. So, for now, we will define an elliptic curve as the set of points $\{(x, y) \in R^2 |\ y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0\} \cup \{0\}$.

2 Groups

A group is a set where the addition operation is defined. For a set to be a group, addition must be defined with the following properties:

1. Closure: If $a, b \in G, then a + b \in G$.
2. Associativity: $(a + b) + c = a + (b + c)$
3. Contains an Identity Element: $a + 0 = 0 + a = a$. For our case, the point at infinity is the identity element.
4. Every Element has an Inverse: For every a, there is some b such that $a + b = 0$.

We can include a fifth property, Commutativity, where $a+b = b+a$ to define abelian groups.

If we can show these properties to hold we can assume other properties to be true. Namely, the identity element and inverses are unique. (*i.e.* there is only one 0, and only one b for each a such that $a + b = 0$).

3 Group Law and Elliptic Curves

To define a group over elliptic curves we can say:

- The elements of the group are the points on the curve

- The identity element is 0, ”the point at infinity”
- The inverse of point P, $-P$ is the point mirrored across the x-axis.
- Given three aligned, non-zero points $P,\ Q,\ R$ then $P+Q+R=0$ and $P+Q=-R$.

4 Geometric Addition

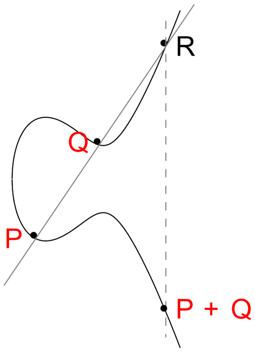

Figure 1: $P+Q=-R$ (*i.e.* P + Q is the inverse of R, the intersection of the line).

Figure 1 shows a geometric view of $P+Q=-R$. If the line through P and Q intersect the line at R, then $P+Q=-R$. Some special cases must be considered in order to define the addition of points.

4.1 What if P or Q equals 0?

As the definition of the identity element, ”the point at infinity”, shows $P+0=P$ and $Q+0=Q$.

4.2 What if $P=-Q$?

Again we can look to the properties that make a group and see that the inverse of P is $-P$, and so $P+-P=0$.

4.3 What if $P=Q$?

If P is equal to Q, then the line drawn between P and Q will be tangent to the curve at that point. Following the rules before $P+P=-R$ where $-R$ is the point where the tangent line intersects the curve. If P is the tangent point, then one can almost imagine a line between P and the point at infinity. The point this line intersects is R and its inverse is $P+P$. See Figure 2.

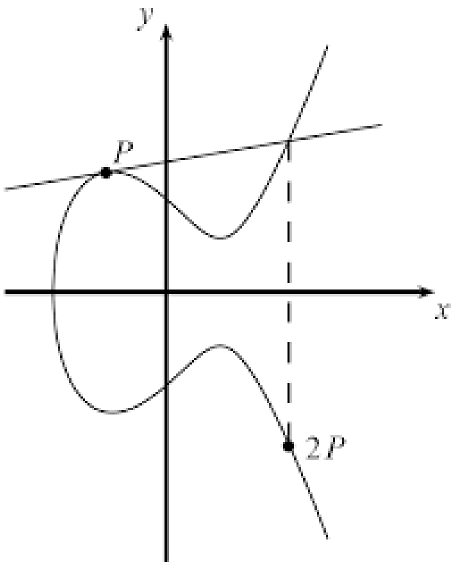

Figure 2: $P + P = -R = 2P$ Multiplication will be discussed more later.

4.4 What if $P \neq Q$, but there is no point R that intersects the curve?

This case will happen when the line only intersects two points on the curve. When this happens, the line must be tangent to the curve. Similar to the previous case, if P is the tangent point and the tangent line intersects the curve at Q, then it is possible to envision the line as instead being between Q and the point of infinity. This line then intersects the curve at P. So it can be said that, in this case, $P + Q = -P$.

5 Algebraic Addition

We just showed how to find many of the edge cases so for simplicity we will only look at the non-symmetric, non-zero points. Where $P = (x_P,\ y_P)$ and $Q = (x_Q,\ y_Q)$. We have already established that P and Q are distinct, so that means the line intersecting the two points must have a defined slope.

$$m = \frac{y_P - y_Q}{x_P - x_Q} \tag{1}$$

Point $R = (x_R,\ y_R)$ can also be found.

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

$$y_R = y_P + m(x_R - x_P) \tag{3}$$

or,

$$y_R = y_Q + m(x_R - x_Q) \tag{4}$$

The case where $P = Q$ is special, and as such the slope is found with a different equation.

$$m = \frac{3x_P^2 + a}{2y_P} \tag{5}$$

m can be seen to be the first derivative of y_P which is $\pm\sqrt{x_P^3 + ax_P + b}$.

6 Scalar Multiplication

We can define another operation over the group, scalar multiplication. It can be written as $nP = P + P + \cdots + P$. nP can be computationally costly to compute, so algorithms such as the Double and Add algorithm are used to reduce the time complexity.

6.1 What if we know P and nP but we want to find n?

This comes to one of the fundamental questions of elliptic curves and the basis of elliptic curve cryptography. It is known as the "Logarithm Problem". A variant of which, known as the "Discrete Logarithm Problem", will be discussed later on. No known algorithm is known to solve the problem in polynomial time, which is what gives elliptic curves important applications in cryptography.