Zero Knowledge Handbook

Amar Singh

November 14, 2018

Contents

Chapter 1

Elliptic Curves

1.1 Elementary Equations

The simplest way to describe an elliptic curve is as the set of all solutions to an equation of the form $y^2 = x^3 + ax + b$ such that $a, b \in \mathbb{R}$ and $-16(4a^3 + 27b^2) \neq 0$.

Although this may seem like a complex equation, it is actually the clever form of a very natural family of equations. To better understand this equation, we ask the question: *if you have two points on an elliptic curve and you take the line between those two points, will you always get a third point on the curve?* The answer is no, but we can *define* things such that the line between any two points on an elliptic curve will always give you another point on the curve. This is the primary intuition behind Elliptic Curve Cryptography.

Elliptic curves in the form $y^2 = x^3 + ax + b$ have a small handful of different shapes as a, b vary. The problem is when we cross the point at which the rounded part pinches off; at this point, the curve becomes ”non-smooth” (or *singular*) and this is no bueno. The condition $-16(4a^3 + 27b^2) \neq 0$ ensures that this case is excluded from our consideration.

The ”canonical” shape of the elliptic curve is given by the specific example $y^2 = x^3 - x + 1$.

1.2 Algebraic Structures

The points on an elliptic curve have an **algebraic structure**. Adding two points will involve taking the line passing between them and finding the third point of intersection with the elliptic curve. In order to make ”adding points” rigorous, we need to discuss special cases.

If we have two points P, Q on an elliptic curve E defined by $y^2 = x^3 + ax + b$, then to compute $P + Q$, we execute the following geometric algorithm:

1. Form the line $y = L(x)$ connecting P and Q
2. Compute the third intersection point of L and E; call it R
3. Reflect R across the x-axis to get the final point $P + Q$

To verify the validity of this algorithm, we can solve the joint system of the curve and the line, which is equivalent to solving

$$L(x)^2 = x^3 + ax + b$$

Since $L(x)$ is a degree 1 polynomial, this equation is a cubic polynomial in x

$$x^3 - L(x)^2 + ax + b = 0$$

If we already have two solutions to this equation with distinct x-values, then there has to be a third because having the root of a polynomial means you can factor, and we have two distinct roots so we know that our polynomial has a divisor

$$(x - p_1)(x - q_1)$$

But this implies that the remainder must be a linear polynomial, and because the leading term is x^3 it has to look like $(x - r_1)$ for some r_1. And so, $(r_1, L(r_1)$ is our third point.

Moreover, $p_1 + r_1 + q_1$ must be equal to the opposite of the coefficient of x^2 in the above equation, so we can solve for it without worrying about how to factor cubic polynomials.

Two Takeaways Here

1. Any time we make a new mathematical definition with the intent of overloading some operators (ie + or -), we need to verify that the operators behave as we expect them to behave in all cases.
2. We're encoding a *computational structure* in an elliptic curve. The ability to add and negate opens up a world of computational possibilities, so now we can ask questions about the efficiency of computing functions within this framework (as well as reversing them).

In this situation, it is desirable for the points of an elliptic curve to form an abelian group such that

1. Additive identity: $\forall P \in E$, $P + 0 = 0 + P = P$
2. Inverse: $\forall P \in E$, $\exists (-P) \in E$ such that $P + (-P) = 0$
3. Commutative: $\forall P, Q \in E$, $P + Q = Q + P$
4. Associative: $(P + Q) + R = P + (Q + R)$.

With this in mind, we need to define the following

1. identity element
2. how to get the additive inverse of a point
3. how to add a point to itself
4. what to do if two points form a vertical line

The intuition behind (3) comes from the fact that, if you want to double a point, or add $P + P = 2P$, then you can't take the line joining those two points because we need two distinct points to define a line. Even so, we can take the *tangent* line to the curve at P and look for the second point of intersection. We know there will be a second point of intersection because of

Theorem 1.2.1 (Bezout's Theorem). *If we have two plane algebraic curves which do not share a common component (i.e. do not have infinitely many common points), then the number of common points of two such curves is at most equal to the product of their degrees.*

1.2.1 Projective Spaces and the Ideal Line

To define our additive identity, we *invent* a new point which is the intersection of all vertical lines and call it **the point at infinity**, also known as "zero". Because it is the additive identity, we demand that it lies on every elliptic curve and we'll say that it reflects zero across the x-axis so we still get 0.

If we want to get the additive inverse of a point $P = (x, y)$, we can just have it be the point $-P = (x, -y)$ reflected across the x-axis; the two points form a vertical line so by our algorithm they "add" to zero.

To better understand why we can define our point at infinity to satisfy the additive identity property, we'll discuss Projective Spaces.

The main idea is that we want to make a geometric space where points are actually lines.

In the context of linear algebra, we take a three dimensional Euclidean space $\mathbb{R}^3$ and look at the lines that pass through the origin. Make each of these lines its own point and call the resulting space $\mathbb{P}^2$, the projective plane.

Every nonzero vector $v \in \mathbb{R}^3$ spans a line (by taking all multiples λv for $\lambda \in \mathbb{R}$). Therefore, instead of representing a point in a projective space by a line, we can represent it by a vector, with the additional condition that two points are the same if they're multiples of each other.

The formal way of saying this is that projective space is the *quotient space*

$$\mathbb{P}^2 = (\mathbb{R}^3 - 0)/v \sim \lambda v$$

If we are working with vectors in $\mathbb{R}^3$, then we're looking at coordinates like (x, y, z) such that $x, y, z \in \mathbb{R}$ and $(0, 0, 0)$ is not allowed. In addition, we're defining things such that (x, y, z) is the same as $(2x, 2y, 2z)$ or $(-6x, -6y, -6z)$ or any other way to scale every component by the same amount. To denote the difference between usual vectors and our new coordinates, we use square brackets and colons...so a point in a 2-dimensional projective space is $[x : y : z]$ such that $x, y, z \in \mathbb{R}$, they are not all zero, and $[x : y : z] = \lambda[x : y : z] = [\lambda x : \lambda y : \lambda z]$ for any $\lambda \in \mathbb{R}$.

Now, let's explore the geometry of this new space. If $P = [x : y : z]$ with $z \neq 0$, then we can always scale by $\frac{1}{z}$ so that the point looks like

$$[x/z : y/z : 1]$$

Now, x/z and y/z can be anything (think of it like $[a : b : 1]$) and different choices provide distinct points. Therefore, when $z \neq 0$, we have this special representation (called the *affine slice*) and it's easy to see that all of these points form a copy of the usual Euclidean plane sitting inside $\mathbb{P}^2$.

Each line (each vector with $z \neq 0$) intersects this new plane in exactly one point, so this describes a one-to-one mapping in the affine slice of the Euclidean plane. But then when $z = 0$, we get some other stuff that makes up the rest of $\mathbb{P}^2$. Since x, y can't both be zero, we'll assume y is not zero, and then we can do the same normalization trick to see that all the points we get are

$$[a : 1 : 0]$$

Since a can be anything and you get distinct points for different choices of a, this forms a copy of the real line inside of $\mathbb{P}^2$ but outside of the affine slice. This line is referred to as the *ideal line* to distinguish it from the lines that lie inside the affine slice $z = 1$. Actually, the ideal line is more than just a line; it's actually a circle. To see why that's the case, consider what happens as a grows very large...we have

$$[a : 1 : 0] = [1 : 1/a : 0]$$

and the right hand side approaches $[1:0:0]$, the last missing point! In other words, $[1:0:0]$ is the *boundary* of the line $[a:1:0]$, and the circle we get here is the boundary of the affine slice $[a:b:1]$.

Using this, we can see what it means for "two parallel lines" to intersect. Take the two lines given by

$$[a:1:1], [b:2:1]$$

If we think of these as being in the affine slice of $\mathbb{R}^2$ such that $z=1$, it's the lines given by $(a,1),(b,2)$, which are obviously parallel. But where do they intersect as a,b get very large

$$[1:1/a:1/a], [1:1/b:2/b]$$

which both become $[1:0:0]$ in the limit. This works because projective space inherits some structure when we pass to the quotient (more specifically, it inherits a metric that comes from the sphere of radius 1).

1.2.2 Homogeneous Equations and the Weierstrass Normal Form

Elliptic curves are defined by homogeneous equations over projective space. Specifically, an elliptic curve equation is any homogeneous degree three equation whose discriminant is zero. By homogeneous, we mean that all the powers of the terms add up to three, so it has the general form

$$0 = a_0z^3 + a_1z^2y + a_2z^2x + a_3y^2x + ...$$

Now the solutions to this equation are required to be *projective* points $[x:y:z]$.

This helps us to understand why we want the special form of elliptic curve $y^2 = x^3 + ax + b$, also known as the *Weierstrass normal form.*

We want the projective point $[0:1:0]$ to be our zero point. If we choose our axes appropriately (swapping the letters x,y,z), then $[0:1:0]$ lies at the intersection of all vertical lines. That point isn't a solution to all homogeneous degree-three curves, but it is a solution to homogeneous equations that look like this

$$y^2z = x^3 + axz^2 + bz^3$$

In fact, there is a theorem that says that for any homogeneous degree three equation you start with, you can always pick your projective axes to get an equivalent equation of the form above. And then, if we pick our classical Euclidean slice to be $[x:y:1]$, we get back to the standard form $y^2 = x^3 + ax + b$. This is also known as the Weierstrass normal form.

After all that math, we come to this closing definition...

Definition 1.2.2. Let k be a field and let E be the equation of an elliptic curve in Weierstrass form. Define $E(k)$ to be the set of projective points on E with coordinates in k along the ideal point $[0:1:0]$. $E(k)$ is a group under the operation of adding points, so we call it the *elliptic curve group* for E over k.

We've just brushed the surface of the algebraic structure of elliptic curves. The next step for a mathematician would be to classify all possible algebraic structure for elliptic curves...LOL reminds me of the classification of finitely generated abelian groups.

1.3 Elliptic Curves over Finite Fields

1.4 Diffie-Hellman Key Exchange

1.5 Shamir-Massey-Omura encryption and Digital Signatures

Chapter 2

zk-SNARK

2.1 Exploring Elliptic Curve Pairings

2.2 Quadratic Arithmetic Programs

2.3 zk-SNARKs Under the Hood

Chapter 3

zk-STARK

3.1 Proofs with Polynomials

3.2 Fast Reed-Solomon Interactive Oracle Proofs of Proximity

3.3 zk-STARKs