Davis Lister and Jacob Fisher

Abstract

We will explore the properties of elliptic curves as a an abelian group, as well as investigating some applications of the group to integer factorization problems and public-key cryptography.

We will define an elliptic curve over a field K as an equation of the form

$$y^2 = x^3 + ax + b,$$

where $a, b \in K$ and the discriminant $-16(4a^3 + 27b^2) \neq 0$. We may impose an abelian group structure on the set

$$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

of K-rational points on an elliptic curve E over the field K. Often, we will implement the group structure on elliptic curves over fields of the form $\mathbb{Z}/p\mathbb{Z}$, though they are not limited to such fields. The group structure may also be imposed over $\mathbb{R}$, for instance.

Let E be an elliptic curve over a field K, with the equation $y^2 = x^3 + ax + b$. We begin by defining the binary operation $+$ on E(K) such that, for $P_1, P_2 \in E(K)$, $P_1 + P_2 = R \in E(K)$. We will define the $+$ operation as follows:

1. If $P_1 = \mathcal{O}$ set $R = P_2$ or if $P_2 = \mathcal{O}$ set $R = P_1$, terminate and return R. Otherwise write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$.
2. If $x_1 = x_2$ and $y_1 = -y_2$, set $R = \mathcal{O}$, terminate and return R.
3. If $P_1 = P_2$, set $\lambda = \frac{3x_1^2+a}{2y_1}$. Otherwise, set $\lambda = \frac{y_1-y_2}{x_1-x_2}$.
4. Let $x_3 = \lambda^2 - x_1 - x_2$, $\nu = y_1 - \lambda x_1$. Then, $R = (x_3, -\lambda x_3 - \nu)$. Terminate and return R.

It is clear that the identity element in the proposed group $(E(K), +)$ is $\mathcal{O}$, by item one of the above definition. Additionally, item two implies that for some $P \in E(K)$, where $P = (x, y)$, $P^{-1} = (x, -y)$, since $P + P^{-1} = \mathcal{O}$. Furthermore, the definition implies that the group is abelian since at each step one may substitute P_1 for P_1 while leaving $P_1 + P_2 = R$ unchanged. In order to prove that the group $(E(K), +)$ is closed, we will interpret the $+$ operation geometrically.

The group operation $+$ can be interpreted as intersecting the secant line drawn between two points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ where $P_1, P_2 \in E(K)$ and $x_1 \neq x_2$ with the curve S, which is given by the equation $y^2 = x^3 + ax = b$. In the case that $x_1 = x_2$, the resulting line will either be the line tangent to S at x_1, or it will be the vertical secant line connecting (x_1, y_1) and (x_2, y_2). We will address the first case later on. In the second case, the secant line will intersect S at $\mathcal{O} \in E(K)$.

Let L be the line drawn between P_1, P_2 where P_1, P_2 are on S. L is given by the equation

$$y = y_1 + (x - x_1)\lambda.$$

Substituting the equation for L into the equation for S we obtain

$$(y_1 + (x - x_1)\lambda)^2 = x^3 + ax + b.$$

By simplifying we arrive at

$$x^3 - \lambda^2 x^2 + 2\lambda x_1 x - 2y_1 x + ax - y_1^2 + 2y_1 x_1 + b = 0.$$

For $A, B \in \mathbb{R}$, the above equation can be written as

$$x^3 - \lambda^2 x^2 + Ax + B = 0.$$

Since $P_1, P_2 \in L \cap S$, the polynomial above will have x_1 and x_2 as solutions. By the fundamental theorem of algebra

$$0 = x^3 - \lambda^2 x^2 + Ax + B = (x - x_1)(x - x_2)(x - x_3).$$

By expanding the factored form of the polynomial we obtain

$$0 = (x - x_1)(x - x_2)(x - x_3) = x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 - x_1x_3 - x_2x_3)x + x_1x_2x_3.$$

Therefore, we can deduce that

$$x_3 = \lambda^2 - x_1 - x_2.$$

From the equation for L, we obtain that

$$y_3 = y_1 + (x_3 - x_1)\lambda = \lambda x_3 + \nu$$

where $\nu = y_1 - \lambda x_1$. In the case that $P_1 = P_2$, $\lambda = \frac{3x_1^2+a}{2y_1}$. As such, L will intersect S at two points and the polynomial $(x - x_1)(x - x_2)(x - x_3) = 0$ will have a double root. However, the group structure will still be maintained since the above proof does not rely on the precise value of λ, only the structure of the equation for S. Therefore, $(E(K), +)$ is closed.

We return to address the requirement that the discriminant, $\Delta = -16(4a^3 + 27b^2) \neq 0$. We we wish to show that $\Delta = 0$ if and only if an elliptic curve S is singular. A singular curve poses problems for a group structure because at the singular point the derivative is not well defined, which would cause the addition the singular point to itself to not be well defined. For any polynomial $f(x_1, x_2, \dots)$ at the singular point P_0

$$\frac{\partial f}{\partial x_1}(P_0) = \frac{\partial f}{\partial x_2}(P_0) = \cdots = 0.$$

First, we wish to show that if S is singular, then $\Delta = 0$. Let $f(x, y) = y^2 - (x^3 + ax + b)$. Suppose S has a singular point at $P_0 = (x_0, y_0)$. Therefore,

$$\frac{\partial f}{\partial x} y_0^2 - (x_0^3 + ax_0 + b) = -3x_0^2 - a = 0 \Longrightarrow a = -3x_0^2,$$

$$\frac{\partial f}{\partial y} y_0^2 - (x_0^3 + ax_0 + b) = -2y_0 = 0 \Longrightarrow y_0 = 0.$$

Since $y_0 = 0$, all singular points will be roots of $y^2 = x^3 + ax + b$. Observe,

$$0 = x_0^3 - 3x_0^3 + b \Longrightarrow b = 2x_0^3.$$

Thus,

$$\Delta = -16(4(-3x_0^2)^3 + 27(2x_0^3)^2) = 0.$$

We wish to show that if $\Delta = 0$, then S is singular. First we will prove a lemma: if $\Delta = 0$, $y = x^3 + ax + b$ has a double root x_0. Note that

$$-16(4a^3 + 27b^2) = 0 \Longrightarrow b = \sqrt{\frac{-4a^3}{27}}.$$

Furthermore, observe that given the above our equation becomes

$$y = x^3 + ax + \sqrt{\frac{-4a^3}{27}}.$$

The roots of the above equation are

$$x_1 = \frac{a}{\sqrt{3}\sqrt[6]{-wa^3}} - \frac{\sqrt[6]{-a^3}}{\sqrt{3}}, x_2 = \frac{i\sqrt{3}\sqrt[3]{-a^3} + \sqrt[3]{-a^3} + i\sqrt{3}a - a}{2\sqrt{3}\sqrt[6]{-a^3}}, x_3 = \frac{-i\sqrt{3}\sqrt[3]{-a^3} + \sqrt[3]{-a^3} - i\sqrt{3}a - a}{2\sqrt{3}\sqrt[6]{-a^3}}.$$

Note that

$$b = \sqrt{\frac{-4a^3}{27}} \Longrightarrow a < 0 \,\text{for}\, b \in \mathbb{R}.$$

Therefore, our second two solutions become identical

$$x_0 = \frac{\sqrt[3]{-a^3} - a}{2\sqrt{3}\sqrt[6]{-a^3}}.$$

Thus $y = x^3+ax+b$ has a double root x_0. By the lemma, we can deduce that one of the roots of $y = x^3+ax+b$ is a root of its derivative, $y' = 3x^2 + a$. Recall that $f(x, y) = y^2 - (x^3 + ax + b)$. Therefore,

$$f(x_0, 0) = 0^2 - (x_0^3 + ax_0 + b) = 0,$$

$$\frac{\partial f}{\partial x}(x_0, 0) = -3x_0^2 - a = 0,$$

$$\frac{\partial f}{\partial y}(x_0, 0) = 2(0) = 0.$$

Thus S is singular. Furthermore, we can conclude that S is singular if and only if $\Delta = 0$.

An important application of the group $(E(K), +)$ is integer factorization. We will begin by discussing Pollard's $p - 1$ algorithm for integer factorization as a preface to our discussion of Lenstra elliptic curve factorization.

We will define the concept of being power smooth. Let B be a positive integer. The prime factorization of an integer $n = \prod p_i^{e_i}$. If $\forall i$ $p_i^{e_i} \leq B$, n is B-power smooth. Now we will attempt to find a nontrivial factor of a large positive integer N using the Pollard p-1 method. Let us choose a positive integer B. Suppose that there is a prime factor p of N such that $p - 1$ is B-power smooth. Let us choose $a > 1$ such that p does not divide a. Often we will choose $a = 2$ for convenience. By Fermat's Little Theorem

$$a^{p-1} \equiv 1 \mod p.$$

Let $m = \mathrm{lcm}(1, 2, 3, \ldots, B)$. Since $p - 1$ is B-power smooth,

$$p - 1 \mid m \Longrightarrow p \mid \gcd(a^m - 1, N) > 1.$$

We will now explore an example of integer factorization with Pollard's $p - 1$ algorithm.