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 $-16(4a^3 + 27b^2) \neq 0$. 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.

We will examine the geometric analogue of the above operation.

We wish to show that the group has an identity element, inverses and is closed.

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

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

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 $\Delta = 0$.