The Group Operation for Elliptic Curves

D. R. Stinson

On pages 184–185 of the text, we gave formulas for defining a binary operation (addition) on points on an elliptic curve. In this note, we discuss the geometric motivation for these formulas. It is easier to understand what the formulas mean if we consider elliptic curves defined over the real numbers.

We use the same equation for an elliptic curve over $\mathbb{R}$ as we did for the modulo p case considered in the text:

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

where $\mathcal{O}$ is the point at infinity.

First we briefly discuss some properties of the curve E. It is easy to see that E is symmetric with respect to the x-axis, since $(x, y) \in E$ if and only if $(x, -y) \in E$. If we examine the roots of the cubic equation $x^3 + ax + b = 0$, we can identify four cases that can occur:

1. the equation has three distinct real roots
2. the equation has one real root and two complex conjugate roots
3. the equation has two distinct real roots, one of which is a double root
4. the equation has one (triple) real root.

Cases 1 and 2 are called *non-singular* curves and cases 3 and 4 are called *singular* curves. It can be shown that the curve E is singular if and only if $4a^3 + 27b^2 = 0$. We are interested only in non-singular curves, so we will assume that $4a^3 + 27b^2 \neq 0$ (which corresponds to the condition $4a^3 + 27b^2 \not\equiv 0 \bmod p$ given in the modular case).

We now give a geometric description of the addition operation on a non-singular elliptic curve E. This will give rise to the algebraic formulas given in the text.

First suppose that $P, Q \in E$, where $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $x_1 \neq x_2$. Let L be the line through P and Q. The line L will hit E in a third point which we denote by R'. If we reflect R' in the x-axis we get another point on E, which we name R. Then we define $P + Q = R$.

Let's work out the algebraic formula to compute R. First, the equation of L is $y = \lambda x + \nu$, where the slope of L is

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},$$

and

$$\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

We are interested in finding the points on $E \cap L$, so we substitute $y = \lambda x + \nu$ into the equation for E, obtaining the following:

$$(\lambda x + \nu)^2 = x^3 + ax + b,$$

which is the same as

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + b - \nu^2 = 0. \tag{1}$$

The roots of Equation (1) are the x-co-ordinates of points on $E \cap L$. We already know two points on $E \cap L$, namely, P and Q. Hence x_1 and x_2 are two roots of Equation (1).

Since Equation (1) is a cubic equation with two real roots, the third root is also real. There is a very quick way to compute the third root x_3, since two roots are already known. Since Equation (1) is monic, the sum of the three roots is minus the coefficient of x^2, or λ^2. Hence,

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

So x_3 is the x-co-ordinate of the point R'. We will denote the y-co-ordinate of R' by $-y_3$, so the y-co-ordinate of R will be y_3. We can compute y_3 by computing the slope λ of L from the the two points (x_1, y_1) and $(x_3, -y_3)$ on L:

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1},$$

or

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

These are the formulas given in the text.

The case when $P = Q$ is handled in a similar matter, except that we use the tangent to E at P as the line L, in place of the line joining P and Q. The slope of this tangent can be computed by implicit differentiation:

$$2y\frac{dy}{dx} = 3x^2 + a.$$

Substituting $x = x_1$, $y = y_1$, we see that the slope of the tangent is

$$\frac{3{x_1}^2 + a}{2y_1}.$$

The remainder of the analysis is identical to the previous case.

From the geometric description of the addition operation, it is easy to see that addition is commutative. It is also clear that $\mathcal{O}$ is the identity element, and (by definition) the inverse of a point $(x, y) \in E$ is $(x, -y)$. It still remains to prove that this addition operation is associative. For a proof of this, as well as further related results on elliptic curves, see the book by Silverman and Tate [1].

References

[1] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1992.