

Why We ♥ Elliptic Curves

M. L. Smedinghoff and S. G. Smedinghoff

October 18, 2005

1 Introduction

Elliptic curves are quite possibly the coolest branch of mathematics. An elliptic curve is an equation of the form $y^2 = x^3 + ax + b$ where a and b are real numbers. Since an elliptic curve is of the form $y^2 = f(x)$, the graph of an elliptic curve is always symmetric across the x axis. Since $f(x)$ is a cubic polynomial, the graph intersects the x -axis in at most three places.

Since elliptic curves are so cool, we can define addition of points on a curve in the following manner: in order to find the sum of two points P and Q on elliptic curve E , we draw a line connecting P and Q . Notice that this line will intersect E at exactly one other point, which we will denote $P * Q$. $P + Q$ will be defined as the reflection of $P * Q$ across the x -axis. There are certain cases for which this definition will not suffice. One such case is where P and Q are the same point. In this case, we draw the tangent line to E at P and find the second point where this line intersects E . We call this point $P * P$. Again, we reflect this point over the x -axis to obtain $P + P$. Another case is where the line connecting P and Q is vertical. In this case, we define $P + Q$ to be \mathcal{O} , the point at infinity. Note that the line connecting any point and \mathcal{O} will be a vertical line, and reflecting \mathcal{O} about the x -axis results in \mathcal{O} .

To better illustrate how cool elliptic curves are, consider the example $y^2 = x^3 - 5x + 5$. Let E be the elliptic curve, $P = (1, 1)$, and $Q = (-1, -3)$. To find $P + Q$, we first find the line that connects these two points. In this case, the line is $y = 2x - 1$. Next we find the intersection of this line and the elliptic curve by $2x - 1$ into E for y .

$$(2x - 1)^2 = x^3 - 5x + 5$$

$$4x^2 - 4x + 1 = x^3 - 5x + 5$$

$$x^3 - 4x^2 - x + 4 = 0$$

$$x^2(x - 4) - 1(x - 4) = 0$$

$$(x^2 - 1)(x - 4) = 0$$

$$(x - 1)(x + 1)(x - 4) = 0$$

Thus the line intersects E with x -values -1 , 1 , and 4 . 4 is the value in which we are interested. Plugging 4 into $2x-1$, we find that $P * Q$ is $(4,7)$. Thus $P + Q$ is $(4,-7)$.

To further illustrate the spectacularity of elliptic curves, let us compute $P + P$. Our first step is to find the line tangent to E at P using implicit differentiation.

$$y^2 = x^3 - 5x + 5$$

$$2y \frac{dy}{dx} = 3x^2 - 5$$

$$\frac{dy}{dx} = \frac{3x^2 - 5}{2y}$$

Evaluating the derivative at P tells us that the tangent line has a slope of -1 , and thus the equation of the tangent line is $y = -x + 2$. Now we proceed as before and find the intersection of the line and E .

$$(-x + 2)^2 = x^3 - 5x + 5$$

$$x^2 - 4x + 4 = x^3 - 5x + 5$$

$$x^3 - x^2 - x + 1 = 0$$

$$x^2(x - 1) - 1(x - 1) = 0$$

$$(x^2 - 1)(x - 1) = 0$$

$$(x - 1)(x + 1)^2 = 0$$

Thus the tangent line intersects E at 1 and -1 . We are interested in the value -1 , so we plug -1 into $-x + 2$ to obtain the value 3 . Thus the tangent line and E intersect at $(-1,3)$, and $P + P = (-1,-3)$.

2 Proposition 1

One of the cool things about the addition of points on an elliptic curve is that it forms a group. This leads us to Proposition 1.

The points on an elliptic curve, together with \mathcal{O} form an abelian group under the operation of addition defined above.

In order to prove that a set is an abelian group, we need to show that it is closed, it has an identity, every element has an inverse, it preserves associativity, and it commutes.

2.1 Closure

Let E be an elliptic curve with points P and Q . Due to the way we have defined $P * Q$, we know that this point is always on E . Since $P + Q$ is simply the reflection of $P * Q$ across the x-axis, we know $P + Q$ will always be on E since all elliptic curves are symmetric around the x-axis. Since $P + Q$ is an element of the set whenever P and Q are in the set, the set is closed.

2.2 Identity

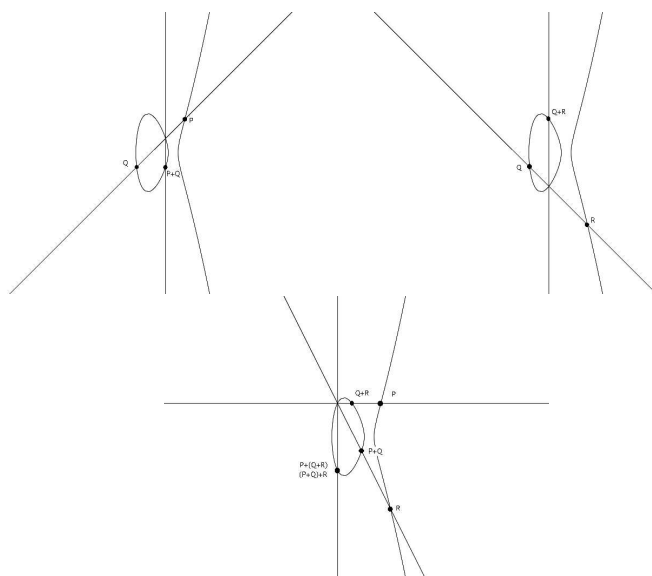
Let E be an elliptic curve with point P . Let \mathcal{O} be the point at infinity. Notice that the line connecting P and \mathcal{O} is a vertical line, so $P * \mathcal{O}$ will be the reflection of P about the x-axis. Since $P + \mathcal{O}$ is the reflection of $P * \mathcal{O}$ about the x-axis, $P + \mathcal{O} = P$. Since $P + \mathcal{O} = P$ for any point P , \mathcal{O} is the identity element.

2.3 Inverses

Let E be an elliptic curve with point P . Let $-P$ be the reflection of P about the x-axis. Notice that $P * -P$ is \mathcal{O} since the line connecting P and $-P$ does not intersect E at a third point. The reflection of \mathcal{O} about the x-axis is simply \mathcal{O} , so $P + -P$ is \mathcal{O} . Therefore every element has an inverse, namely its reflection across the x-axis.

2.4 Associativity

Associativity is hard to prove, but the following pictures should give us an intuitive idea of why associativity holds.



2.5 Commutivity

Let E be an elliptic curve with points P and Q . In order to compute $P + Q$, we must first find the line that goes through these two points. This line intersects E in at most one other place (if it does not intersect E , we call the third intersection point \mathcal{O}). Since there is only one line that we can draw through P and Q , it is easy to see that $P * Q = Q * P$ is the intersection point of the line and E . Now recall that $P + Q$ is the reflection of $P * Q$ across the x-axis and $Q + P$ is the reflection $Q * P$ across the x-axis. Since $P * Q = Q * P$, $P + Q = Q + P$, and therefore the set is commutative.

3 Proposition 2

Because rational numbers are so fabulous, we often look at only points both of whose coordinates are rational, which we will call rational points. Note that we consider \mathcal{O} , the point at infinity, to be a rational point as well. Rational points are simply a fabulous subset of elliptic curves, which leads us to the following proposition:

The set of rational points on an elliptic curve E forms an abelian group under the operation of addition defined above.

In order to prove that the set of rational points on an elliptic curve forms a group, it suffices to show closure since the other four properties of an abelian group all carry over from the superset of real points. Let E be an elliptic curve of the form $y^2 = x^3 + ax + b$ where a and b are rational numbers. Let P and Q be rational points on E . Let $y = mx + n$ be the line connecting P and Q . Notice that m and n have to be rational since P and Q are rational points. Now to find $P * Q$, we must find the intersection of the line and E . We obtain $(mx + n)^2 = x^3 + ax + b$. Notice that this equation is a cubic polynomial with rational coefficients. We already know that the x-coordinates of P and Q are solutions to this equation. Since we have two solutions to our cubic polynomial, $p(x)$, we can write $p(x)$ as a product of three linear terms, two of which are rational. Two rationals times an irrational cannot be rational, so we know the that third linear term must be rational as well. We have just determined that the x-coordinate of the intersection between E and $y = mx + n$ is rational. Plugging the x-coordinate into $y = mx + n$ yields a rational y-coordinate, so $P * Q$ is a rational point. Reflecting $P * Q$ over the x-axis simply negates the y-coordinate, so $P + Q$ is rational as well. We have just shown that adding any two rational points results in a third rational point, so we know the set of rational points on an elliptic curve is closed. Since the set is closed, it forms an abelian group under addition.

4 Proposition 3

Let E be an elliptic curve with rational point P . We define the order of P as the smallest integer $n \geq 1$ such that $nP = \mathcal{O}$ (where $nP = P + P + \dots + P$ n times). Note that the order of \mathcal{O} is 1 since \mathcal{O} is the identity. We now have the following proposition regarding order:

If P is a rational point on an elliptic curve E , then P has order two if and only if P is of the form $(x,0)$.

Let E be an elliptic curve with rational point P . P has order 2 if and only if P is its own inverse. We already noted that the inverse of an element is its reflection across the x-axis. Since reflection across the x-axis negates the y-coordinate, only points with a y-coordinate of zero will remain unchanged after reflection. Therefore, a point will only be its own inverse if it is of the form $(x,0)$.

5 Theorem 1

In fact, every rational point of finite order on an elliptic curve has integral coordinates. This property makes it very easy to evaluate points mod p . We denote the number of rational points mod p as N_p . Note that the point at infinity is included in N_p . For some special elliptic curves, we can determine N_p .

If E is the elliptic curve given by $y^2 = x^3 + 1$ and $\gcd(\phi(p), 3) = 1$, then $N_p = p + 1$.

Let E be the elliptic curve given by $y^2 = x^3 + 1$. Since $\gcd(\phi(p), 3) = 1$, we can always find a solution to the equation $x^3 \equiv q - 1 \pmod{p}$ as long as q is not congruent to 1 (mod p). So $q - 1$ and p are relatively prime. If q is congruent to 1 (mod p), then the congruence becomes $x^3 \equiv 0 \pmod{p}$ the solution to which is $x \equiv 0 \pmod{p}$. Therefore we can plug $q - 1$ into the original congruence for x^3 , giving us $y^2 \equiv q \pmod{p}$. We know that $\frac{p-1}{2}$ numbers are squares ≥ 1 mod p , and each of these squares had two square roots. Thus for every square q , we will find two values of y . All together, this yields $2\frac{p-1}{2} = p - 1$ points on the E . (We have generated the y-coordinates; we can get the x-coordinates by evaluating $x^3 = (q - 1) \pmod{p}$). $q = 0$ will provide one more solution bringing the total to p points. Adding in the point at infinity gives us a grand total of $p + 1$ points. Therefore $N_p = p + 1$.

6 Conclusion

Let E be an elliptic curve with points P and Q . Notice that E is very cool from the above propositions and theorem. Since E is so cool, we love elliptic curves. Therefore we have just proven our title. Tadah!