ELLIPTIC CURVES

ASHLEY NEAL

In most situations, an **Elliptic Curve** E is the graph of an equation of the form

$$y^2 = x^3 + Ax + B,$$

where A and B are constants. This is called the Weierstrass equation for an elliptic curve. Also, A, B, x, y are usually elements of some field. We add a point ∞ to the elliptic curve, we regard it as being at the top and bottom of the y-axis (which is (0:1:0)=(0:-1:0) in the projective space). A line passes through ∞ exactly when it is vertical.

Group Law: Adding points on an Elliptic Curve

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on an elliptic curve E given by $y^2 = x^3 + Ax + B$. Define $P_3 = (x_3, y_3)$ as follows. Draw the line through P_1 and P_2. This intersects E at a third point P_3'. Reflect P_3' across the x-axis to obtain P_3. We define $P_1 + P_2 = P_3$.

The following calculations give explicit formulas for P_3.

Case 1. $x_1 \neq x_2, P_1, P_2 \neq \infty$

The line L through P_1 and P_2 has slope

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

so L is given by the equation $y = m(x - x_1) + y_1$. Then to find where L intersects E, we must solve

$$(m(x - x_1) + y_1)^2 = x_3 + Ax + B,$$

which is equivalent to solving

$$x_3 - m^2x^2 + (A + 2m^2x_1 - 2my_1)x + (B - m^2x_1^2 + 2mx_1y_1 + y_1^2) = 0.$$

Since we already know two roots (x_1 and x_2 since P_1 and P_2 satisfy the the equation) we can find the third point of intersection as follows. If a cubic $x_3 + ax_2 + bx + c$ has roots r, s, t

$$x_3 + ax_2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \dots,$$

then $a = -(r + s + t)$, therefore

$$t = -a - r - s.$$

Hence the third point on intersection is given by

$$x = m^2 - x_1 - x_2, y = m(x - x_1) + y_1.$$

Reflecting across the x-axis gives $P_3 = (x_3, y_3)$ where

$$x_3 = m^2 - x_1 - x_2, y_3 = m(x_1 - x_3) - y_1.$$

Case 2. $x_1 = x_2$ but $y_1 \neq y_2$, and $P_1, P_2 \neq \infty$

Then the line L through P_1 and P_2 is a vertical line and therefore intersects E at ∞. Then reflecting across the x-axis gives ∞. Thus

$$P_1 + P_2 = \infty.$$

Case 3. $P_1 = P_2 = (x_1, y_1)$.
When two points on a curve are very close to each other, the line through them approximates a tangent line. So when $P_1 = P_2$, we let the line L through P_1 and P_2 be the tangent line. The slope of the tangent line is given by $m = \frac{dy}{dx}$, so $y^2 = x^3 + Ax + B$ implies $2y\frac{dy}{dx} = 3x^2 + A$ so $m = \frac{dy}{dx} = \frac{3x^2+A}{2y}$. Thus L, the line tangent to P_1, has slope

$$m = \frac{3x_1^2 + A}{2y_1}.$$

If $y_1 = 0$, then L has undefined slope and is therefore vertical. So as in 2,

$$P_1 + P_2 = \infty.$$

If $y_1 \neq 0$, then L is given by $y = m(x - x_1) + y_1$ as before so we obtain the cubic equation

$$0 = x^3 - m^2 x + \cdots .$$

We only know one root, but it is a double root since L is tangent to E at P_1. So then the other point of intersection is given by

$$x = m^2 - 2x_1, y = m(x - x_1) + y_1.$$

Therefore $P_3 = (x_3, y_3)$ where

$$x_3 = m^2 - 2x_1, y_3 = m(x_1 - x_3) - y_1.$$

Case 4. $P_2 = \infty, P_1 = (x_1, y_1)$
Then the line L through P_1 and P_2 is vertical since E is symmetric about the x-axis. L intersects E at $P_1' = (x_1, -y_1)$ (the reflection of P_1 across the x-axis). Then reflect P_1' across the x-axis to get

$$P_3 = (x_1, y_1) = P_1.$$

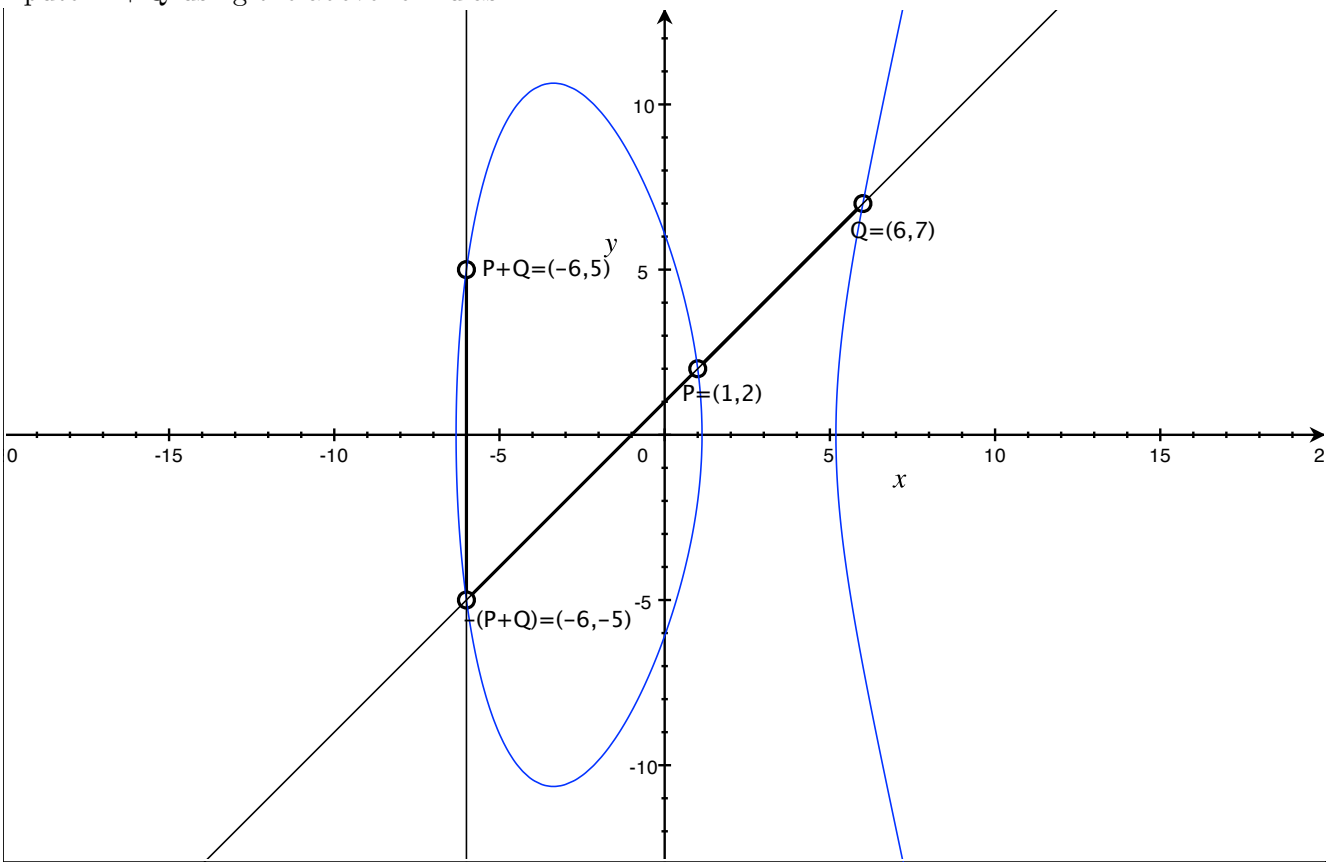
Therefore

$$P_1 + \infty = P_1.$$

Then extend this to include $\infty + \infty = \infty$.

Group Law. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax + B$. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E with $P_1, P_2 \neq \infty$. Define $P_1 + P_2 = P_3 = (x_3, y_3)$ as follows:*
1. If $x_1 \neq x_2$, then $x_3 = m^2 - x_1 - x_2, y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{y_2 - y_1}{x_2 - x_1}$.
2. If $x_1 = x_2$ but $y_1 \neq y_2$, then $P_1 + P_2 = \infty$.
3. If $P_1 = P_2$ and $y_1 \neq 0$, then $x_3 = m^2 - 2x, y_3 = m(x_1 - x_3) - y_1$, where $m = \frac{3x_1^2 + A}{2y_1}$.
4. If $P_1 = P_2$ and $y_1 = 0$, then $P_1 + P_2 = \infty$.
Moreover, define $P + \infty = P$ for all points P on E.

Example: Let $E : y^2 = x^3 - 34x + 37$ be defined over $\mathbb{Q}$, $P = (1, 2)$ and $Q = (6, 7)$. We will compute $P + Q$ using the above formulas.



Since $x_1 \neq x_2$, we will use formula 1.
$m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{7-2}{6-1} = \frac{5}{5} = 1$
$x_3 = m^2 - x_1 - x_2 = (1)^2 - (1) - (6) = -6$
$y_3 = m(x_1 - x_3) - y_1 = (1)((1) - (-6)) - (2) = 7 - 2 = 5$
Therefore $P + Q = (1, 2) + (6, 7) = (-6, 5)$.

Theorem 2.1. *The addition of points on an elliptic curve E satisfies the following properties:*
1. (commutativity) $P_1 + P_2 = P_2 + P_1$ for all P_1, P_2 on E.
2. (existence of identity) $P + \infty = P$ for all points P on E.
3. (existence of inverses) Given P on E, there exists P' on E with $P + P' = \infty$. This point P' will usually be denoted $-P$.
4. (associativity) $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$ for all P_1, P_2, P_3 on E.
Therefore the points on E form an additive abelian group with ∞ as the identity element.

Proof. Identity: $P + \infty = P$ for all P on E by definition.
Inverses: Given $P = (x, y)$, there exists $P' = (x, -y)$ such that $P + P' = \infty$. P' is the reflection of P across the x-axis.
Commutativity: This follows immediately from the fact that the line through P_1 and P_2 is the same as the line through P_2 and P_1.

We can also verify this using the formulas from the group law.
1. Let $x_1 \neq x_2$, then

$$P_1 + P_2 = (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1)$$

where $m = \frac{y_2 - y_1}{x_2 - x_1}$ and

$$P_2 + P_1 = (n^2 - x_2 - x_1, n(x_2 - x_3) - y_2)$$

where $n = \frac{y_1 - y_2}{x_1 - x_2}$.

$$n = \frac{y_1 - y_2}{x_1 - x_2} = \frac{-y_2 + y_1}{-x_2 + x_1} \cdot \frac{-1}{-1} = \frac{y_2 - y_1}{x_2 - x_1} = m.$$

So

$$m^2 - x_1 - x_2 = n^2 - x_2 - x_1.$$

$$n(x_2 - x_3) - y_2 = m(x_2 - x_3) - y_2 = mx_2 - mx_3 - y_2$$

and

$$m(x_1 - x_3) - y_1 = mx_1 - mx_3 - y_1$$

so we need to show

$$mx_2 - y_2 = mx_1 - y_1.$$

Substituting in $m = \frac{y_2 - y_1}{x_2 - x_1}$ and simplifying gives

$$mx_2 - y_2 = \frac{y_2 - y_1}{x_2 - x_1}x_2 - y_2 = \frac{(y_2 - y_1)x_2 - y_2(x_2 - x_1)}{x_2 - x_1} = \frac{y_2x_2 - y_1x_2 - y_2x_2 + y_2x_1}{x_2 - x_1} = \frac{y_2x_1 - y_1x_2}{x_2 - x_1}$$

and

$$mx_1 - y_1 = \frac{y_2 - y_1}{x_2 - x_1}x_1 - y_1 = \frac{(y_2 - y_1)x_1 - y_1(x_2 - x_1)}{x_2 - x_1} = \frac{y_2x_1 - y_1x_1 - y_1x_2 + y_1x_1}{x_2 - x_1} = \frac{y_2x_1 - y_1x_2}{x_2 - x_1}.$$

Thus

$$mx_2 - y_2 = \frac{y_2x_1 - y_1x_2}{x_2 - x_1} = mx_1 - y_1$$

2. Let $P_1 = (x_1, x_2), P_2 = (x_2, y_2)$
If $P_1 + P_2 = \infty$, then $P_2 + P_1 = \infty$ since $x_2 = x_1$ and $y_2 \neq y_1$. Then

$$P_1 + P_2 = \infty = P_2 + P_1.$$

3 and 4. Let $P_1 = P_2$, then

$$P_1 + P_2 = P_1 + P_1 = P_2 + P_1.$$

Associativity: Associativity can be verified directly from the formulas, but it is very tedious. We choose to use a different method.

First we will deal with the cases where ∞ occurs.
If $P_1 = \infty$,

$$(\infty + P_2) + P_3 = P_2 + P_3 = \infty + (P_2 + P_3).$$

Similarly, associativity holds when P_2 or P_3 equals ∞.
If $P_1 + P_2 = \infty$,

$$(P_1 + P_2) + P_3 = \infty + P_3 = P_3.$$

Now we need to show $P_1 + (P_2 + P_3) = P_3$.
Let L be the line through P_2 and P_3. Then $L \cap E = \{P_2, P_3, -(P_2 + P_3)\}$. $P_1 + P_2 = \infty$ implies $P_2 = -P_1$. Let L' be the reflection of L across the x-axis. Then $L' \cap E = \{-P_2, -P_3, (P_2 + P_3)\} = \{P_1, -P_3, (P_2 + P_3)\}$. So then

$$P_1 + (P_2 + P_3) = P_3.$$

Theorem 2.6. *Let $C(x, y, z)$ be a homogeneous cubic polynomial, and let C be the curve in $\mathbf{P}^2_K$ described by $C(x, y, z) = 0$. Let ℓ_1, ℓ_2, ℓ_3 and m_1, m_2, m_3 be the lines in $\mathbf{P}^2_K$ such that $\ell_i \neq m_j$ for all i, j. Let P_{ij} be the point of intersection of ℓ_i and m_j. Suppose P_{ij} is a nonsingular point on the curve C for all $(i, j) \neq (3, 3)$. In addition, we require that if, for some i, there are $k \geq 2$ of the points P_{i1}, P_{i2}, P_{i3} equal to the same point, then ℓ_i intersects C to order at least k at this point. Also, if, for some j, there are $k \geq 2$ of the points P_{1j}, P_{2j}, P_{3j} equal to the same point, then m_j intersects C to order at least k at this point. Then P_{33} also lies on the curve C.*

If Theorem 2.6 is satisfied, then let P, Q, R be points on E. Define the lines

$$\ell_1 = \overline{PQ}, \ell_2 = \overline{\infty, Q+R}, \ell_3 = \overline{R, P+Q}, m_1 = \overline{QR}, m_2 = \overline{\infty, P+Q}, m+3 = \overline{P, Q+R}.$$

We have the intersections:

$\cap$	ℓ_1	ℓ_2	ℓ_3
m_1	Q	$-(Q+R)$	R
m_2	$-(P+Q)$	∞	$P+Q$
m_3	P	$Q+R$	x

Then by Theorem 2.6, x lies on E. $m_3 \cap E = \{P, Q+R, x\}$ and $\ell_3 \cap E = \{R, P+R, x\}$ so by the definition of addition,

$$x = -(P + (Q + R))$$

and

$$x = -((P + Q) + R).$$

Reflecting across the x-axis, we have

$$P + (Q + R) = (P + Q) + R.$$

We still need to show that the hypotheses of Theorem 2.6 are satisfied, namely that the orders of intersection are correct and that the lines ℓ_i are distinct from the the lines m_i.

If some ℓ_i equals some m_i, Theorem 2.6 does not apply. If P, Q, R are collinear, then $P+Q = -R$ so

$$(P + Q) + R = -R + R = \infty.$$

Also, $Q + R = -P$ so

$$P + (Q + R) = P + -P = \infty.$$

Thus,

$$(P + Q) + R = -R + R = \infty = P + (Q + R).$$

Lemma 2.11. *Let P_1, P_2 be the points on an elliptic curve. Then $(P_1 + P_2) - P_2 = P_1$ and $-(P_1 + P_2) + P_2 = -P_1$.*

Proof. The two relations are refections of each other, so we just need to show the second one. The line L through P_1 and P_2 intersects the elliptic curve E at $P_3' = -(P_1 + P_2)$. So $L \cap E = \{P_1, P_2, -(P_1 + P_2)\}$. Then regarding L as the line through $-(P_1 + P_2)$ and P_2 yields

$$-(P_1 + P_2) + P_2 = -P_1.$$

□

If $P, Q, Q + R$ are collinear,

$$P + (Q + R) = -Q$$

and

$$P + Q = -(Q + R)$$

so

$$(P + Q) + R = -(Q + R) + R = -Q$$

by Lemma 2.11.

Suppose $\ell_i = m_j$ for some i, j. We consider the various cases. By above, we can assume that all points in the table of intersections are finite, except for ∞ and possibly x. Note that each ℓ_i and each m_j meets E in three points (counting multiplicity), one of which is P_{ij}. If the two lines coincide, then the other two points must coincide in some order.
1. $\ell_1 = m_1$: Then P, Q, R are collinear, and associativity follows from the calculations above.
2. $\ell_1 = m_2$; In this case, P, Q, ∞ are collinear, so $P + Q = \infty$; associativity follows from the calculations made in the discussion of ∞.
3. $\ell_2 = m_1$: Similar to the previous case.
4. $\ell_1 = m_3$: Then $P, Q, Q + R$ are collinear; associativity was proved above.
5. $\ell_3 = m_1$: Similar to the previous case.
6. $\ell_2 = m_2$: Then $Q + R = \pm(P + Q)$.
If $P + Q = Q + R$,

$$P = (P + Q) - Q = (Q + R) - Q = (R + Q) - Q = R$$

by Lemma 2.11. Therefore

$$(P + Q) + R = R + (P + Q) = P + (P + Q) = P + (R + Q) = P + (Q + R)$$

by commutativity.
If $P + Q = -(Q + R)$,

$$(P + Q) + R = -(Q + R) + R = -Q$$

and

$$P + (Q + R) = P - (P + Q) = -(Q + P) + P = -Q$$

Thus,

$$(P + Q) + R = -Q = P + (Q + R).$$

7. $\ell_2 = m_3$: The line m_3 through P and $(Q + R)$ intersects E in ∞, so

$$P + (Q + R) = \infty \implies P = -(Q + R).$$

But $-(Q + R) = P, Q, R$ are collinear, so associativity holds.
8. $\ell_3 = m_2$: Similar to the previous case.
9. $\ell_3 = m_3$: Since a line can not intersect E in more than three points (by Bezout's Theorem), either: $P = R, P + Q = Q + R, R + Q + R, P = P + Q$.
If $Q + R = P + Q$, then

$$R = (R + Q) - Q = (P + Q) - Q = P$$

by Lemma 2.11 so $R = P$.
If $P = R$, see case 6.
If $P = P + Q$, then

$$\infty = P - P = (P + Q) - P = Q \implies Q = \infty$$

so associativity holds by above calculations.
The case where $Q + R = R$ is similar.

If $\ell_i \neq m_j$ for all i, j, then the hypotheses of the theorem are satisfied, so the addition is associative, as proved above. □

The Discrete Log problem

Let p be a prime, and a, b be integers $\neq 0 \mod p$. Also suppose we know there exists k such that $a^k = b \mod p$. The classic discrete log problem is to find k. This can be generalized to any group G. Let $a, b \in G$, and suppose we know there exists k such that $a^k = b$. The discrete log problem is to find k. In particular, we can consider $E(F_q)$ for some elliptic curve. Here the discrete log problem is given a, b points on E, find $k \in \mathbb{Z}$ such that $ka = b$. ka means adding the point a to itself k times.

Much of cryptography is based on the discrete log problem, and how difficult it can be to solve. There are methods for solving the discrete log problem for some elliptic curves, however, there is no known general solution. The following link contains a list of "bad" types of curves (curves where the discrete log problem is easily solved): `http://en.wikipedia.org/wiki/Elliptic_curve_cryptography#Implementation_considerations`

References: Elliptic Curves: Number Theory and Cryptography by Lawrence C. Washington