23MAC260 Elliptic Curves: Week 2

Last updated February 8, 2024

1 Adding Points on Elliptic Curves

Last week we defined elliptic curves: they are curves of the form

$$C = \left\{[X, Y, Z] \in \mathbb{P}^2 \mid Y^2Z - G(X, Z) = 0\right\}$$

where $G(X, Z)$ is homogeneous of degree 3 and its dehomogenisation $G_d(x)$ has 3 distinct roots.

This week we'll see how to **add together** points on an elliptic curve C.

We start with the following lemma.

Lemma 1.1 (Weak Bézout Theorem). *Let $C \subset \mathbb{P}^2$ be a curve of the form*

$$C = \left\{[X, Y, Z] \in \mathbb{P}^2 \mid F(X, Y, Z) = 0\right\}$$

where F is an irreducible cubic polynomial. Let L be any line in $\mathbb{P}^2$. Then $C \cap L$ consists of 3 points, counted with multiplicity.

Here "counted with multiplicity" means that if C and L intersect tangentially at a point p, then p counts as two intersections; if L is the tangent line to C at an inflection point p, then p counts as 3 intersections.

Proof. A line in $\mathbb{P}^2$ is defined by a homogeneous linear equation

$$aX + bY + cZ = 0$$

where a, b, c are constants, not all 0. Suppose without loss of generality $c \neq 0$: then we can solve for Z to get

$$Z = \frac{aX + bY}{c}.$$

Substituting this into F gives a homogeneous cubic $\widetilde{F}(X, Y)$ of degree 3. Intersection points in $C \cap L$ then correspond to zeroes of $\widetilde{F}$.

Dividing out the highest possible power of Y from $\widetilde{F}$, we can write it as

$$\widetilde{F}(X, Y) = Y^k G(X, Y)$$

where $k \in \{0, 1, 2, 3\}$ and the polynomial $G(X, Y)$ has degee $3-k$ and is not divisible by Y. Roots of G then correspond to roots of its dehomogenisation $G_d(x)$. Since we are working over $\mathbb{C}$, this polynomial has $3-k$ roots counted with multiplicity, so $\widetilde{F}$ has 3 roots counted with multiplcity. $\square$

Now let's see how to add points.

Notation: Let C denote an elliptic curve.

(a) In Week 1 we saw that the point $[0, 1, 0] \in \mathbb{P}^2$ always lies on C. We denote this point by O.

(b) Let P and Q be two points on C. Let $\overline{PQ}$ denote:

- the line joining P to Q, if $P \neq Q$;
- the tangent line to C at P, if $P = Q$.

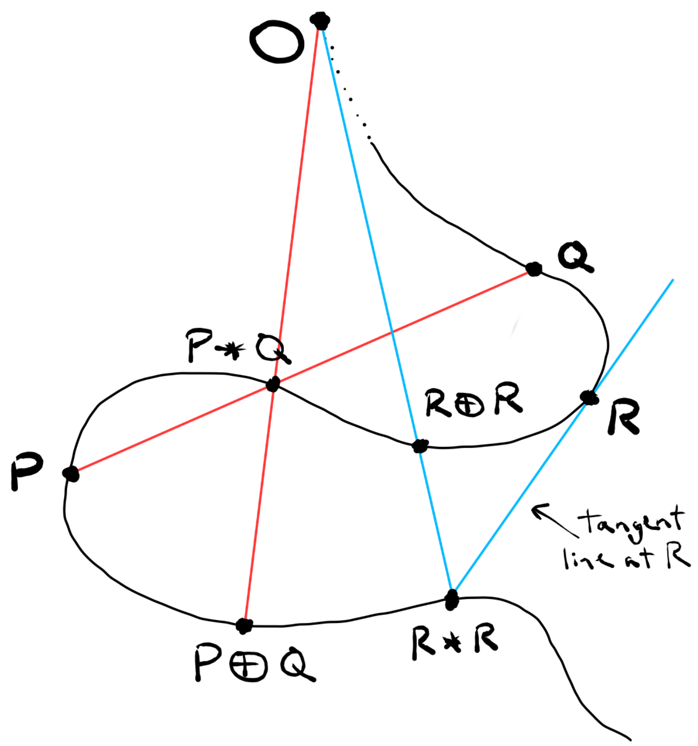
Then $P * Q$ denotes the third point of intersection of $\overline{PQ}$ with C.

Note that Lemma 1.1 guarantees that $\overline{PQ}$ always intersects C in 3 points (counted with multiplcity).

Definition 1.2 (Elliptic Curve Addition)**.** *Let C be an elliptic curve. We define an operation $\oplus$ called* **addition** *on C by*

$$P \oplus Q = O * (P * Q)$$

Picture:



The key point (of this whole module!) is that the operation we just defined makes the elliptic curve C into an **abelian group**. Let's see what that means in more detail.

Theorem 1.3. *The operation $\oplus$ has the following properties:*

1. *$\oplus$ is associative:*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$$

   for all points $P, Q, R \in C$.

2. *For all points $P \in C$ we have*

$$O \oplus P = P \oplus O = P.$$

   In other words, O is the identity element for $\oplus$.

3. *For all points $P \in C$ we have*

$$(O * P) \oplus P = P \oplus (O * P) = O$$

   In other words, $O * P$ is the inverse of P.

4. *For all points $P, Q \in C$ we have*

$$P \oplus Q = Q \oplus P.$$

Proof.

1. This is the hardest part to prove; we will delay the proof until the next lecture.

2. By definition $O \oplus P = O * (O * P)$. Suppose the line $\overline{OP}$ intersects C in a third point Q, so that $O * P = Q$. Then $\{O, P, Q\}$ all lie on a line. So $O * Q = P$. Hence

$$\begin{aligned} O \oplus P &= O * (O * P) \\ &= O * Q \\ &= P. \end{aligned}$$

   Using Statement 4, we also get $P \oplus O = P$.

3. We want to prove that

$$(O * P) \oplus P = O.$$

   Again, say that $O * P = Q$, so $\{O, P, Q\}$ lie on a line.Then

$$\begin{aligned} (O * P) \oplus P &= Q \oplus P \\ &= O * (Q * P) \end{aligned} \tag{†}$$

   But $Q * P = O$, again because the 3 points lie on a line. So $(\dagger) = O * O$.

Now recall that O is an **inflection point** on C: that means that the tangent line to C at O intersects C with multiplicity 3 at O. Therefore $O * O = O$, and so

$$\begin{aligned}(O * P) \oplus P &= O * O \\ &= O.\end{aligned}$$

Again using Statement 4 we get $P \oplus (O * P) = P$ also.

4. To prove that $P \oplus Q = Q \oplus P$, it is enough to prove that $P * Q = Q * P$. But the definition of $P * Q$ only uses the line $\overline{PQ}$, which is unchanged if we swap P and Q.

□

2 Examples of point addition

Let's add some points on the curve C given by

$$Y^2 Z = X^3 + Z^3$$

First note that this indeed an elliptic curve: here we have $G(X, Z) = X^3 + Z^3$, so $G_d(x) = x^3 + 1$ which has 3 distinct roots in $\mathbb{C}$ (check!).

To carry out computation, it is convenient to work in the affine plane. As we have seen, the part of C in the affine plane is defined by the dehomogenised equation

$$y^2 = x^3 + 1. \tag{1}$$

This curve contains the two points

$$P = (2, 3) \quad \text{and} \quad Q = (-1, 0).$$

Let's compute their sum $P \oplus Q$.

- The first step is to find the line $\overline{PQ}$. This has equation

$$\begin{aligned} y &= mx + c \quad \text{where} \\ m &= \frac{3 - 0}{2 - (-1)} \\ &= 1 \end{aligned}$$

  So the line is $y = x + c$. Plugging in for example the coordinates of P, we find $3 = 2 + c$, so $c = 1$. So the equation of the line $\overline{PQ}$ is

$$\overline{PQ} : \ y = x + 1. \tag{2}$$

- The next step is to find $P * Q$: by definitiion it is the third point of intersection of the line $\overline{PQ}$ with the curve C. To find this, subsitute 2 into the curve equation 1: this gives

$$\begin{aligned} (x + 1)^2 &= x^3 + 1 \\ \Leftrightarrow x^3 - x^2 - 2x &= 0. \end{aligned}$$

We know 2 solutions of this equation already, coming from the points P and Q: namely, $x = 2$ and $x = -1$. The third solution is $x = 0$, and this is the x-coordinate of the point $P * Q$.

Substituting $x = 0$ into 2 gives $y = 1$, and so we have found

$$P * Q = (0, 1).$$

- The final step is to go from $P * Q$ to $P \oplus Q$. To do this, we need to find the line joining $P * Q$ to the point $O = [0, 1, 0]$.

  On Problem Sheet 1, you proved that every line in $\mathbb{P}^2$ that passes through $O = [0, 1, 0]$ is given by an equation of the form $aX + bZ = 0$. Dehomogenising, this gives an equation

  $$x = -\frac{b}{a}$$

  which is the equation of a vertical line in the xy-plane. If this line passes through the point $P * Q = (0, 1)$, it must be the line $x = 0$. Putting $x = 0$ in our curve equation (1) we get

  $$\begin{aligned} y^2 &= 1 \\ \Leftrightarrow y &= \pm 1. \end{aligned}$$

  The solution $y = 1$ gives us the point $(0, 1) = P * Q$. So the point we want corresponds to the other solution:

  $$\begin{aligned} P \oplus Q &= O * (P * Q) \\ &= (0, -1). \end{aligned}$$

Remark: In this example we saw that $P * Q$ and $P \oplus Q$ were related by changing the sign of the y-coordinate:

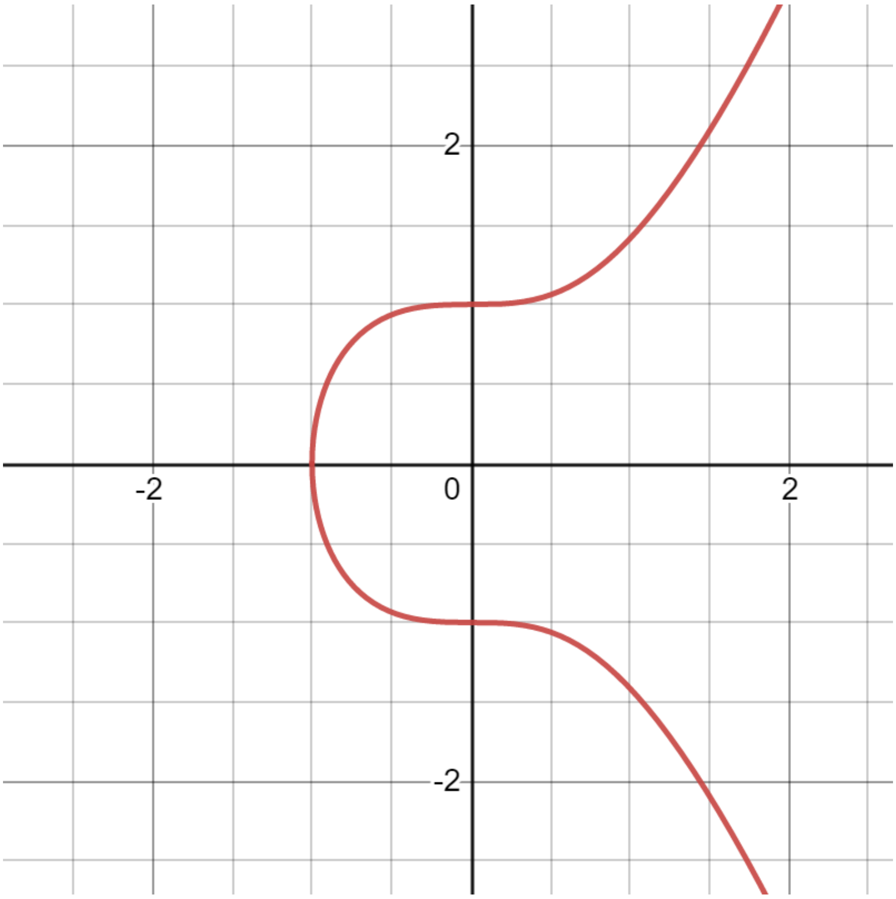
$$\begin{aligned} P * Q &= (0, 1) \\ P \oplus Q &= (0, -1). \end{aligned}$$

This is not an accident: in general for a point $S = (x, y)$ on an elliptic curve C, we have

$$O * S = (x, -y)$$

since the line through (x, y) and $(x, -y)$ passes through O.

The graph below shows the curve C. You can fill the points P, Q, the line $\overline{PQ}$, and the points $P * Q$, $P \oplus Q$ and see that the picture agrees with our calculations.



Question: What is $P \oplus P$? To compute this, we need to find the **tangent** line to C at P. The slope of this line is given by the derivative

$$\left(\frac{dy}{dx}\right)_P$$

You will use this to find $P \oplus P$ on Problem Sheet 2.

3 Associativity of point addition (Non-examinable)

Now we come back to Part 1 of Theorem 1.3:

Theorem 3.1. *For an elliptic curve C, the addition operation $\oplus$ on C is associative: in other words*

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$$

for all points P, Q, R in C.

The proof is based on the following:

Proposition 3.2. *Let C be an irreducible cubic curve in $\mathbb{P}^2$: in other words $C = V(F)$ where F is an irreducible homogeneous polynomial of degree 3. Let C_1 be another cubic curve, and say*

$$C \cap C_1 = \{p_1, \dots, p_9\}.$$

Then for any other cubic curve C_2 passing through $p_1, \dots, p_8$, the curve C_2 must pass through p_9 also.

The proof of the Proposition is based on Bézout's theorem; it is a (non-examinable) question on Problem Sheet 2.

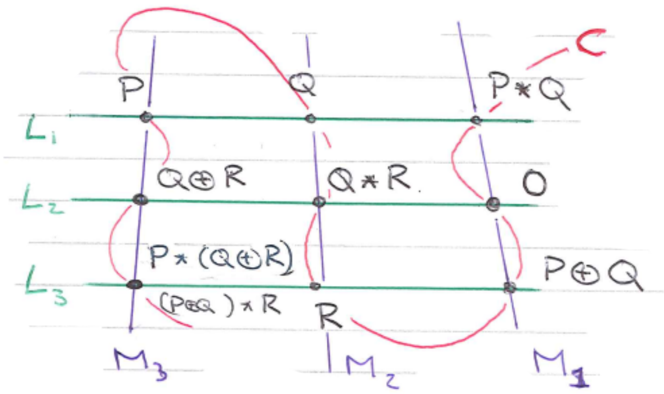
Sketch proof of Theorem 3.1. To prove the claim, it is enough to prove the identity

$$(P \oplus Q) * R = P * (Q \oplus R).$$

We define lines

$$\begin{aligned} L_1 &= \overline{PQ} \\ L_2 &= \overline{O(Q * R)} \\ L_3 &= \overline{(P \oplus Q)R} \\ M_1 &= \overline{O(P * Q)} \\ M_2 &= \overline{QR} \\ M_3 &= \overline{P(Q \oplus R)} \end{aligned}$$

The arrangement is shown in this picture:



Let $C_1 = L_1 \cup L_2 \cup L_3$. Then C_1 is a cubic curve, and

$$C \cap C_1 = \{P,\ Q,\ P * Q, O,\ Q * R,\ Q \oplus R,\ P \oplus Q,\ R,\ (P \oplus Q) * R\}.$$

Let $C_2 = M_1 \cup M_2 \cup M_3$. Then C_2 is a cubic curve, and

$$C \cap C_2 = \{O,\ P * Q,\ P \oplus Q, Q,\ R,\ Q * R,\ P,\ Q \oplus R,\ P * (Q \oplus R)\}.$$

(For these equalities, we are using the fact that C is irreducible, so by Bézout's theorem it intersects each of C_1 and C_2 in exactly 9 points.)

We will complete the proof in the "generic" case that all the points

$$O,\ P,\ Q,\ R,\ P * Q,\ Q * R,\ P \oplus Q,\ Q \oplus R$$

are distinct. The full proof must also consider special cases where at least two of the points are equal.

In this "generic" case, the two sets $C \cap C_1$ and $C \cap C_2$ share 8 points. Proposition 3.2 then implies that in fact the two sets must be equal. So we have

$$(P \oplus Q) * R = P * (Q \oplus R).$$

$\square$