MATH 115: NOTES ON CURVE THEORY 4

MARTIN OLSSON

1. Elliptic curves

Having an essentially complete description of conics in $\mathbb{P}^2(k)$ we now turn to elliptic curves. Throughout we assume that $6 \neq 0$ in k. The theory can be developed without this assumption but it makes some of the calculations easier.

For this class, an *elliptic curve* is a subset $E \subset \mathbb{P}^2(k)$ given by an equation

$$Y^2Z = X^3 - AXZ^2 - BZ^3,$$

with

$$\Delta = 16(4A^3 - 27B^2) \neq 0.$$

Recall that this implies that E is nonsingular at every point. We also calculated earlier that there is only one point at infinity of E given by

$$O = [0 : 1 : 0].$$

Consider a line $L \subset \mathbb{P}^2(k)$ and its intersection $L \cap E$. We define the *multiplicity* of a point $P \in L \cap E$ as follows. This is a rather ad hoc definition but will suit our purposes.

If L is the line at infinity then we have already seen that $E \cap L$ consists of the single point O. In this case we define the multiplicity of O in $E \cap L$ as 3.

If L a line of the form

$$X = \alpha Z$$

then $E \cap L$ consists of O and solutions to the equation

$$y^2 = \alpha^3 - A\alpha - B.$$

This has either two solutions or no solutions, unless

$$\alpha^3 - A\alpha - B = 0$$

in which case there is one solution. In the former case we say that each point of the intersection has multiplicity 1. In the later case we say that the multiplicity of O is 1 and the multiplicity of $[\alpha : 0 : 1]$ is 2. Note that in this last case L is the tangent line at the point $[\alpha : 0 : 1]$. Indeed in general at a point $[\alpha : \beta : 1]$ the tangent line is given by the equation

$$(-3\alpha^2 + A)X + 2\beta Y + (\beta^2 + 2A\alpha + 3B)Z = 0,$$

which for the point $[\alpha : 0 : 1]$ reduces to

$$(-3\alpha^2 + A)X + (2A\alpha + 3B)Z = 0,$$

We therefore must show that

$$\alpha = (2A\alpha + 3B)/(3\alpha^2 - A),$$

which follows by noting that

$$\alpha(3\alpha^2 - A) = 3\alpha^3 - A\alpha = 3A\alpha + 3B - A\alpha = 2A\alpha + 3B.$$

Finally let us consider a line L of the form

$$Y = mX + bZ,$$

with $m \neq 0$. Note that this does not contain O so the intersection $E \cap L$ is given by solutions to the equation

$$(mx + b)^2 = x^3 - Ax - B. \tag{1.0.1}$$

If $[\alpha : \beta : 1]$ is a point of the intersection then the multiplicity of this point is defined to be the multiplicity of the $(x - \alpha)$-factor in the cubic polynomial 1.0.1.

Exercise: Show that if the multiplicity of a point P in $L \cap E$ is ≥ 2, then L is the tangent line to E at P.

In addition to giving the definition of the multiplicity of a point in $L \cap E$, this also gives the following result:

Proposition 1.1. *Let L be a line in $\mathbb{P}^2(k)$. Let N be the sum of the multiplicities of the points in $E \cap L$. Then if $N \geq 2$ then $N = 3$.*

In particular, if $L \subset \mathbb{P}^2(k)$ is a line such either $L \cap E$ contains two points or L is a tangent line to E, then we write

$$L \cap E = \{P, Q, R\},$$

where $P, Q, R \in E$ are points some of which may be equal.

2. The group law of an elliptic curve

Let $E \subset \mathbb{P}^2(k)$ be an elliptic curve as in the preceding section. We define a map

$$+ : E \times E \to E$$

by sending (P, Q) to the point $P + Q$ define as follows:

(1) Let L_{PQ} be the line through P and Q (the tangent line if $P = Q$), and let R be the third point of intersection.

(2) Consider the line L_{OR} between R and O (the tangent line to O if $O = R$), and let $P + Q$ be the third point of intersection of $L_{OR} \cap E$.

Proposition 2.1. *The operation $+$ makes E an abelian group.*

Proof. We won't give a formal proof here, though geometrically the axioms follow immediately. □

In the case when $k = \mathbb{Q}$, which we assume for the remainder of this lecture, there are three main results which gives us a handle on the group E.

Theorem 3 (Mordell)**.** *The group E is finitely generated.*

For us the main consequence of this is that

$$E = E_{\text{tors}} \times \mathbb{Z}^r,$$

where

$$E_{\text{tors}} = \{P \in E | \text{there exists } n > 0 \text{ such that } nP = 0\}$$

and this group is finite. The number r is also an invariant of E and is called the *rank*. This structure of E follows from Mordell's theorem and the structure theorem for finitely generated abelian groups (which if you haven't seen before you will learn in 113).

The second very deep theorem is the following:

Theorem 4 (Mazur). *The group E_{tors} is either*

$$\mathbb{Z}/(m), \quad 1 \leq m \leq 10, \textit{ or } m = 12,$$

or

$$\mathbb{Z}/(2) \times \mathbb{Z}/(m), m = 2, 4, 6, 8.$$

Finally we have the following very restrictive structure of the torsion points:

Theorem 5 (Lutz-Nagell). *Suppose A and B are integers. If $[a : b : 1] \in E_{\text{tors}}$ is a torsion point, then a and b are integers, and either $b = 0$ or $b^2 | \Delta$.*

Example 5.1. We can use the above theorems to compute E_{tors} for the elliptic curve

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

This curve has discriminant

$$\Delta = 16(4 \cdot 125 - 27 \cdot 16) = 2^6 \cdot 17.$$

Therefore if $[a : b : 1]$ is a torsion point, we must have

$$b = 0, 1, 2, 4, \text{or } 8.$$

Now the case $b = 0$ clearly occurs with the point $[1 : 0 : 1]$. Let $f(x)$ denote the function $x^3 - 5x + 4$. This function has derivative $3x^2 - 5$ which is positive for $|x| \geq 2$. Also we have

$$f(-3) = -27 + 15 + 4 = -8, \quad f(5) = 125 - 25 + 4 = 104.$$

Combining these two statements we see that the only possible integer values for x for which $f(x)$ is between 0 and 64 is

$$x = -2, -1, 0, 1, 2, 3, 4.$$

Computing each of these values we find that the only possible torsion points are

$$[0 : \pm 2 : 1], \quad [3 : \pm 4 : 1], O, [1 : 0 : 1].$$

Also one computes that

$$[0 : 2 : 1] + [1 : 0 : 1] = [3 : 4 : 1].$$

However, if you compute

$$[0 : 2 : 1] + [0 : 2 : 1]$$

then you find that the x-coordinate is 25/4. Since this is not an integer, then by the Lutz-Nagell theorem $[0 : 2 : 1]$ is not a torsion point, and therefore $[3 : 4 : 1]$ is not a torsion point either.

This implies that

$$E_{\mathrm{tors}} = \{O, [1 : 0 : 1]\} \simeq \mathbb{Z}/(2).$$

This also shows that the rank of E is ≥ 1. It can in fact be shown that the rank equals 1 in this case.