DAY 4 SUPPLEMENT: THE ADDITION LEMMA

CURVES THAT CLASSIFY GEOMETRY PROBLEMS J-LO MC2022

This is a series of exercises that rigorously proves the addition lemma. Recall that $\mathrm{ord}_p(r)$ is defined by the property that we can write $r = \frac{m}{n} p^{\mathrm{ord}_p(r)}$ with m, n relatively prime to p (and $\mathrm{ord}_p(0) = \infty$). We defined $E(p)$ to be the set of rational points of E such that at least one of the coordinates has denominator divisible by p, as well as the point O. For $P \in E(p)$, we defined

$$t(P) = \begin{cases} \frac{x}{y} & \text{if } P = (x, y), \\ 0 & \text{if } P = O. \end{cases}$$

Lemma 1 (Addition Lemma). *Let $P, Q \in E(p)$, and suppose that $t(P)$ and $t(Q)$ both have p-adic valuation greater than or equal to n for some integer $n > 0$. Then $P + Q$ is also in $E(p)$, and*

$$\mathrm{ord}_p(t(P) + t(Q) - t(P + Q)) \geq 3n.$$

Let's first get the relatively easy cases out of the way.

(1) Prove the lemma is true if any of P, Q, or $P + Q$ is equal to O.

So from now on we can assume that the line through P and Q is not vertical.

Copying the cuspidal cubic construction

Suppose the line $y = mx + v$ intersects the elliptic curve $y^2 = x^3 + ax^2 + bx + c$ at $P = (x_1, y_1)$, $Q = (x_2, y_2)$, and $P \star Q = (x_3, y_3)$. Define new variables

$$t = \frac{x}{y} \qquad \text{and} \qquad s = \frac{1}{y}.$$

So for example, the point P can now be written in t, s coordinates as $(t_1, s_1) = (\frac{x_1}{y_1}, \frac{1}{y_1})$, and we have $t_1 = t(P)$, $t_2 = t(Q)$, and $t_3 = t(P \star Q)$.

We first consider the case $t_1 \neq t_2$; the case $t_1 = t_2$ is handled in a later section.

(2) Show that (t_1, s_1), (t_2, s_2), and (t_3, s_3) satisfy the equations

$$s = \alpha t + \beta \qquad \text{and} \qquad s = t^3 + at^2 s + bts^2 + cs^3.$$

(What are α and β in terms of m and v? How do we know that $v \neq 0$?)

(3) Plugging the first equation into the second gives a cubic in t, with roots t_1, t_2, t_3. Use this to find an expression for $t_1 + t_2 + t_3$ in terms of a, b, c, α, β.

HOW DIVISIBLE BY p ARE WE?

Recall that $P, Q \in E(p)$, and that t_1 and t_2 have p-adic valuation at least n.

(4) Prove $\text{ord}_p(s_1)$ and $\text{ord}_p(s_2)$ are both at least $3n$. (Hint: Day 3 problem (8))

The next major task is to show that the p-adic valuation of α is large.

(5) Show that $\alpha = \frac{s_2-s_1}{t_2-t_1}$. Why is this not enough to prove $\text{ord}_p(\alpha) \geq 2n$? (We will need to find another expression for α.)

(6) Show that (t_1, s_1) and (t_2, s_2) satisfy the equation

$$s_2 - s_1 = (t_2^3 - t_1^3) + a((t_2^2 - t_1^2)s_2 + t_1^2(s_2 - s_1)) + b((t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)) + c(s_2^3 - s_1^3).$$

(7) Put terms divisible by $t_2 - t_1$ on one side and terms divisible by $s_2 - s_1$ on the other. Use this to obtain a new expression for α, and prove that $\text{ord}_p(\alpha) \geq 2n$.

Finally, we can use the fact that $\text{ord}_p(\alpha) \geq 2n$ to complete this case of the lemma.

(8) Using what you know about s_1, t_1, and α, prove that $\text{ord}_p(\beta) \geq 3n$.

(9) Use the expression you found from problem (3) to prove

$$\text{ord}_p(t_1 + t_2 + t_3) \geq 3n.$$

(10) Prove that $\text{ord}_p(t_3) \geq n$ and hence $\text{ord}_p(s_3) \geq 3n$. Use this to show $P + Q \in E(p)$, and then finish the proof of this case of the lemma.

THE CASE $t(P) = t(Q)$

As before, let $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $P \star Q = (x_3, y_3)$, and use the change of variables $t = \frac{x}{y}$ and $s = \frac{1}{y}$. We have $P, Q \in E(p)$, $t_1 = t_2$, and $\text{ord}_p(t_1) \geq n$. The proof of problem (4) still holds, so $\text{ord}_p(s_1), \text{ord}_p(s_2) \geq 3n$.

(11) Use the fact that $t_1 = t_2$ to show that

$$0 = (at_1^2 - 1)(s_2 - s_1) + bt_1(s_2^2 - s_1^2) + c(s_2^3 - s_1^3).$$

(12) Factor out $s_2 - s_1$ and show the other factor is nonzero. Conclude that $P = Q$.[1]

(13) Compute the tangent line $y = mx + v$ to $y^2 = x^3 + ax^2 + bx + c$ at P. Check that $v \neq 0$, so we can define the line $s = \alpha t + \beta$ as in problem (2).

(14) Prove that $\text{ord}_p(\alpha) \geq 2n$.

(15) Check that the rest of the argument goes through as above and finish proving the lemma.

[1]This implies that the map $t : E(p) \to \mathbb{Q}$ is injective; in other words, there is at most one point in $E(p)$ on each line through the origin.