Lecture 14

Jose Capco (jcapco@risc.jku.at)

Theorem 1. Let $P, Q \in E_n \backslash \{O\}$ and $R \in E$ such that $P + Q + R = O$ then

- $-P \in E_n$
- $R \in E_n$. In particular, $-R = P + Q \in E_n$ and so E_n is a group.
- $p^{5n} \mid t_P + t_Q + t_R$

Proof. The first item is clear because if $P \in E_n \backslash \{O\}$ then $t_{-P} = -t_P$, so $v(t_{-P}) \geq n$.

Clearly if $P + Q = O$ then $R = O \in E_n$, so we assume that $Q \neq -P$. We know that R is the third point in $\overline{PQ} \cap E$ ($\overline{PQ}$ is possibly the tangent line if $P = Q$).

We aim to show that $\overline{PQ}$ is not the 'vertical line' in the ts-plane (aka. U_y) and the slope of this line in U_y has a positive valuation (i.e. $v(\alpha) > 0$). If we do this, then we see that $\overline{PQ} \cap U_y$ can be represented by $s = \alpha t + \beta$ for some $\alpha, \beta \in \mathbb{Q}$. In this case

$$(\alpha t + \beta) = t^3 + at(\alpha t + \beta)^2 + b(\alpha t + \beta)^3$$

so $R \in U_y$ and (by Vieta) the sum of the zeros of the roots of the above polynomial is

$$t_P + t_Q + t_R = -(3\alpha^2\beta b + 2\alpha\beta a)(1 + a\alpha^2 + \alpha^3 b)^{-1} \qquad (1)$$

Notice that if we show that $v(\alpha) > 0$ then $1 + a\alpha^2 + \alpha^3 b \neq 0$.

We will first show that the line $\overline{PQ}$ is not a vertical line in U_y and that its slope in this chart has a valuation greater than $2n$.

Let us first suppose that $t_P \neq t_Q$, then the line $\overline{PQ}$ in U_y can indeed be written as (i.e. it is not a vertical line) $s = \alpha t + \beta$ for some $\alpha, \beta \in \mathbb{Q}$ and we specifically have

$$\alpha = \frac{s_P - s_Q}{t_P - t_Q}$$

Using the equation $s = t^3 + ats^2 + bs^3$ we get

$$\begin{aligned} s_P - s_Q = t_P^3 - t_Q^3 + a(t_P s_P^2 - t_Q s_Q^2) + b(s_P^3 - s_Q^3) = \\ t_P^3 - t_Q^3 + at_P(s_P^2 - s_Q^2) + as_Q^2(t_P - t_Q) + b(s_P^3 - s_Q^3) \end{aligned}$$

so we can write $A(s_P - s_Q) = B(t_P - t_Q)$ where

$$\begin{aligned} A &:= 1 - at_P(s_P + s_Q) - b(s_P^2 + s_P s_Q + s_Q^2) \\ B &:= (t_P^2 + t_P t_Q + t_Q^2) + as_Q^2 \end{aligned}$$

We can see that $v(A) = 0$ and $v(B) \geq 2n$, thus

$$v(\alpha) = v(B) \geq 2n$$

We want to show that the inequality $v(\alpha) \geq 2n$ also holds when $P = Q$. So suppose $t_P = t_Q$, then the line $\overline{PQ}$ is just the tangent line to P. We will obtain the equation of the line by computing the slope (in U_y) and if the slope is 'infinite' we will know that the line vertical. The slope is computed by implict differentiation of $s^2 = t^3 + ats^2 + bs^3$ with respect to t

$$\frac{ds}{dt} = 3t^2 + as^2 + 2ast\frac{ds}{dt} + 3bs^2\frac{ds}{dt}$$

which yields

$$\alpha = \frac{ds}{dt}(P) = (3t_P^2 + as_P^2)(1 - 2at_Ps_P - 3bs_P^2)^{-1}$$

and the denominator has valuation 0, so we can indeed write this line as $s = \alpha t + \beta$. The valuation of α is the valuation of its numerator which is greater than $2n$ as desired.

This implies that $\beta = s_P - \alpha t_P$ has a non-negative valuation and so by (1) $v(t_R) \geq n$ which implies that E_n is a group.

In fact $v(t_P + t_Q + t_R) \geq 5n$. For this we need to be more precise with $v(\beta)$, namely

$$v(\beta) = v(s_P - \alpha t_P) \geq \min\{v(s_P), v(\alpha) + v(t_P)\} \geq 3n$$

and the rest follows from the fact that $v(\alpha) \geq 2n$ and equation (1). □

Corollary 2. For any $n \in \mathbb{N}$ the map

$$\begin{array}{cccc} \lambda_n : & E_n/E_{5n} & \longrightarrow & (\mathbb{Z}/p^{5n}, +) \\ & & & \\ & [O] & \longmapsto & 0 \\ & [(x,y)] & \longmapsto & x/y \bmod p^{5r} \end{array}$$

is an injective group homomorphism.

Proof. We already know from the above Theorem that E_n is a subgroup of E and $E_m \geq E_n$ if $m \leq n$. Consider the following map[1]

$$\begin{array}{cccc} \tilde{\lambda}_n : & E_n & \longrightarrow & (\mathbb{Z}/p^{5n}, +) \\ & & & \\ & O & \longmapsto & 0 \\ & (x,y) & \longmapsto & x/y \bmod p^{5n} \end{array}$$

Suppose that $P \in E_{5n} \backslash \{O\}$ then $v(t_P) \geq 5n$ implying that

$$t_P \equiv 0 \bmod p^{5n}$$

So by definition $E_{5n} = \tilde{\lambda}_n^{-1}(0)$. We just need to see that λ_n is a group homomorphism, but this follows immediately from the third item of the above theorem, namely for $P, Q \in E_n \backslash \{O\}$ we have: if $Q \neq -P$ then

$$t_P + t_Q \equiv t_{P+Q} \bmod p^{5n}$$

otherwise $t_{-P} = -t_P$ so $t_P + t_{-P} = 0$. □

The following Lemma will prove Nagell-Lutz and its Corollary from last lecture (recall we left E_1 is torsion-free in the partial proof of the Corollary)

Lemma 3. Recall that we assume $E/\mathbb{Q}$ to be an elliptic curve defined by an integral short Weirstrass equation, we then have:

1. E_1 is torsion-free i.e. $\mathrm{Tor}(E) \cap E_1 = \{O\}$ (E_n defined for any prime $p \neq 2, 3$)
2. If $P \in \mathrm{Tor}(E) \backslash \{O\}$ then $x_P, y_P \in \mathbb{Z}$
3. If $P \in \mathrm{Tor}(E) \backslash \{O\}$ then either $y_P = 0$ or $y_P^2 \mid \Delta$

Proof.

[1] notice we abused notation here, x/y (for $(x, y) \in E_n$) can be expressed as a fraction x'/y' whose denominator is not divisibly by p, and so this is just $(x' \bmod p^{5n})(y' \bmod p^{5n})^{-1}$

1. Now, if $P \in E_1 \cap \mathrm{Tor}(E)$ and $P \neq O$ (we are proving by contradiction) then there is an $m > 1$ such that $mP = O$ but $(m-1)P \neq O$ (i.e. $\mathrm{ord}(P) = m$). First we claim that $\gcd(m, p) = 1$. Suppose, by contradiction, that $p \nmid m$. Since $P \in E_1$ there an $n \in \mathbb{N}$ such that $P \in E_n \backslash E_{n+1}$ (i.e. $v(t_P) = n$). Then, by the above corollary, $p^{5n} \mid mt_P$. But, the only torsion points in $\mathbb{Z}/p^{5n}$ are divisible by p and so $p \mid m$.

Write $m = pq$ for some $q \geq 1$, then $qP \neq O$ and has order p and because E_1 is a group we know that $qP \in E_1$. Denote $Q := qP$ and suppose now that $Q \in E_n \backslash E_{n+1}$ for some $n \in \mathbb{N}$ (we are re-assigning n). Then $p^{5n} \mid pt_Q$ or simply $p^{5n-1} \mid t_Q$. The final contradiction comes from the fact that $5n - 1 > n + 1$ (for $n \geq 1$) so $Q \in E_{n+1}$.

2. If, by contradiction, either x_P or y_P is not an integer then there exists a prime number p such that $v_p(x_P) < 0$ i.e. $v_p(t_P) > 0$. Hence, for that p, $P \in E_1$ (remember the definition of E_1 depends on the elliptic curve E defined by an integral short Weierstrass equation and the prime number p). But P is a torsion point and E_1 is torsion-free and this gives us the contradiction.

3. We know that, given the condition for E, $y_P = 0$ iff P is a 2-torsion point. So we assume P and $2P$ are not O, both being torsion points. By the previous result we know that $x_P, y_P, x_{2P}, y_{2P} \in \mathbb{Z}$. Let $f(x) = x^3 + ax + b$, so the elliptic curve is defined by $y^2 = f(x)$. One checks the following identity (Bézout identity for discriminant)

$$4a^3 + 27b^2 = -27(x^2 + ax - b)f(x) + (3x^2 + 4a)f'(x)^2$$

So it suffices to show that $y_P \mid f'(x_P)$ (since we already know that $y_P^2 \mid f(x_P)$. We recall the duplication formula:

$$x_{2P} = \left(\frac{f'(x_P)}{2y_P}\right)^2 - 2x_P$$

and since we know from the previous result that x_{2P}, y_P are integers, we conclude that $y_P \mid f'(x_P)$.

□

So now we know that the torsion subgroup of an elliptic curve over $\mathbb{Q}$ is finite. But one can say even more. Barry Mazur proved in a paper in 1977 that the torsion subgroup of an elliptic curve $E/\mathbb{Q}$ can have at most 16 points, specifically we have the following theorem:

Mazur Theorem. Let E be an elliptic curve over $\mathbb{Q}$ then $\mathrm{Tor}(E)$ is either

- Cyclic and isomorphic to $\mathbb{Z}/n$ for some natural number $1 \leq n \leq 12$ with $n \neq 11$
- or isomorphic to $\mathbb{Z}/2n \oplus \mathbb{Z}/2$ for some natural number $1 \leq n \leq 4$.

The theorem is very easy to understand but cannot be proven in this course and has a rather deep proof. The proof uses a mathematical tool called *deformation theory*, more specifically *deformation of Galois representations* and for this you will need many things in algebraic and arithmetic geometry and deeper theories about elliptic curves.

Now that we know many things about the torsion subgroup of elliptic curves over $\mathbb{Q}$, we would like to know more about the non-torsion points. The fact is that, people already knew that the torsion subgroups of $E/\mathbb{Q}$ are finite even before the Nagell-Lutz theorem. This was known already in the 1920's while the theorem was proven in 1930's. The reason is because of a rather strong theorem that was first conjectured in 1901 by Poncaire: Elliptic curves over $\mathbb{Q}$ are finitely generated abelian groups. The proof of this conjecture was accomplished by the American mathematician Louis Mordell.

Mordell-Weil Theorem. Elliptic curves over $\mathbb{Q}$ are finitely generated as groups.

For the proof of this we will need at least two session. But since we do not have this time we may just give some idea of the proof in the next sesion[2]

[2] its rigorous proof requires some algebraic number theory.