Lecture 13

Jose Capco (jcapco@risc.jku.at)

We have inadvertently used a notation, that we will make formal

Notation. Let E be an elliptic curve and $P \in E\backslash\{O\}$ then we often write it's coordinates x_P and y_P i.e. $P = (x_P, y_P)$.

Let us recall/restate Nagell-Lutz Theorem

Nagell-Lutz Theorem. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ defined in such a way that $a, b \in \mathbb{Z}$ and suppose $\Delta := 4a^3 + 27b^2$ is its discriminant. The non-trivial torsion points of E are points $P \in \mathbb{A}^2(\mathbb{Q})$ ($P = (x_P, y_P)$) satisfying

1. $x_P, y_P \in \mathbb{Z}$
2. If $y_P \neq 0$ then $y_P^2 \mid \Delta$

The Nagell-Lutz algorithm suggest that for such elliptic curves (i.e. over $\mathbb{Q}$ and defined by an integral short Weierstrass equation) the torsion subgroup is finite. It also yields an easy algorithm to determine the (finite) torsion points of an elliptic curve defined by an integral short Weierstrass equation. We will call this algorithm the *Nagell-Lutz algorithm*:

Algorithm 1: Finding torsion subgroup of $E(\mathbb{Q})$

Input: $E(\mathbb{Q}) : y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$ with $4a^3 + 27b^2 \neq 0$
Output: $\mathrm{Tor}(E)$

```
compute discriminant Δ := 4a^3 + 27b^2
find all d_1, ..., d_k ∈ ℕ such that d_i^2 | Δ
set D := {0, ±d_1, ..., ±d_k}
find all points P_1, ..., P_n ∈ E\{O} such that their y-coordinates are in D
set S := {P_1, ..., P_n}
foreach P in S do
    for j in 2, ..., #S do
        set Q := jP
        if Q = O then break the j-loop
        if Q ∉ S then
            set S := S\{Q}
            break the j-loop
        end
    end
end
return S
```

Here is another example using Nagell-Lutz Theorem (which we have not yet proven) to show that we can find an elliptic curve $E/\mathbb{Q}$ such that E has infinite points

Example 1. Let $E : y^2 = x^3 + ax + 1$ be an elliptic curve over $\mathbb{Q}$ with $a \in 2\mathbb{Z} + 1$. One point of this elliptic curve is $P = (0, 1)$. We claim that P is not a torsion point. Otherwise, $2P$ is a torsion point. We know that $2P$ is not a 2-torsion point because the y-coordinate of P is not 0. So we compute $2P$:

$$x_{2P} = \mu^2 - 2x_P = \mu^2 \qquad \mu = \frac{3x_P^2 + a}{2y_P}$$

since $x_P = 0, y_P = 1$ we get $x_{2P} = \left(\frac{a}{2}\right)^2$. By Nagell-Lutz Theorem $x_{2P} \in \mathbb{Z}$ so $a \in 2\mathbb{Z}$ which is a contradiction. Thus, P is not a torsion point and so E has infinite number of points.

To prove the Nagell-Lutz we will often make use of p-adic valuations of elements in $\mathbb{Q}$ ...

Notation and Definition. Let $p \in \mathbb{N}$ be a prime number then we (have already seen) know for any $n \in \mathbb{Z}$ $v_p(n) \in \mathbb{N}_0$ is the non-negative number such that $p^{v_p(n)} \mid\mid n$. We can also take v_p of any $q \in \mathbb{Q}^*$ by extending the domain of definition namely

$$v_p : \mathbb{Q}^* \to \mathbb{Z} \qquad v_p(a/b) := v_p(a) - v_p(b) \, (a, b \in \mathbb{Z} \backslash \{0\})$$

Often it is useful to extend this to 0 by defining an additional point ∞ (greater than any integer) in the codomain $v_p(0) = \infty$ so we simply get the map $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$.

We call this map the *p-adic valuation* and this has the property

- $v_p(q_1 q_2) = v_p(q_1) + v_p(q_2)$
- $v_p(q_1 + q_2) \geq \min\{v_p(q_1), v_p(q_2)\}$ and equality if[1] $v_p(q_1) \neq v_p(q_2)$

If the context is clear sometimes we drop the subscript p. We also often abuse notation and write $p^k \mid\mid q$ if $v_p(q) = k$, or $p^k \mid q$ if $v_p(q) \geq k$. If $q \in \mathbb{Q}$ and $v_p(q) \geq 0$, then we also abuse $\mod p$ notation. Namely, if we write $q = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ such that $\gcd(a, b) = 1$, then $b \bmod p \neq 0$ in $\mathbb{F}_p$ and we defined

$$q \bmod p := (a \bmod p)(b \bmod p)^{-1} \in \mathbb{F}_p$$

Before we prove Nagell-Lutz, let us dicuss its consequences:

Corollary 2. Nagell-Lutz Theorem implies

- $E/\mathbb{Q}$ has a finite torsion subgroup
- Suppose $E/\mathbb{Q} : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$ and consider a prime number p such that $p \nmid \Delta_E$. Then we have a *(good) reduction* to an elliptic curve over $\mathbb{F}_p$ i.e. a well-defined map[2] $\rho : E(\mathbb{Q}) \to E(\mathbb{F}_p)$

$$\rho : \begin{array}{ccl} O & \longmapsto & O \\ P & \longmapsto & \begin{cases} (x_P \bmod p, y_P \bmod p) & \text{if } v_p(x_P) \geq 0 \text{ and } v_p(y_P) \geq 0 \\ O & \text{otherwise} \end{cases} \end{array}$$

is a group homomorphism and a monomorphism (i.e. injective) if restricted to $\mathrm{Tor}(E(\mathbb{Q}))$. Hence $\#\,\mathrm{Tor}(E(\mathbb{Q})) \mid \#E(\mathbb{F}_p)$

Partial Proof. The first item is immediate from Nagell-Lutz Theorem: If (x_P, y_P) is a point of an elliptic curve $E/\mathbb{Q}$ then $(c^2 x_P, c^3 y_P)$ is a point of another elliptic curve $E' : y^2 = x^3 + c^4 ax + bc^6$ where $c \in \mathbb{N}$ is the least common multiple of the denominator of a and b respectively (this new elliptic curve has a discriminat which is $c^{12}\Delta_E \neq 0$). This gives an isomorphic isogeny from E to E' namely

$$\begin{array}{ccc} E & \xrightarrow{\sim} & E' \\ O & \longmapsto & O \\ (x_P, y_P) & \longmapsto & (c^2 x_P, c^3 y_P) \end{array}$$

Since E' is an elliptic curve defined by an integral short Weierstrass form, we can apply the Nagell-Lutz theorem and conclude that $\mathrm{Tor}(E')$ and thus $\mathrm{Tor}(E)$ is finite.

For the remainder of the proof, we look at the point of elliptic curves in the projective plane. A point $P \in \mathbb{P}^2(\mathbb{Q})$ can be represented uniquely, up to sign change, by $(x_P : y_P : z_P)$ with $x_P, y_P, z_P \in \mathbb{Z}$ and $\gcd(x_P, y_P, z_P) = 1$. So there is a well-defined *reduction*

$$\mathbb{P}^2(\mathbb{Q}) \to \mathbb{P}^2(\mathbb{F}_p)$$

[1] not 'iff'

[2] here $E(\mathbb{F}_p) = x^3 + (a \bmod p)x + (b \bmod p)$

for any prime number p (bringing each such representation to mod the coordinates). This reduction brings lines in $\mathbb{P}^2(\mathbb{Q})$ to lines in $\mathbb{P}^2(F_p)$ (equation of a projective line is encoded also as a point in $\mathbb{P}^2$). So the map ρ is well-defined and is a group homomorphism, by the way we defined from group addition law of elliptic curves.

To prove the final part of the corollary we need to show that a non-trivial point in the kernel of ρ is not a torsion point of $E(\mathbb{F}_p)$. Suppose that $P = (x_P : y_P : z_P) \in E(\mathbb{Q})\backslash\{O\}$ (so $z_P \neq 0$) be a point in the kernel of ρ such that $x_P, y_P, z_P \in \mathbb{Z}$ and $\gcd(x_P, y_P, z_P) = 1$. So

$$(x_P : y_P : z_P) \equiv (0 : 1 : 0) \bmod p$$

which means that $v(y_P) = 0$ and $v(x_P) > 0$. If we now switch back to the affine points (i.e. points of the form $(x_P/z_P : y_P/z_P : 1)$), we see that the non-trivial points in the kernel are exactly those points $Q \in E$ ($Q = (x_Q : y_Q : 1)$) such that $v_p(x_Q/y_Q) > 0$ (i.e. y_Q cannot be zero in the kernel).

We have shown, we can define the kernel as the subgroup of $E(\mathbb{Q})$

$$E_1 := \{P \in E(\mathbb{Q})\backslash\{O\} \,:\, v(x_P/y_P) \geq 1\} \cup \{O\}$$

We will show in the proof of Nagell-Lutz that E_1 has no non-trivial torsion point and this is a key information in the proof of Nagell-Lutz. □

The above proof suggests that the Nagell-Lutz algorithm above can be easily modified to provide the torsion subgroup of any elliptic curve over $\mathbb{Q}$.

From now on let us fix $E/\mathbb{Q}$ an elliptic curve defined by $y^2 = x^3 + ax + b$ where $a, b \in \mathbb{Z}$ with discriminant $\Delta \in \mathbb{Z}$ and fix a prime number p.

We define a family of sets, indexed by $\mathbb{N}$, that we will show to be groups and satisfy containment in sequence (i.e. a *filtration of groups*)

Notation. Suppose $P \in E$, often we need to go look at it in the projective space $\mathbb{P}^2(\mathbb{Q})$, so this point is $(x_P : y_P : 1)$. If $y_P \neq 0$ then we will sometimes look at E in the affine chart U_y, in this case the point can be represented as

$$\left(\frac{x_P}{y_P} : 1 : \frac{1}{y_P}\right)$$

and it is the point $(t_P, s_P) \in U_y$ where $t_P = \frac{x_P}{y_P}$ and $s_P = \frac{1}{y_P}$ and (t_P, s_P) satisfies

$$s = t^3 + ats^2 + bs^3$$

Definition. For $n \in \mathbb{N}$, define

$$E_n := \{P \in E\backslash\{O\} \,:\, v(x_P/y_P) \geq n\} \cup \{O\}$$

In this definition (we hope it is clear), we require that y_P not be 0.

Clearly we have reverse set containment i.e. $E_n \supset E_{n+1}$ for any $n \in \mathbb{N}$, we will show in particular that E_n are groups (so we actually have a *filtration* of groups) and this will be a tool in proving Nagell-Lutz theorem. To prove Nagell-Lutz we will also need to know the following results which we give as exercise ...

Exercise 1. Show that for any $n \in \mathbb{N}$

$$E_n = \{P \in E\backslash\{O\} \,:\, v(x_P) \leq -2n, v(y_P) \leq -3n\} \cup \{O\}$$

More specifically show that for any point $P \in E\backslash\{O\}$

$$v(x_P) < 0 \Leftrightarrow v(y) < 0$$

and if $v(x_P) < 0$ then there is an $n \in \mathbb{N}$ such that $v(x_P) = -2n$ and $v(y_P) = -3n$.

Lemma 3. Let $P, Q \in E_n \backslash \{O\}$ $(n \in \mathbb{N})$ then $t_P = t_Q$ iff $Q = P$.

Proof. One direction is clear. Suppose the condition $t_P = t_Q$ holds, then we only need to show that $s_P = s_Q$. We have $v(t_P) = v(t_Q) = r$ for some $r \geq 1$ (in fact $r \geq n$), this $p \mid s_P$ and $p \mid s_Q$ (since from the exercise: $v(s_P) = v(s_Q) = 3r$). If we show that for any $k \in \mathbb{N}$ we have

$$s_P = s_Q \bmod p^k$$

then we have also shown that $s_P = s_Q$. We prove by induction, the hypothesis is given for us for free since $r \geq 1$. So let $k \geq 1$ be a number such that $s_P = s_Q \bmod p^k$. Then, since s_P, s_Q are both divisible by p, we know that $s_P^i = s_Q^i \bmod p^{k+1}$ if $i = 2, 3$ and so

$$s_P = t_P^3 + at_P s_P^2 + bs_P^3 \equiv t_Q^3 + at_Q s_Q^2 + bs_Q^3 = s_Q \bmod p^{k+1}$$

□