November 15, we have no class. November 22, we do a SAGE (computer) session in WN-S329.

1. Material covered

(sketch)

These notes are not meant as course notes and are not carefully written. They serve mainly as a summary and/or reminder for what we have done in class.

On November 8, we covered what corresponds to Chapters 11 and 12 of Cassels and Sections II.3-5 and IV.3 of Silverman-Tate.

Throughout, we will assume that we have an elliptic curve E over $\mathbb{Q}$, given by

$$y^2 = x^3 + ax^2 + bx + c,$$

with $a, b, c \in \mathbb{Z}$. We also have a prime p.

- We discussed the p-adic valuation v_p on $\mathbb{Q}$, and the discrete valuation ring $\mathbb{Z}_{(p)}$, which is called R in Silverman-Tate, section II.4. See exercises 2.6-8 of Silverman-Tate and the beginning of chapter 2 in Cassels. Cassels also defines the p-adic numbers Q_p in section chapter 2, but we have not used those.
- We defined the reduction $\tilde{E}$ over $\mathbb{F}_p$ by

  $$y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c},$$

  with $\overline{a}, \overline{b}, \overline{c}$ the images of a, b, c in $\mathbb{F}_p$, and let $\tilde{E}_{\rm ns}(\mathbb{F}_p)$ be the set of nonsingular points over $\mathbb{F}_p$.
- We let $E_0(\mathbb{Q}) \subset E(\mathbb{Q})$ be the set of points of nonsingular reduction, and $E_1(\mathbb{Q})$ the kernel of reduction. Then we have

  $$E_1(\mathbb{Q}) = \{\mathcal{O}\} \cup \{\, (x,y) \in E(\mathbb{Q}) \ : \ v_p(x) < 0 \text{ or } v_p(y) < 0\}.$$

- We proved the following statement: for any affine point (x, y) in $E(\mathbb{Q})$ with $v_p(x) < 0$ or $v(y) < 0$, there is an integer $n > 0$ such that $v_p(x) = -2n$ and $v_p(y) = -3n$.
- We concluded that for every point (x, y) in $E(\mathbb{Q})$ there are integers m, n, e with $\gcd(m, e) = \gcd(n, e) = 1$ and $x = m/e^2$ and $y = n/e^3$.
- We defined

  $$E_n(\mathbb{Q}) = \{\mathcal{O}\} \cup \{\, (x,y) \ : \ v_p(x) \le -2n, \ v_p(y) \le -3n \,\},$$

  which is called $\mathfrak{G}^{(n)}$ in Cassels and $C(p^n)$ in Silverman-Tate.
- Our elliptic curve has a projective model given by

  $$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3,$$

  of which another affine part, with $Y \neq 0$ and coordinates

  $$s = \frac{Z}{Y} = \frac{1}{y} \qquad \text{and} \qquad t = \frac{X}{Y} = \frac{x}{y},$$

  is given by

  $$s = t^3 + at^2s + bts^2 + cs^3.$$

- Since $x^3 + ax^2 + bx + c$ is monic, every root in $\mathbb{Q}$ is an integer, so no element of $E(\mathbb{Q})[2]$, besides $\mathcal{O}$, is contained in $E_1(\mathbb{Q})$; these are the points at infinity for the affine part given by $Y \neq 0$ with coordinates (s, t), so in terms of these coordinates we have

  $$\begin{aligned} E_n(\mathbb{Q}) &= \{(s,t) \in E(\mathbb{Q}) \ : \ v_p(t) \ge n \text{ and } v_p(s) \ge 3n\} \\ &= \{(s,t) \in E(\mathbb{Q}) \ : \ v_p(t) \ge n \text{ and } v_p(s) > 0\}. \end{aligned}$$

- Stated the following proposition (proof at the end of class, see below).
  Proposition. Suppose $n \ge 1$ and $P_1, P_2, P_3 \in E(\mathbb{Q})$ collinear with $P_1, P_2 \in E_n(\mathbb{Q})$. Then we have

  $$v_p\Big(t(P_1) + t(P_2) + t(P_3)\Big) \ge 3n.$$

- Concluded from the proposition that for each $n \geq 1$, the subset $E_n(\mathbb{Q})$ is a group and there is an injective homomorphism
$$E_n(\mathbb{Q})/E_{3n}(\mathbb{Q}) \hookrightarrow p^n\mathbb{Z}_{(p)}/p^{3n}\mathbb{Z}_{(p)} \cong p^n\mathbb{Z}/p^{3n}\mathbb{Z} \cong \mathbb{Z}/p^{2n}\mathbb{Z}$$
of abelian groups.
- We have a filtration
$$\ldots \subset E_{n+1}(\mathbb{Q}) \subset E_n(\mathbb{Q}) \subset \ldots \subset E_1(\mathbb{Q}) \subset E_0(\mathbb{Q}) \subset E(\mathbb{Q}),$$
and we say that the level of a point $P \in E_1(\mathbb{Q})$ is that integer n for which we have $P \in E_n(\mathbb{Q}) \setminus E_{n+1}(\mathbb{Q})$, i.e., the level is n if and only if $v_p(x) = -2n$ and $v_p(y) = -3n$, which is equivalent to $n = v_p(t)$ (assuming we already know $P \in E_1(\mathbb{Q})$).
- We showed how it follows that $E_1(\mathbb{Q})$ is torsion-free.
- We concluded that torsion points have integral coordinates.
- We also concluded that if $\tilde{E}$ is nonsingular, then there is an injective homomorphism (Silverman-Tate, IV.3)
$$E(\mathbb{Q})_{\text{tors}} \hookrightarrow \tilde{E}(\mathbb{F}_p).$$
- We also showed how the theorem of Nagell-Lutz follows: if $(x, y) \in E(\mathbb{Q})$ is a torsion point, then $x, y \in \mathbb{Z}$ and $y|D$, where the discriminant D equals $-4a^3c+a^2b^2+18abc-4b^3-27c^2$. In fact, one can also prove the stronger fact $y^2|D$ (exercise).

2. Proof of Proposition

The proposition above can be found in both Cassels (Lemma 2 of chapter 11) and Silverman-Tate (page 50-54, ending with $t_1 + t_2 + t_3 \in p^{3\nu}R$). Cassels uses a clever trick (as always) that makes the computation very efficient. However, he does not really explain what's behind it. It avoids the lengthy computation that Silverman-Tate needs on page 52. Here I will split it up into two steps so that you see what actually happens.

Lemma. Suppose p divides a, b, and c and $P_1, P_2, P_3 \in E(\mathbb{Q})$ are collinear with $P_1, P_2 \in E_0(\mathbb{Q})$. Then we have
$$v_p\Big(t(P_1) + t(P_2) + t(P_3)\Big) \geq \min\big(v_p(a), v_p(b), v_p(c)\big).$$

Proof. First note that the reduction $\tilde{E}$ has a singular point at $(0, 0)$, as $\overline{a} = \overline{b} = \overline{c} = 0$. Let the line that contains P_1, P_2, P_3 be given by the linear equation $\alpha x + \beta y = \gamma$, with $v_p(\alpha), v_p(\beta), v_p(\gamma) \geq 0$ and one of the three valuations equal to 0. The first part of Cassels' trick uses that $E_0(\mathbb{Q})$ is a group, so $P_3 = -P_1 - P_2 \in E_0(\mathbb{Q})$. Therefore, all three points have nonsingular reduction. As the line does not intersect the curve $\tilde{E}$ in any more than the three points $\tilde{P}_i$, the reduction of the line does not go through $(0, 0)$. This shows $v_p(\gamma) = 0$ and after dividing the equation for the line by γ, we may assume $\gamma = 1$. In terms of the coordinates s and t, the line is then given by $s = \alpha t + \beta$. The values $t(P_i)$ (for $i = 1, 2, 3$) are the roots of the equation we get by substituting $s = \alpha t + \beta$ in the equation for E, so of
$$\alpha t + \beta = t^3 + at^2(\alpha t + \beta) + bt(\alpha t + \beta)^2 + c(\alpha t + \beta)^3.$$
This can be written as $h(t) = 0$ for $h(t) = c_3t^3 + c_2t^2 + c_1t + c_0$, with
$$c_3 = 1 + a\alpha + b\alpha^2 + c\alpha^3 \qquad \text{and} \qquad c_2 = \beta(a + 2b\alpha + 3c\alpha^2)$$
and two coefficients c_1, c_2 that do not matter. Since the values $t(P_i)$ are roots of h, we have
$$h(t) = c_3(t - t(P_1))(t - t(P_2))(t - t(P_3)).$$
Comparing coefficients of t^2 gives
$$t(P_1) + t(P_2) + t(P_3) = -\frac{c_2}{c_3}.$$
From the fact that p divides a, b, c we get $v_p(c_3) = 0$, so from $v_p(\alpha), v_p(\beta) \geq 0$, we find
$$v_p\Big(t(P_1) + t(P_2) + t(P_3)\Big) = v_p(c_2) \geq v_p\big(a + 2b\alpha + 3c\alpha^2\big) \geq \min\big(v_p(a), v_p(b), v_p(c)\big).$$
□

Proof of the proposition above. Suppose $n \geq 1$ and let E' be the elliptic curve given by

$$y'^2 = x'^3 + a'x'^2 + b'x' + c'$$

with

$$a' = p^{2n}a, \qquad b' = p^{4n}b, \qquad c' = p^{6n}c.$$

Then there is a morphism

$$\tau\colon E \to E', \qquad (x, y) \mapsto (x', y') = (p^{2n}x, p^{3n}y).$$

For any $P = (x, y) \in E_n(\mathbb{Q})$ we have $v_p(x) \leq -2n$ and $v_p(y) \leq -3n$, so for $\tau(P) = (x', y')$ we have $v_p(x') \leq 0$ and $v_p(y') \leq 0$, so $\tau(P)$ does not reduce to $(0, 0)$ and we have $\tau(P) \in E'_0(\mathbb{Q})$. This implies that for $P_1, P_2, P_3 \in E(\mathbb{Q})$ with $P_1, P_2 \in E_n(\mathbb{Q})$, we have $\tau(P_1), \tau(P_2), \tau(P_3) \in E'(\mathbb{Q})$ and $\tau(P_1), \tau(P_2) \in E'_0(\mathbb{Q})$. If P_1, P_2, P_3 are collinear, then so are $\tau(P_1), \tau(P_2), \tau(P_3)$, so with $t' = x'/y'$ we conclude

$$v_p\Big(t'(\tau(P_1)) + t'(\tau(P_2)) + t'(\tau(P_3))\Big) \geq \min\big(v_p(a'), v_p(b'), v_p(c')\big) \geq 2n$$

from the lemma. From $t(P) = p^n t'(\tau(P))$, we conclude

$$v_p\Big(t(P_1) + t(P_2) + t(P_3)\Big) = v_p\Big(p^n\big(t'(\tau(P_1)) + t'(\tau(P_2)) + t'(\tau(P_3))\big)\Big) \geq n + 2n = 3n.$$

□

3. Homework

In exercise 2.12 of Silverman-Tate, find the full torsion subgroup for all examples for which there is no nontrivial 2-torsion.

Furthermore, do three of the exercises below, except for problems you already did last time of course. Do not choose only the easiest ones, and do not choose problems from different sources that are almost the same problems!

(1) Cassels, chapter 12: everything except for exercise 4.
(2) Silverman-Tate, chapter 2: 1,2,4,5,11.
(3) Silverman-Tate, chapter 4: 7.