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 1, we did/saw the following statements.

- We finished chapter 4 of the notes on complex elliptic curves and sections III.4-6 of Silverman-Tate.
- We mentioned Mazur's Theorem on torsion subgroups of $E(\mathbb{Q})$ for an elliptic curve E over $\mathbb{Q}$.
- We saw degenerate Weierstrass curves and stated that for such curves C over k (with characteristic not 2) with a singular point P defined over the ground field k, the set $C(\mathbb{Q}) \setminus \{P\}$ has a group structure determined by the rule that three points on a line add to 0 (or multiply to 1, if you prefer to write the group structure multiplicatively). See Cassels, chapter 9; also Silverman-Tate gives some examples in III.7).
  - We proved that for curves C with a cusp (namely $y^2 = x^3$ after translating the x-coordinate appropriately), the group is isomorphic to the additive group k.
  - We also proved that for curves C with a node where both tangent lines are defined over the ground field (namely $y^2 = x^3 + \gamma^2 x^2$ after translating the x-coordinate appropriately), the group is isomorphic to the multiplicative group k^*.
  - We stated without proof that for curves C with a node where the tangent lines are *not* defined over the ground field (namely $y^2 = x^3 + Cx^2$ for C not a square, after translating the x-coordinate appropriately), the group is isomorphic to the multiplicative group of elements in $k(\sqrt{C})$ of norm 1; in other words, if γ is an element (not in k) such that $\gamma^2 = C$, then the group $C(\mathbb{Q}) \setminus \{P\}$ is isomorphic to the multiplicative group
$$\{\, r + s\gamma \ : \ N(r + s\gamma) = r^2 - Cs^2 = 1 \,\}.$$
- We showed how to reduce points from $\mathbb{P}^2(\mathbb{Q})$ to $\mathbb{P}^2(\mathbb{F}_p)$.
- We showed that any elliptic curve E over $\mathbb{Q}$ given by
$$y^2 = x^3 + ax^2 + bx + c$$
with $a, b, c \in \mathbb{Z}$ has a reduction modulo a prime p, namely $\tilde{E}$ given by
$$y^2 = x^3 + \overline{a}x^2 + \overline{b}x + \overline{c},$$
where $\overline{a}, \overline{b}, \overline{c}$ denote the images of a, b, c in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. It may have a singular point, but if we set
$$E_0(\mathbb{Q}) = \{\, P \in E(\mathbb{Q}) \ : \ \overline{P} \text{ is not singular on } \tilde{E} \,\},$$
then there is a reduction map
$$E_0(\mathbb{Q}) \to \tilde{E}_{\mathrm{ns}}(\mathbb{Q})$$
that is a homomorphism, where $\tilde{E}_{\mathrm{ns}}(\mathbb{Q})$ is the set of nonsingular points on $\tilde{E}$.
- I mentioned that if $\tilde{E}$ has a singular point at $(0, 0)$, then $E_0(\mathbb{Q})$ consists of $\mathcal{O}$ and those affine points (x, y) for which p does not divide the numerator of both x and y (follows easy from the definition of reduction).
- The kernel of reduction, so the set of all points $P \in E(\mathbb{Q})$ that reduce to $\overline{\mathcal{O}}$, is denoted $E_1(\mathbb{Q})$. I mentioned without proof that it consists of $\mathcal{O}$ and all points (x, y) for which p divides the denominator of x or y (which implies p divides the denominator of x *and* y).
- Note that during class, the subscripts in $E_1(\mathbb{Q})$, $E_0(\mathbb{Q})$, and $\tilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ were superscripts, but with the subscripts, they correspond with the notation in section VII.2 of Silverman (not Silverman-Tate). In Cassels, the corresponding notation, used in chapter 11, is $\mathfrak{G}^{(1)}$, $\mathfrak{G}^{(0)}$, and $\overline{\mathfrak{G}}^{(0)}$, respectively. In Silverman-Tate, the group $E_1(\mathbb{Q})$ corresponds to $C(p^1)$ in section II.4. We will continue with the material of these chapters next time.

- **Not** (yet) done:
  - p-adic numbers.
  - proof of Lemma 3 of Cassels' chapter 10.
  - Lemma 1 and 2 of Cassels' chapter 10 (which we probably won't need).
  - The lemma that says that on an elliptic curve E given by
$$y^2 = x^3 + ax^2 + bx + c,$$
with $a, b, c \in \mathbb{Z}$, the coordinates of a point (x, y) can be written as $x = m/e^2$ and n/e^3 with $\gcd(m, e) = \gcd(n, e) = 1$.

2. Useful remark about torsion subgroups

Here is something to prove about finite abelian groups and their torsion (does not count as homework).

Suppose A is a finite abelian group, so that there are primes $p_1, \ldots, p_t$ and positive integers $r_1, \ldots, r_t$, such that A is isomorphic to
$$\mathbb{Z}/p_1^{r_1}\mathbb{Z} \oplus \mathbb{Z}/p_2^{r_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p_t^{r_t}\mathbb{Z}.$$

- Show that $A[2]$ and $A/2A$ have the same size.
- Suppose that G is an abelian group and $f\colon A \to G$ is a homomorphism with kernel $2A$. Let $A[2^\infty]$ denote the subgroup of all 2-power torsion, i.e.,
$$A[2^\infty] = \{\, x \in A \;:\; \exists n \geq 0 : 2^n x = 0 \,\}.$$
Show that if H is a subgroup of $A[2^\infty]$ and $\#f(H) = \#A[2]$, then $H = A[2^\infty]$.

3. Homework

Do four 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) Exercises of chapter 4 of complex elliptic curves.
(2) Silverman-Tate: exercises of chapter 3 (in 3.9, you only need to do three of the curves). The first few of these problems are about heights (sections II.1-3), which we used in a sketch of the proof of the Mordell-Weil theorem in class. You are more than welcome, though, to read this part and do exercises belonging to it.
(3) Cassels: exercises from paragraph 10; you may replace $\mathbb{Q}_p$ by $\mathbb{Q}$ everywhere.