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 October 25, we did/saw the following statements. Unless mentioned otherwise, references refer to the notes on complex elliptic curves. A similar account with several explicit examples is also given in Silverman-Tate, sections III.4-6, and Cassels, chapter 13-15 (which also does the case without a rational 2-torsion point).

- Compared function fields and Riemann-Roch on the algebraic side (over any field) with function field on the complex analytic side (where functions with specific poles can be made very explicitly).
- Reviewed 3.9 from the notes on complex elliptic curves (without the specific degrees of the A and B).
- Did 3.10 and stated that the map $\psi\colon E \to \tilde{E}$, when given in terms of the equations as in exercise 3.18, is given by $(x, y) \mapsto (x + a + b/x, (1 - b/x^2)y)$. Also mentioned why $\tilde{E}$ has a rational 2-torsion point and did the remarks between 4.7 and 4.8.
- Saw that multiplication by 2 is the composition of two isogenies (namely ψ and the analogous map $\tilde{E} \to \tilde{\tilde{E}}$) and an isomorphism, as done between 4.8 and 4.9.
- Stated Mordell-Weil theorem.
- Stated (very vaguely) that the height is a quadratic form.
- Stated weak Mordell-Weil theorem.
- Sketched how weak Mordell-Weil theorem and the notion of heights combine to give the Mordell-Weil theorem.
- Mentioned the exact sequences
$$E(\mathbb{Q}) \xrightarrow{[2]} E(\mathbb{Q}) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E[2])$$
and
$$E(\mathbb{Q}) \xrightarrow{\psi} \tilde{E}(\mathbb{Q}) \to H^1(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \langle T \rangle),$$
where T is a 2-torsion point, and stated that these Galois cohomology groups can be made explicit when the action is trivial, i.e., the 2-torsion points are either all rational (first case), or their is at least one rational point T.
- Defined map $\varphi\colon E(\mathbb{Q}) \to R^*/(R^*)^2$ and showed that any three points on a line (so with sum $\mathcal{O}$) that are not 2-torsion points, map to elements with product 1. Also mentioned a slightly different (but equivalent) definition for φ, worked out in more detail below, which can give an alternative finish of the proof of Lemma 4.3 (also taking care of the 2-torsion points).
- Stated without proof Lemmas 4.4, 4.5, and 4.8. Lemma 4.5 stated as that the image of the map $E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is contained in the subgroup generated by -1 and primes dividing $W_e(e)$.
- Showed how Lemmas 4.6 and 4.9 follow.
- **Not** done:
  - proofs of 4.4 and 4.5.
  - 4.7.
  - image of torsion in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ (only 2-power torsion gives nontrivial image) is of size $\#(E[2] \cap E(\mathbb{Q})$, see comment in the middle of page 90 of Silverman-Tate.
  - an example, see below.

2. Alternative definition of φ

The definition of the map

$$\varphi\colon E(\mathbb{Q}) \to R^*/R^{*2}$$

as given in the notes has two drawbacks. First of all, the choice of the extra term $W_e(\overline{X})$ for the case $x = e$ appears arbitrary. Second, having φ defined differently for the 2-torsion points makes that all proofs are bound to use numerous case distinctions. We will give and explain an equivalent definition of φ that depends on a choice of a 2-torsion point T and that gives just one formula that works for all non-2-torsion points, as well as T (yet still not for the other 2-torsion points, so case distinction is still not avoided completely).

Suppose that W has a rational root e, and let W_e be as in the notes, so that $W(X) = (X - e)W_e(X)$. Set $R_e = \mathbb{Q}[X]/W_e(X)$ and write $\overline{X}$ for the image of X in R_e (as well as for its image in R). The Chinese Remainder Theorem gives an isomorphism

$$\gamma\colon R = \mathbb{Q}[X]/W(X) \to \mathbb{Q}[X]/(X - e) \times \mathbb{Q}[X]/W_e(X) \to \mathbb{Q} \times R_e$$

and the composition $R \to \mathbb{Q}$ of γ with the projection onto the factor $\mathbb{Q}$ is given by $\overline{X} \mapsto e$. Note also that for any polynomial $p(X)$, the image $p(\overline{X}) \in R$ is a unit if and only if p is coprime with W, i.e., no root of W (in $\overline{\mathbb{Q}}$) is a root of p.

The composition

$$\gamma \circ \varphi\colon E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2} \times R_e^*/R_e^{*2} \tag{1}$$

sends a point (x, y) with $y \neq 0$, i.e., $W(x) \neq 0$, to $(x - e, x - \overline{X})$.

Note that if the quadratic polynomial W_e factored as $W_e(X) = (X - e')(X - e'')$, then the Chinese Remainder Theorem would yield an isomorphism $R_e \to \mathbb{Q} \times \mathbb{Q}$ sending $\overline{X}$ to (e', e'') and the composition of the isomorphism $R^*/R^{*2} \to \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$ with φ would be

$$E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}, \qquad (x, y) \mapsto (x - e, x - e', x - e'').$$

We will not assume that W_e has rational roots. For any point $(x, y) \in E(\mathbb{Q})$, we have $y^2 = (x-e)W_e(x)$, so $x-e$ and $W_e(x)$ determine the same class in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. Therefore, the composition of (1) is also given by

$$E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2} \times R_e^*/R_e^{*2}, \qquad (x, y) \mapsto (W_e(x), x - \overline{X}),$$

which is defined for all points except those with $W_e(x) = 0$, but including the 2-torsion point $(e, 0)$!

We now express this map in terms of R (where the expression becomes more ugly), so we need to invert the isomorphism γ of the Chinese Remainder Theorem. Note that the element $W_e(\overline{X})/W_e(e) \in R$ maps under γ to $(1, 0) \in \mathbb{Q} \times R_e$. This makes it easy to check that $\gamma\colon R \to \mathbb{Q} \times R_e$ sends the element

$$x - \overline{X} + (W_e(x) - e + x) \cdot \frac{W_e(\overline{X})}{W_e(e)}$$

to the element $(W_e(x), x - \overline{X})$ we want. So $\varphi\colon E(\mathbb{Q}) \to R^*/R^{*2}$ can be given by

$$(x, y) \mapsto x - \overline{X} + (W_e(x) - e + x) \cdot \frac{W_e(\overline{X})}{W_e(e)}$$

for all points (x, y) with $W_e(x) \neq 0$.

Of course, this formula is much more cumbersome than the definition of φ given in the notes, but it does explain that for $x = e$ we indeed get the image $x - \overline{X} + W_e(\overline{X})$, as given in the notes. Also, it can reduce the number of case distinctions in proofs, as in lemma 4.3: after first doing the case that none of the points involved is a 2-torsion point, this new formula can be used to take the limit $x \to e$, which gives the case that one of the points involved is a 2-torsion point (although you would need some extra general arguments to justify that you may take the limit).

3. Example

Let E denote the elliptic curve given by $y^2 = x(x-3)(x-4)$. We will give a sketch of the computations that shows that $E(\mathbb{Q})$ has rank 0. Set $e_1 = 0$, $e_2 = 3$, and $e_3 = 4$ and $T_i = (E_i, 0)$ for $i = 1, 2, 3$. Let

$$\varphi\colon E(\mathbb{Q}) \to R^*/R^{*2} \cong \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2} \times \mathbb{Q}^*/\mathbb{Q}^{*2}$$

be the usual map that sends $P = (x, y)$ to $(x - e_1, x - e_2, x - e_3)$ if $P \notin \{T_1, T_2, T_3\}$; for $P = T_i$ we replace $x - e_i$ by $W_{e_i}(x)$, and $\varphi(\mathcal{O}) = 1$. The image of the composition of φ with the projection on the i-th factor $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is contained in the subgroup generated by -1 and the primes dividing $W_{e_i}(e_i)$ by Lemma 4.5. In fact, for the first factor we do not need -1. We have $W_{e_i}(e_i) = 12, -3, 4$ for $i = 1, 2, 3$. Given that the product of the three coordinates is a square, we find that the image is contained in the subgroup

$$H = \{(1, \pm 1, \pm 1), (2, \pm 1, \pm 2), (3, \pm 3, \pm 1), (6, \pm 3, \pm 2)\},$$

where for each element the signs are such that the product is positive. The images of T_1, T_2, T_3 are easily determined to be

$$\begin{aligned}
\varphi(T_1) &= (12, -3, -4) = (3, -3, -1),\\
\varphi(T_2) &= (3, -3, -1),\\
\varphi(T_3) &= (4, 1, 4) = (1, 1, 1).
\end{aligned}$$

We see that T_3 is contained in the kernel $\ker\varphi = 2E(\mathbb{Q})$, so there is a point T with $2T = T_3$. Indeed $T = (2, 2)$ is such a point, as is $T + T_i$ for any $i \in \{1, 2, 3\}$. We have $\varphi(T) = (2, -1, -2)$, so we have found two nontrivial elements in $\operatorname{im}\varphi \subset R^*/R^{*2}$ that generate a group $G \subset H$ of order 4. This is the image of the 2-power torsion subgroup (T has order 4), and has the same size as $E[2] \cap E(\mathbb{Q})$, cf. Tate-Silverman, middle page 90.

Since H has order 8, we have $\operatorname{im}\varphi = G$ or $\operatorname{im}\varphi = H$. Suppose $\operatorname{im}\varphi = H$. Then we would have $(1, -1, -1) \in \operatorname{im}\varphi$, so there is a point (x, y) with $x = z_1^2$, $x - 3 = -z_2^2$, and $x - 4 = -z_3^2$ for some rational $z_1, z_2, z_3 \in \mathbb{Q}^*$. The first two equations imply $z_1^2 + z_2^2 = 3$, which has no rational solutions (see first exercise of first homework). We conclude $\operatorname{im}\varphi \neq H$, so $\operatorname{im}\varphi = G$ and $\#(E(\mathbb{Q})/2E(\mathbb{Q})) = \#\operatorname{im}\varphi = 4$.

For a finitely generated abelian group $A = S \times \mathbb{Z}^r$ with S finite, we have $\#(A/2A) = 2^r \cdot \#S[2]$, where $S[2]$ is the 2-torsion of S (i.e., the kernel of multiplication by 2). We apply this to $A = E(\mathbb{Q})$. Given that $\#(E[2] \cap E(\mathbb{Q})) = 4$, we find

$$2^r = \frac{\#(E(\mathbb{Q})/2E(\mathbb{Q}))}{\#(E[2] \cap E(\mathbb{Q}))} = \frac{4}{4} = 1$$

for the rank r of $E(\mathbb{Q})$, so $E(\mathbb{Q})$ has rank 0.

4. Homework

Do four of the exercises below.

(1) Exercises 17 and 18 of chapter 3 of complex elliptic curves (count together as one).
(2) Exercises of chapter 4 of complex elliptic curves.
(3) Silverman-Tate: exercises 3.6, 3.8, 3.9 (here, you only need to do three of the curves).
(4) Cassels: exercise from paragraph 14 (in exercise 1, you only need to do three of the curves).