

MATH 732
THE ARITHMETIC OF ELLIPTIC CURVES
ASSIGNMENTS

A note about assignments: The following are the exercises and assignments I suggest you try. The book by Silverman has a very nice collection of exercises, and I suggest you try as many of those as you can. I will select some exercises from each chapter.

Assignment 1 (Selmer's example). The goal of this assignment is to understand E. Selmer's first example of a curve that violates the local-to-global principle. Show that C/\mathbb{Q} has points locally everywhere (in \mathbb{Q}_p , for all p , and in \mathbb{R}) but has no global points (in \mathbb{Q}). The curve is given by:

$$C : 3x^3 + 4y^3 + 5z^3 = 0.$$

This example (and others) are discussed by Selmer in the first section of "The diophantine equation $ax^3 + by^3 + cz^3 = 0$ ", Acta Math. 85 (1951), 203-362.

Assignment 2. Let E be an elliptic curve defined over \mathbb{Q} and let C be a projective non-singular curve, also defined over \mathbb{Q} and with only one point at infinity (also the point $\mathcal{O} = [0, 1, 0]$). Let P_1, P_2, \dots, P_n be all the affine points of intersection of E and C , defined over $\overline{\mathbb{Q}}$, and counted with multiplicity (i.e. it is possible that $P_1 = P_2$, for example). Then:

$$P_1 + P_2 + \dots + P_n = \mathcal{O}$$

where the addition is occurring on $E(\overline{\mathbb{Q}})$ and \mathcal{O} is the origin of E .

Assignment 3. Read through (and understand) problem 3.7 in the book.

Assignment 4 (Exercise 3.8.(a)). Let E/\mathbb{C} be an elliptic curve. We will later see that there is a lattice (a free abelian group of rank 2) $L \subset \mathbb{C}$ and a complex analytic isomorphism of groups $\mathbb{C}/L \cong E(\mathbb{C})$. (N.B. This isomorphism is given by convergent power series, not by rational functions.) Assuming this, prove that

$$\deg([m]) = m^2 \quad \text{and} \quad E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Assignment 5 (Exercise 3.24). Let E/K be an elliptic curve with complex multiplication over K (i.e. $\text{End}_K(E)$ is strictly larger than \mathbb{Z} .) Prove that for all primes $p \neq \text{char}(K)$, the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the Tate module $T_p(E)$ is abelian. In other words, prove that the image of the representation:

$$\rho_p : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(T_p(E)) \cong \text{GL}(2, \mathbb{Z}_p)$$

is abelian in this case. [Hint: Use the fact that the non-trivial endomorphism in $\text{End}_K(E)$ commute with the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.]

Assignment 6. Exercises from Chapter IV : 4.2, 4.3 and 4.5.

Assignment 7. Understand the definition of "supersingular reduction". Then attempt these problems from Chapter V : 5.6, 5.10, 5.12.

Assignment 8. Exercises from Chapter VI : 6.4, 6.6.

Assignment 9. Exercises from Chapter VII : 7.1, 7.2, 7.3, 7.4, 7.7 and (at least) Ben must do 7.9.

Assignment 10. Exercises from Chapter VIII:

- 8.1 and 8.2;
- 8.4 (“Kummer Theory”, prove it if you have never seen it);
- Find the curves with torsion subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ in the list given by 8.12. Prove that indeed that is the torsion subgroup.
- 8.17;
- 8.19.

Assignment 11. (Elliptic curves with non-trivial rank.) The goal here is a systematic way to find curves of rank at least $r \geq 0$, without using tables of elliptic curves:

- (1) Find 5 non-isomorphic elliptic curves over \mathbb{Q} with rank ≥ 5 . You must prove that the rank is at least 5. One way of doing this is to exhibit 5 points and then calculate the canonical height matrix associated to these 5 points. If the determinant is non-zero, then they are linearly independent.
- (2) Find 6 non-isomorphic elliptic curves over \mathbb{Q} with rank ≥ 6 . If so, then you can probably find 8 curves of rank ≥ 8 as well.
- (3) (Significantly harder) Find 10 non-isomorphic elliptic curves over \mathbb{Q} of rank ≥ 10 .

Assignment 12. Let $p \geq 2$ be a prime. Find Weierstrass equations for all elliptic curves E/\mathbb{Q} such that:

- (1) $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/7\mathbb{Z}$ and
- (2) $\nu_p(j(E))$ is negative and divisible by p , i.e. $j(E)$ has a power of p^p in the denominator.

Note: If you want to know why do we care, ask Ben.

E-mail address: alozano@math.cornell.edu

DEPARTMENT OF MATHEMATICS (MALOTT 584), CORNELL UNIVERSITY.