Homework 2: Points of finite order

Deadline: 14th June (23:55 JST), 2024 at TACT

Exercise 4. Let p be a prime and let $E : y^2 = x^3 + px$. Find all points of finite order in $E(\mathbb{Q})$.

Exercise 5. Proof part (iv) of Proposition 4.1: Let E be an elliptic curve defined over $\mathbb{Q}$. Show that the group $E(\mathbb{C})$ has exactly nine points of order dividing 3. Show that these form a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Exercise 6. Prove the following refinement of Lemma 4.4: Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$ be an elliptic curve. Assume that $P = (x, y) \in E(\mathbb{Q})$ with $x, y \in \mathbb{Z}$ satisfies $2P = (X, Y)$ for some $X, Y \in \mathbb{Z}$. Show that then either $y = 0$ or $y^2 | D$, where $D = 4A^3 + 27B^2$.

(cf. [ST], Exercise 2.11)

Exercise 7. Let E be an elliptic curve defined over $\mathbb{Q}$. Show that if $(x, y) \in E(\mathbb{Q})$ with $\mathrm{ord}_p(x) < 0$ for some prime p, then there exists a $\nu \in \mathbb{Z}_{\geq 1}$ with

$$\mathrm{ord}_p(x) = -2\nu, \qquad \text{and} \qquad \mathrm{ord}_p(y) = -3\nu.$$

References

[ST] J. H. Silverman, J. Tate: *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.