Homework 1: Rational points on conics & elliptic curves

Deadline: 3rd May (23:55 JST), 2024 at TACT

Exercise 1.

(i) Show that there are no solutions to $x^2 + y^2 - 3 = 0$ over $\mathbb{Z}/4\mathbb{Z}$.

(Based on the local-to-global principle, this shows that there is no rational point on this conic.)

(ii) Show that there exists a solution to $x^2 + 1 = 0$ over $\mathbb{Q}_5$.

For this, it suffices to show that for each $m \geq 1$ the congruence

$$x^2 + 1 \equiv 0 \mod 5^m$$

has a solution $x_m \in \mathbb{Z}/5^m\mathbb{Z}$, such that $x_1 \equiv 2 \mod 5$ and $x_{m+1} \equiv x_m \mod 5^m$ for all $m \geq 1$.

Exercise 2. Find all rational points on the conic

$$C\colon\ x^2 - 3xy + y^2 - 5 = 0,$$

given as a 1-parameter family.

(Hint: Compare with Section 1.1 of [ST]).

Exercise 3. A number $n \geq 1$ is called a *congruent number* if it is the area of a right triangle with rational side lengths $a, b, c \in \mathbb{Q}$.

(i) Show that $n \geq 1$ is a congruent number if and only if the elliptic curve

$$E\colon\ y^2 = x^3 - n^2 x$$

has a rational point $(x, y) \in E(\mathbb{Q})$ with $y \neq 0$.

(ii) Show that $n = 1$ is not a congruent number.

For (ii) you do not need to use (i).

References

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