Elliptic Curves - Coursework 1

Due 15 November

You can earn at most 5 points. Choose a combination that adds up to 5.

1) **(1 point)** Prove that a p-adic number $\alpha \in \mathbb{Q}_p$ is in $\mathbb{Q}$ if and only if it has an eventually periodic expansion, that is, there exists some N and s such that $a_i = a_{i+s}$ for all $i > N$.

2) **(1 point)** Let n be a positive integer. Then n can be represented as a sum of four squares of integers:

$$n = u_1^2 + u_2^2 + u_3^2 + u_4^2, \qquad u_1, u_2, u_3, u_4 \in \mathbb{Z}.$$

(Hint) One can suppose $n = p$ a prime (product of two sums of four squares is a sum of four squares). Let a, b be integers such that $a^2 + b^2 + 1 \equiv 0 \pmod{p}$. Consider a lattice $\Lambda \subset \mathbb{Z}^4$ consisting of integers (u_1, u_2, u_3, u_4) such that

$$u_1 \equiv au_3 + bu_4 \pmod{p} \text{ and } u_2 \equiv bu_3 - au_4 \pmod{p}$$

3) **(1 point)** Consider the cubic curve $C : X^3 + 2Y^3 + 4Z^3 - 7XYZ = 0$. Show that none of the inflection points of C are defined over $\mathbb{Q}$. Using Nagell's algorithm transform C into the Weierstrass form. Express the transformation as a birational map $\phi : \mathbb{P}^2 \to \mathbb{P}^2$. Can you find the base locus $B(\phi) \cap C$ of your transformation? To which points do these map to under the isomorphism induced by ϕ?

4) **(2 points)** (i) Show that the intersection of two quadric surfaces, that is, the simultaneous solutions to two homogeneous equations of degree 2 in 4 variables, can be put in the Weierstrass form, if a smooth point is known.

(ii) Show that the group law on

$$X^2 = Y^2 - T^2, \qquad Z^2 = Y^2 + T^2$$

with $(1, 1, 1, 0)$ as neutral element is given by $\mathbf{x}_3 = \mathbf{x}_1 + \mathbf{x}_2$ where

$$\begin{aligned} x_3 &= x_2 t_2 y_1 z_1 - x_1 t_1 y_2 z_2 \\ y_3 &= y_2 t_2 z_1 x_1 - y_1 t_1 z_2 x_2 \\ z_3 &= z_2 t_2 x_1 y_1 - z_1 t_1 x_2 y_2 \\ t_3 &= t_2^2 x_1^2 - t_1^2 x_2^2 = t_2^2 y_1^2 - t_1^2 y_2^2 = t_2^2 z_1^2 - t_1^2 z_2^2 \end{aligned}$$

5) **(2 points)** Suppose that $P = (x, y)$ is a point on the cubic curve

$$y^2 = x^3 + ax^2 + bx + c$$

(i) Show that the x-coordinate of the point $2P$ is given by the formula

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

(ii) Derive a similar formula for the y-coordinate of $2P$ in terms of x and y.

(iii) Find a polynomial in x whose roots are the x-coordinates of the $P = (x, y)$ satisfying $3P = \mathcal{O}$. (Hint. Use the equivalent condition $2P = -P$.)

(iv) For the particular curve $y^2 = x^3 + 1$, find all the points satisfying $3P = \mathcal{O}$. Note that you will need complex numbers.