Topics: Reduction of elliptic curves modulo primes, zeta functions.

10.1. Let a and b be integers such that $a \equiv 16 \pmod{35}$ and $b \equiv 29 \pmod{35}$, and consider the elliptic curve over $\mathbf{Q}$ given by the Weierstrass equation

$$E: \ y^2 = x^3 + ax + b.$$

(a) Prove that the discriminant of E is not divisible by 5 nor by 7.

(b) Show that the torsion subgroup of E is trivial.

10.2. Let E be an elliptic curve over $\mathbf{F}_p$, where p is a prime.

Let $N_1 = \#E(\mathbf{F}_p)$ and $a = p + 1 - N_1$. Let α, β be the (possibly complex) roots of the quadratic polynomial

$$x^2 - ax + p = (x - \alpha)(x - \beta),$$

so that $\alpha\beta = p$ and $\alpha + \beta = a$.

For every $m \in \mathbf{Z}_{\geqslant 1}$, let

$$N_m = p^m + 1 - \alpha^m - \beta^m.$$

(Note that this is consistent with the above definition of N_1.)

Finally, define formally (don't worry about convergence issues)

$$Z_E(T) = \exp\left(\sum_{m=1}^{\infty} N_m \frac{T^m}{m}\right).$$

Use the definition of N_m and the expansion $-\log(1-x) = \displaystyle\sum_{m=1}^{\infty} \frac{x^m}{m}$ to prove that

$$Z_E(T) = \frac{pT^2 - aT + 1}{(1-T)(1-pT)}.$$

10.3. Let E be an elliptic curve over $\mathbf{F}_p$, where p is a prime.

We pick up where Tutorial Question 10.2 left off.

For a complex variable s, define the zeta function of E by

$$\zeta_E(s) = Z_E(p^{-s}).$$

(a) Find the values $s \in \mathbf{C}$ where the function ζ_E is not defined.

(b) Prove the functional equation $\zeta_E(s) = \zeta_E(1-s)$.

(c) Let α, β denote the (complex) roots of the quadratic polynomial $x^2 - ax + p$. Prove that if $|a| \leqslant 2\sqrt{p}$ then $\beta = \overline{\alpha}$ and $|\alpha| = |\beta| = \sqrt{p}$.

(d) Prove the Riemann Hypothesis for ζ_E: if $\zeta_E(s) = 0$ then $\mathsf{Re}\,(s) = 1/2$.

[**Hint**: Use the Hasse bound and part (c).]

10.4. Let $f: \ G \longrightarrow H$ be a function between abelian groups.

Prove that f is a group homomorphism if and only if the following two conditions are satisfied:

(a) for all $g \in G$ we have $f(-g) = -f(g)$;

(b) for all $g_1, g_2, g_3 \in G$, if $g_1 + g_2 + g_3 = 0_G$, then $f(g_1) + f(g_2) + f(g_3) = 0_H$.

10.5. (*) Let E be an elliptic curve over $\mathbf{Q}$, p a prime not dividing the discriminant of E, and $\tilde{E}$ the reduction of E modulo p.

Recall the function $\varphi : E_{\text{tors}}(\mathbf{Q}) \longrightarrow \tilde{E}(\mathbf{F}_p)$ by $\varphi(\mathcal{O}) = \tilde{\mathcal{O}}$ and $\varphi(x, y) = (\tilde{x}, \tilde{y})$.

Use Tutorial Question 10.4 to prove that φ is a group homomorphism.

(For condition (b), there are a few special cases to consider; feel free to restrict to the generic case where P_1, P_2, P_3 are distinct points that are not the point at infinity. To prove that the condition holds, review how the formulas for the group law were obtained in the lectures.)