UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Tuesday, 6 June, 2017 9:00 am to 12:00 pm

PAPER 125

ELLIPTIC CURVES

*Attempt no more than **FOUR** questions.*

*There are **FIVE** questions in total.*

The questions carry equal weight.

STATIONERY REQUIREMENTS
Cover sheet
Treasury Tag
Script paper

SPECIAL REQUIREMENTS
None

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1

(a) Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves. Explain how the degree of ϕ may be read off from the rational functions defining ϕ. Illustrate by computing the degree of the multiplication-by-2 map.

(b) Let P_1, P_2 be points on $y^2 = x^3 + ax + b$. Show that if s_1, s_2, s_3 are the elementary symmetric polynomials in x_1, x_2, x_3 the x-coordinates of $P_1, P_2, P_1 + P_2$ then

$$(s_2 - a)^2 = 4s_1(s_3 + b).$$

Use this to prove that $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form.

(c) Let $E/\mathbb{F}_p$ be an elliptic curve. Find a formula for $\#E(\mathbb{F}_{p^2})$ in terms of $N = \#E(\mathbb{F}_p)$ and p.

2

Let K be a finite extension of $\mathbb{Q}_p$, with valuation ring $\mathcal{O}_K$ and residue field k. Let $n \geqslant 2$ be an integer coprime to p.

(a) What does it mean for an elliptic curve E/K to have good reduction? In this case show that there is a surjective group homomorphism $E(K) \to \widetilde{E}(k)$ and describe its kernel.

(b) What is a formal group $\mathcal{F}$ over $\mathcal{O}_K$? State a condition in terms of the leading coefficient for a morphism of formal groups to be an isomorphism.

(c) Under the hypothesis in (a), show that if $P \in E(K)$ then $K([n]^{-1}P)/K$ is an unramified extension, and the composite of all such extensions (as P varies) has degree at most $n[K(E[n]) : K]$.

3

(a) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + kx$ where $k \geqslant 1$ is an integer. Show that if p is a prime not dividing $2k$ then $\#\widetilde{E}(\mathbb{F}_p) = p + 1$ if and only if $p \equiv 3 \pmod 4$. Deduce that $\#E(\mathbb{Q})_{\mathrm{tors}}$ divides 4. Can it ever equal 4?

(b) Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x(x+1)(x+m^2)$ where $m \geqslant 2$ is an integer. Show that if E has good reduction at 5 or 7 then $E(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

[*You may use any general facts about formal groups provided you state them clearly.*]

4

EITHER

Write an essay on Galois cohomology and its application to the proof of the weak Mordell-Weil theorem.

OR

Write an essay on heights and their application to the proof of the Mordell-Weil theorem.

5

Describe a procedure, that often works in practice, for determining the rank of an elliptic curve with a rational 2-torsion point.

(a) Let $\nu(x)$ be the number of distinct prime divisors of an integer x. Show that if $E/\mathbb{Q}$ is an elliptic curve with Weierstrass equation $y^2 = x(x^2 + ax + b)$ with $a, b \in \mathbb{Z}$ then

$$\operatorname{rank} E(\mathbb{Q}) \leqslant \nu(b) + \nu(a^2 - 4b).$$

(b) Show that p is not a congruent number for all primes p in a suitable congruence class (of odd numbers) mod 8.

END OF PAPER