UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Thursday, 6 June, 2013 1:30 pm to 4:30 pm

PAPER 22

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 $p \geqslant 3$ be a prime and $E/\mathbb{F}_p$ an elliptic curve with Weierstrass equation $y^2 = f(x)$. Find, with proof, a non-zero differential on E that is invariant under all translation maps. Assuming that

$$\deg(\phi + \psi) + \deg(\phi - \psi) = 2 \deg \phi + 2 \deg \psi$$

for all $\phi, \psi \in \operatorname{End}(E)$, show that $E(\overline{\mathbb{F}}_p)[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2$ for all primes $\ell \neq p$, and that $E(\mathbb{F}_p) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for some integers m and n.

(b) Let $E/\mathbb{F}_3$ be the elliptic curve $y^2 = x^3 + x^2 + 2$ and $\phi : E \to E$ the isogeny

$$(x, y) \mapsto \left(\frac{x^3 + x + 2}{(x-1)^2}, \frac{(x^3 + 2x + 1)y}{(x-1)^3} \right).$$

What is the degree of ϕ? For which integers m and n is $m\phi + n\widehat{\phi}$ separable?

[*General facts about morphisms between smooth projective curves may be quoted without proof. You are not required to check that the map* ϕ *in (b) is an isogeny.*]

2

What is a formal group over a ring R? Show that if $\mathcal{F}$ is a formal group over $\mathbb{Z}$ then $\mathcal{F}(p\mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ for all odd primes p. What can be proved by the same methods when $p = 2$? Find examples of formal groups $\mathcal{F}$ and $\mathcal{G}$ over $\mathbb{Z}$ with $\mathcal{F}(2\mathbb{Z}_2) \not\cong \mathcal{G}(2\mathbb{Z}_2)$.

3

(a) Explain what it means for an elliptic curve $E/\mathbb{Q}$ to have good reduction at a prime p. Determine the set of primes of good reduction in the case $E/\mathbb{Q}$ has equation $y^2 = x^3 + 15^2$.

(b) The elliptic curve $E/\mathbb{Q}$ in (a) has rational points $P_1 = (0, 15)$, $P_2 = (-6, -3)$, $P_3 = (4, 17)$. Compute $2P_1$ and $P_1 + P_2$. Show that $\widetilde{E}(\mathbb{F}_7)$ is not cyclic, and find its order. Deduce that if $P \in E(\mathbb{Q})$ then $6P$ does not have integral co-ordinates.

(c) State and prove the Lutz–Nagell theorem. Determine which of the points P_1, P_2, P_3 in (b) have infinite order.

[*You may quote any results you need about formal groups. If* $f(x) = x^3 + ax + b$ *then* $y^2 = f(x)$ *has discriminant* $-16(4a^3 + 27b^2)$ *and*

$$(3x^2 + 4a)f'(x)^2 - 27(x^3 + ax - b)f(x) = 4a^3 + 27b^2.]$$

4

Write an essay on Kummer theory and the weak Mordell–Weil theorem.

5

Let $E/\mathbb{Q}$ be an elliptic curve with a rational 2-torsion point. Explain a procedure that often allows one to compute the rank of $E(\mathbb{Q})$. Illustrate by showing that the primes $p \equiv 3 \pmod 8$ are not congruent numbers.

END OF PAPER