UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Friday, 4 June, 2010 9:00 am to 12:00 am

PAPER 22

ELLIPTIC CURVES

*Attempt no more than **THREE** questions.*

*There are **FOUR** questions in total.*

The questions carry equal weight.

E denotes an elliptic curve, $\mathbb{F}_q$ the field with q elements, $\mathbb{Q}_p$ the field of p-adic numbers and $\#X$ the cardinality of X.

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 E be an elliptic curve over an algebraically closed field k. Prove that E is isomorphic to an elliptic curve in (generalised) Weierstrass form.

Prove that $P \mapsto (P) - (O)$ defines a bijection between E and $\mathrm{Pic}^0 E$.

(b) Let $\Lambda \subset \mathbb{C}$ be a lattice. Show that the field of elliptic functions with respect to Λ is generated over $\mathbb{C}$ by the Weierstrass $\wp$-function and its derivative. [*You may use the standard properties of elliptic functions, provided you state them explicitly.*]

2

Let $E/\mathbb{F}_q$ be an elliptic curve.

(a) Define the qth power *Frobenius map* $E \to E$. Define the *zeta-function* $Z_{E/\mathbb{F}_q}(T)$, and prove that it is a rational function of T.

(b) Show that $E : y^2 = x^3 + x^2 + x + 1$ defines an elliptic curve over $\mathbb{F}_3$ and determine $\#E(\mathbb{F}_{27})$.

[*You may use the properties of endomorphisms of elliptic curves, provided you state them explicitly.*]

3

(a) Define what is meant by a (one-parameter commutative) *formal group* over a ring R and by a homomorphism between two formal groups.

If $h(T) = aT + \ldots$ is such a homomorphism, prove that h is an isomorphism if and only if $a \in R^\times$.

(b) Suppose $E/\mathbb{Q}$ is an elliptic curve with good reduction at $p = 2$, and at $p = 5$ the reduced curve has $\#\tilde{E}(\mathbb{F}_5) = 3$. Show that E has good reduction at 5 and that the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is cyclic of order at most 5. (You should carefully state any results that you use.)

4

Let $E/\mathbb{Q} : y^2 = x(x+5)(x-5)$; note that $\Delta_E = 2^6 5^6$ and $(-4,6) \in E(\mathbb{Q})$.

(a) Explain why the given equation defines a global minimal Weierstrass model over $\mathbb{Q}$, and list the primes of bad reduction for E.

(b) Prove that $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; you may use the fact that $\#\tilde{E}(\mathbb{F}_3) = 4$ and $\#\tilde{E}(\mathbb{F}_7) = 8$ without proof.

(c) Show that $E(\mathbb{Q}_5)/2E(\mathbb{Q}_5) \cong (\mathbb{Z}/2\mathbb{Z})^2$, all coming from E/E_0. Compute the image of the Kummer map

$$E(\mathbb{Q}_5)/2E(\mathbb{Q}_5) \hookrightarrow \mathbb{Q}_5^\times/(\mathbb{Q}_5^\times)^2 \times \mathbb{Q}_5^\times/(\mathbb{Q}_5^\times)^2 .$$

in terms of the representatives $\{1, 2, 5, 10\}$ of $\mathbb{Q}_5^\times/(\mathbb{Q}_5^\times)^2$; you may use the fact that $\sqrt{-1} \in \mathbb{Q}_5$ without proof.

(d) Using the Kummer map over $\mathbb{Q}_5$, $\mathbb{R}$ and $\mathbb{Q}$, prove that $E/\mathbb{Q}$ has Mordell-Weil rank 1.

END OF PAPER