UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Friday, 10 June, 2011 9:00 am to 12:00 pm

PAPER 23

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) Define what is meant by an *isogeny of elliptic curves*, and show that an isogeny is automatically a group homomorphism.

(b) Give an example of elliptic curves E, E' defined over $\mathbb{Q}$ and an isogeny $\phi : E \to E'$ defined over $\mathbb{Q}$, such that points in $\ker \phi$ are not all defined over $\mathbb{Q}$.

(c) Suppose K is an algebraically closed field of characteristic $\neq 2, 3$. Prove that every automorphism of an elliptic curve E in simplified Weierstrass form is of the form $x \mapsto u^2 x,\ y \mapsto u^3 y$ for $u \in K^\times$. Use this to classify possible automorphism groups of elliptic curves over K.

(d) For every isomorphism class of elliptic curves $E/\mathbb{C}$ with $\operatorname{Aut} E \neq \{\pm 1\}$ write down a homothety class of lattices $\Lambda \in \mathbb{C}$ with $\mathbb{C}/\Lambda \cong E$.

2

(a) Suppose $E/\mathbb{Q}$ has no primes of multiplicative reduction. By analysing $E(\mathbb{Q}_p)$ for $p = 2, 3, 5$, show that the group of rational torsion points $E(\mathbb{Q})_{\text{tors}}$ has order at most 6.

(b) Prove that $E : y^2 = x(x-6)(x+6)$ has $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. [You may use that E has j-invariant 1728.]

3

(i) (a) Let K be an algebraically closed field, and suppose $\phi : E \to E'$ is an isogeny of elliptic curves over K. Define the dual isogeny $\hat{\phi}$, and list the formulae for $\phi\hat{\phi}$, $\hat{\phi}\phi$, $\widehat{\phi\psi}$ and $\widehat{\phi + \psi}$, proving all but the last one.

(b) Prove that every endomorphism ϕ of E satisfies a quadratic equation $x^2 - ax + d$ in $\operatorname{End} E$ with $a, d \in \mathbb{Z}$.

(ii) State the Mordell–Weil Theorem and the Weak Mordell Theorem for elliptic curves over number fields. Prove that the latter implies the former ('Descent Theorem'), stating the properties of heights that you use.

4

Let $E/\mathbb{Q} : y^2 = x(x+6)(x-6)$. This is a global minimal Weierstrass model for E, and $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (you do not have to prove this). Note also that $(-3, 9) \in E(\mathbb{Q})$.

(a) Find all primes where E has bad reduction.

(b) Show that $E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^2$, all coming from 2-torsion on E.

(c) Prove that $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) \cong (\mathbb{Z}/2\mathbb{Z})^3$.

(d) Considering the image of the Kummer map

$$\kappa_{E/\mathbb{Q}} : \quad E(\mathbb{Q})/2E(\mathbb{Q}) \quad \hookrightarrow \quad \mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \ \times \ \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$$

and that of $\kappa_{E/\mathbb{Q}_2}$, deduce that $E/\mathbb{Q}$ has Mordell-Weil rank 1. [You may use that $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ are representatives for $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ without proof.]

END OF PAPER