UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Thursday, 31 May, 2012 9:00 am to 11:00 am

PAPER 27

ELLIPTIC CURVES

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

*There are **FOUR** 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

Let $\Lambda \subset \mathbb{C}$ be a lattice and

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

the Weierstrass $\wp$-function with respect to Λ. Prove that the field of elliptic functions is generated by $\wp(z)$ and $\wp'(z)$. Prove also that the map $f(z) = (\wp(z), \wp'(z))$, suitably extended to $z \in \Lambda$, gives a well-defined group isomorphism from $\mathbb{C}/\Lambda$ to the elliptic curve

$$E_\Lambda : \qquad y^2 = 4x^3 - 60G_4 x - 140 G_6\,,$$

where $G_4 = \sum_{w \in \Lambda} w^{-4}$ and $G_6 = \sum_{w \in \Lambda} w^{-6}$. You should check that E_Λ is non-singular.

[You may assume that the expression for $\wp(z)$ converges locally uniformly to an elliptic function, which is analytic on $\mathbb{C} \setminus \Lambda$ and has double poles on $z \in \Lambda$. Basic results on the zeroes and poles of elliptic functions, as well as the convergence properties of $\sum_{w \in \Lambda} w^\alpha$, may be used without proof.]

2

Let E be an elliptic curve over a number field K, given by

$$E : \qquad y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

for some distinct $\alpha, \beta, \gamma \in \mathcal{O}_K$. Prove that $E(K)/2E(K)$ is finite. You may assume that for any $P \in E(K)$ and any point Q with $P = 2Q$, the field extension $K(Q)/K$ is independent of the choice of Q and can be written in the form $K(Q) = K(\sqrt{a}, \sqrt{b})$, for some $a, b \in \mathcal{O}_K$.

When $K = \mathbb{Q}$, find an explicit upper bound on the size of $E(\mathbb{Q})/2E(\mathbb{Q})$. The bound may be crude, but should be given as a function only of $m = \max(|\alpha|, |\beta|, |\gamma|)$.

[Any results about extensions of number fields and ramification of primes may be used without proof.

No version of the Mordell–Weil theorem, weak Mordell–Weil theorem or descent theorem may be assumed.]

3

(i) Explain what is meant by a *formal group.* If F is a formal group over $\mathbb{Z}_p$ and $n \in \mathbb{N}$ is coprime to p, prove that multiplication by n is a bijection on $F(p\mathbb{Z}_p)$.

(ii) For an elliptic curve E over $\mathbb{Q}_p$ given by a minimal Weierstrass model, define the subgroup $E_1(\mathbb{Q}_p)$ and state its relation to the associated formal group.

(iii) Deduce that the points

$$P = \left(\frac{364}{15^2}, \frac{-11737}{15^3}\right), \qquad Q = \left(\frac{2059}{21^2}, \frac{-98783}{21^3}\right),$$

on the elliptic curve

$$E: \qquad y^2 + y = x^3 - x + 6$$

must have infinite order. [You may assume that the model is minimal at all primes.]

(iv) The canonical height of these points of and their sum is

$$\hat{h}_E(P) = 6.61\ldots \qquad \hat{h}_E(Q) = 7.87\ldots \qquad \hat{h}_E(P \oplus Q) = 21.98\ldots$$

to two decimal places. Find the height pairing of P and Q and show that P and Q generate a subgroup of $E(\mathbb{Q})$ isomorphic to $\mathbb{Z} \times \mathbb{Z}$. [You may find it helpful to use the fact that if the group generated by P and Q is not of this form, then there are non-zero integers n and m such that $nP = mQ$.]

4

Let E be the elliptic curve given by

$$E: \qquad y^2 = x(x-2)(x-10)\,.$$

Determine the torsion subgroup of $E(\mathbb{Q})$. Find a rational point of infinite order and show that E has rank 1 over $\mathbb{Q}$.

END OF PAPER