UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Thursday, 4 June, 2009 9:00 am to 12:00 pm

PAPER 26

ELLIPTIC CURVES

*Attempt **ALL** 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 (a) Describe the group law on an elliptic curve in terms of the chord and tangent process. Prove that the group law is associative.

(b) Let E be an elliptic curve of the form

$$y^2 + axy + by = x^3 + bx^2$$

where the discriminant $\Delta = -b^3(16b^2 + (8a^2 - 36a + 27)b + a^4 - a^3)$ is non-zero. Let P be the point $(x, y) = (0, 0)$. Compute the points $\pm 2P$ and $\pm 3P$. Deduce that $5P = 0_E$ if and only if $a = b + 1$.

(c) Give examples of elliptic curves over $\mathbb{Q}$ with rational points of orders 4, 5 and 6.

2 Let E_D be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation

$$y^2 = x^3 - D^2 x$$

with discriminant $\Delta = 64D^6$, where D is an odd integer.

(a) Determine the set of primes of bad reduction for E_D.

(b) For p a prime of good reduction we write $\#\widetilde{E}_D(\mathbb{F}_p) = 1 + p - a_p$. Show that $a_p = 0$ if and only if $p \equiv 3 \pmod 4$. State Hasse's bound for a_p.

(c) Prove that $E_5(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}$.

(d) Use the identity $(x^2 - D^2)^2 + (2xD)^2 = (x^2 + D^2)^2$ to show there are infinitely many right-angled triangles with rational side lengths and area 5.

3 What is a formal group? Write down a condition in terms of the leading coefficient for a homomorphism of formal groups to be an isomorphism.

Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$ and maximal ideal $\pi\mathcal{O}_K$. State and prove a theorem classifying formal groups over K. Deduce that if $\mathcal{F}$ is a formal group over $\mathcal{O}_K$ then $\mathcal{F}(\pi\mathcal{O}_K)$ contains a subgroup of finite index isomorphic to $\mathcal{O}_K$ under addition.

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.

END OF PAPER