UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Wednesday 6 June 2001 1.30 to 4.30

PAPER 19

ELLIPTIC CURVES

Attempt ***ALL FOUR*** *questions. The questions carry equal weight.*

You may not start to read the questions printed on the subsequent pages until instructed to do so by the Invigilator.

1 (i) Let a, b, c be positive integers, with no common factor, such that $a^2 + b^2 = c^2$. Prove that there exist integers n, m, with $n > m > 0$ and $(n, m) = 1$, such that

$$a = n^2 - m^2, \quad b = 2nm, \quad c = n^2 + m^2.$$

(ii) Prove that there is no right-angled triangle, all of whose sides have integer length, and whose area is the square of an integer.

2 Let E be an elliptic curve over a field k, and φ an endomorphism of E. We write $\widehat{\varphi}$ for the dual endomorphism.

(i) Prove that the endomorphism $tr(\varphi) = \varphi + \widehat{\varphi}$ is an integer (we view $\mathbb{Z}$ as embedded in the endomorphism ring of E in the natural fashion).

(ii) Now assume that k is a finite field with q elements, and let φ denote the Frobenius endomorphism of E over k. Prove that

$$\sharp(E(k)) = q + 1 - tr(\varphi).$$

(You may assume that $1 - \varphi$ is separable).

(iii) Now take $k = \mathbb{Z}/5\mathbb{Z}$, and let E be the elliptic curve over k defined by $y^2 = x^3 + x + 1$. Prove that $tr(\varphi) = -3$. Deduce that $tr(\varphi^2) = -1$, and hence show that E has 27 points in the field with 5^2 elements.

3 (i) Let p be a prime number, $\mathbb{Q}_p$ the field of p-adic numbers, E an elliptic curve defined over $\mathbb{Q}_p$, and $\widehat{E}$ the formal group of E. Let m be any non-zero integer prime to p. For each finite extension L of $\mathbb{Q}_p$, prove that the group $\widehat{E}(L)$ is uniquely divisible by m. Assume now that E has good reduction, and let K denote the maximal unramified extension of $\mathbb{Q}_p$. Prove that $E(K)$ is divisible by m.

(ii) Let E be the elliptic curve

$$y^2 + xy = x^3 - 120x + 576.$$

Prove that $E(\mathbb{Q})$ contains no elements of finite order. (You may assume that the discriminant of the given Weierstrass equation is $-2^9 \cdot 3^6 \cdot 101$).

4

Write an essay on the Galois cohomology of elliptic curves, emphasizing how it can be used to study the group of rational points on an elliptic curve defined over $\mathbb{Q}$.