UNIVERSITY OF CAMBRIDGE

MATHEMATICAL TRIPOS Part III

Monday, 6 June, 2016 9:00 am to 12:00 pm

PAPER 125

ELLIPTIC CURVES

*Attempt no more than **FOUR** questions.*

*There are **FIVE** 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

(i) Let $E \subset \mathbb{P}^2$ be a smooth plane cubic defined over $\mathbb{Q}$, with $0_E \in E(\mathbb{Q})$ a point of inflection. Show that E can be put in the Weierstrass form $y^2 = f(x)$ where f is a monic cubic polynomial. Define the group law on E via the chord and tangent process, and verify that $E(\mathbb{Q})$ is a group.

(ii) Show that if $0_E \neq T \in E[2]$ and $K = \mathbb{Q}(T)$ then there is a group homomorphism $\alpha : E(\mathbb{Q}) \to K^*/(K^*)^2$ satisfying $\alpha(P) = x(P) - x(T) \mod (K^*)^2$ for all $P \neq 0, T$.

2

(i) State and prove Hasse's Theorem.[*You should outline the proof of any results you need about degrees of isogenies, but general facts about invariant differentials may be quoted without proof.*]

(ii) Show that if $\psi : E \to E'$ is an isogeny of elliptic curves over $\mathbb{F}_p$ then the groups $E(\mathbb{F}_p)$ and $E'(\mathbb{F}_p)$ have the same order, but need not be isomorphic.

3

(i) Define a formal group, and an isomorphism of formal groups. Let K be a finite extension of $\mathbb{Q}_p$ with valuation ring $\mathcal{O}_K$ and uniformiser π. Show 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 $(\mathcal{O}_K, +)$. [*You should explicitly give the constructions of* $\log(T)$*, but need only sketch that for* $\exp(T)$*.*]

(ii) Show that if $E/\mathbb{Q}$ is an elliptic curve with $E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ then E has at least 4 primes of bad reduction.

4

EITHER

(i) Write an essay on heights and their application to the proof of the Mordell-Weil Theorem.

OR

(ii) Write an essay on Galois cohomology and its application to the proof of the Weak Mordell-Weil Theorem.

5

Explain the method of descent by 2-isogeny, that often allows us to compute the rank of an elliptic curve over $\mathbb{Q}$. Illustrate by computing the ranks of the elliptic curves $y^2 = x(x^2 - x + 1)$ and $y^2 = x(x^2 + 5x - 6)$.

END OF PAPER