MAT3, MAMA

MATHEMATICAL TRIPOS Part III

Friday, 31 May, 2019 1:30 pm to 4:30 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
Rough 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) State and prove Hasse's theorem.

(b) Let $E/\mathbb{F}_3$ be the elliptic curve $y^2 = x^3 - x - 1$. Determine for which integers $r \geqslant 1$ we have $\#E(\mathbb{F}_{3^r}) = 3^r + 1$. [*You may assume that if* ϕ *is an endomorphism of* E *then* $\phi^2 - [\operatorname{tr}\phi]\phi + [\deg\phi] = 0$ *where* $\operatorname{tr}\phi = \deg(1+\phi) - 1 - \deg\phi$.]

2 Let $D \geqslant 1$ be a square-free integer and $E/\mathbb{Q}$ the elliptic curve $y^2 = x^3 - D^2 x$.

(a) Let p be a prime with $p \equiv 3 \pmod 4$. Let $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ be the group of non-singular points on the reduction of E mod p. Prove that $\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_p)$ is either cyclic of order p or non-cyclic of order $p+1$.

(b) What is a formal group, and what is an isomorphism of formal groups? State and prove conditions under which multiplication-by-n is an isomorphism of formal groups.

(c) What is a congruent number? Highlighting the roles played by parts (a) and (b), prove that D is a congruent number if and only if $\operatorname{rank} E(\mathbb{Q}) \geqslant 1$.

3 Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x(x+1)(x+4)$.

(a) Let $P_1 = (-1, 0)$ and $P_2 = (-2, 2)$. Compute $P_1 + P_2$ and $2P_2$.

(b) By using Hasse's theorem, or otherwise, exhibit two primes p of good reduction for which $\#\widetilde{E}(\mathbb{F}_p) = 8$. Hence compute the torsion subgroup of $E(\mathbb{Q})$.

(c) Compute the rank of $E(\mathbb{Q})$.

(d) Show that if $r, s, t \in \mathbb{Q}^*$ with $r^2, s^2, 1, t^2$ in arithmetic progression then $(-2s^2, 2rst) \in E(\mathbb{Q})$. Deduce the result of Euler that there are no non-constant four term arithmetic progressions of square numbers.

4 Write an essay on Kummer theory and its applications to the proof of the weak Mordell-Weil theorem.

5 (a) Define the height $H(P)$ of a point $P \in \mathbb{P}^N(\mathbb{Q})$. Show that if $F : \mathbb{P}^1 \to \mathbb{P}^1$ is a $\mathbb{Q}$-rational morphism of degree d, then there exist constants $c_1, c_2 > 0$ such that

$$c_1 H(P)^d \leqslant H(F(P)) \leqslant c_2 H(P)^d$$

for all $P \in \mathbb{P}^1(\mathbb{Q})$.

(b) Let $E/\mathbb{Q}$ be an elliptic curve. Define the logarithmic height $h : E(\mathbb{Q}) \to \mathbb{R}$. Show that there is a unique function $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}$ satisfying

(i) $|h(P) - \widehat{h}(P)|$ is bounded for all $P \in E(\mathbb{Q})$,

(ii) $\widehat{h}(mP) = m^2 \widehat{h}(P)$ for all $m \in \mathbb{Z}$ and $P \in E(\mathbb{Q})$,

(iii) $\widehat{h}(P + T) = \widehat{h}(P)$ for all $T \in E(\mathbb{Q})_{\text{tors}}$ and $P \in E(\mathbb{Q})$.

(c) For $B > 0$ we put $N(B) = \#\{P \in E(\mathbb{Q}) : \widehat{h}(P) \leqslant B\}$. Show that $N(B) < \infty$ and that if $N(B)/\sqrt{B} \to \infty$ as $B \to \infty$ then $\operatorname{rank} E(\mathbb{Q}) \geqslant 2$.

END OF PAPER