A12216W1

SECOND PUBLIC EXAMINATION

Honour School of Mathematics Part C: Paper C3.7
Master of Science in Mathematical Sciences: Paper C3.7

Elliptic Curves

TRINITY TERM 2023

Thursday 01 June, 2:30pm to 4:15pm

You may submit answers to as many questions as you wish but only the best two will count for the total mark. All questions are worth 25 marks.

You should ensure that you observe the following points:

- start a new answer booklet for each question which you attempt.
- indicate on the front page of the answer booklet which question you have attempted in that booklet.
- cross out all rough working and any working you do not want to be marked. If you have used separate answer booklets for rough work please cross through the front of each such booklet and attach these answer booklets at the back of your work.
- hand in your answers in numerical order.

If you do not attempt any questions, you should still hand in an answer booklet with the front sheet completed.

Do not turn this page until you are told that you may do so

1. (a) [11 marks] State and prove *Hensel's Lemma.*

   (b) [6 marks] Let p be a prime and a an integer.

      (i) Show that if p divides a then $x^p - x + a$ splits into linear factors over $\mathbb{Z}_p$, and otherwise $x^p - x + a$ has no roots in $\mathbb{Z}_p$.

      (ii) Compute an integer x such that $x \equiv 1 \bmod 3$ and $x^3 - x + 3 = 0 \bmod 3^4$.

      (iii) Hence, or otherwise, find integers x and y such that $x^3 - x = 3^y - 3$ and $x > 3$.

   (c) [8 marks] Let p be a prime. Show that $x^2 + 7y^3 + 5z^5 = 0$ has a solution $x, y, z \in \mathbb{Z}_p$ with $(x, y, z) \neq (0, 0, 0)$.
   [*Hint: It may help to observe* $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} > 1$.]

2. (a) [6 marks] Compute the torsion subgroup of the elliptic curve $y^2 = x^3 + 5x^2 + 3x + 7$.

   (b) [6 marks] Let n be an integer with $n > 2$. Show that the equation $y^2 = x^3 + x + (n^2 - 2)$ has infinitely many rational solutions.

   (c) [13 marks] Let R be a field of characteristic zero and let

$$F(X, Y) := \frac{X + Y}{1 + XY} \in R[[X, Y]].$$

      (i) Prove that F defines a formal group over R.

      (ii) Compute explicitly the formal logarithm $\log_F(T)$.

      (iii) Hence find an explicit isomorphism $f(T) \in TR[[T]]$ from F to the formal multiplicative group

$$\widehat{G}_m(X, Y) = X + Y + XY$$

      with $f(T)$ a rational function in T.

3. (a) [14 marks] Let $\mathcal{C} : Y^2 = X(X^2 + aX + b)$, where $a, b \in \mathbb{Z}, b \neq 0, a^2 - 4b \neq 0$, and let $\mathcal{D} : V^2 = U(U^2 + a_1 U + b_1)$, where $a_1 = -2a$ and $b_1 = a^2 - 4b$. Let the map q be defined by

$$q : \mathcal{D}(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2, \;\; (u, v) \mapsto u \text{ when } u \neq 0,$$

$$q : (0, 0) \mapsto b_1, \;\; q : \underline{\mathbf{o}} \mapsto 1.$$

      (i) Show that $q(P + Q) = q(P)q(Q)$ in the case when none of $P, Q, P + Q$ are $(0, 0)$ or $\underline{\mathbf{o}}$.

      (ii) Let $P = (u, v) \in \mathcal{D}(\mathbb{Q})$ with $P \neq (0, 0)$. Explicitly compute the sum $P + (0, 0)$, and deduce that $q(P + (0, 0)) = q(P)q((0, 0))$.

      (iii) By considering the remaining cases, prove that q is a homomorphism.

   (b) [11 marks] Compute the rank of the elliptic curve $y^2 = x(x^2 - 3x + 10)$.