SECOND PUBLIC EXAMINATION

Honour School of Mathematics Part C: Paper C3.7

Honour School of Mathematics and Computer Science Part C: Paper C3.7

Master of Science in Mathematical Sciences: Paper C3.7

ELLIPTIC CURVES

TRINITY TERM 2020

Monday 08 June

Opening time: 09:30 (BST)

You have 2 hours 45 minutes to complete the paper and upload your answer file

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:

1. Write with a black or blue pen OR with a stylus on tablet (colour set to black or blue).
2. On the first page, write
   - your candidate number
   - the paper code
   - the paper title
   - and your course title (e.g. FHS Mathematics and Statistics Part B)
   - but ***do not*** enter your name or college.
3. For each question you attempt,
   - start writing on a new sheet of paper,
   - indicate the question number clearly at the top of each sheet of paper,
   - number each page
4. Before scanning and submitting your work,
   - add to the first page, in numerical order, the question numbers attempted,
   - cross out all rough working and any working you do not want to be marked,
   - and orient all scanned pages in the same way.
5. Submit a single PDF document with your answers for this paper.

If you do not attempt any questions at all on this paper, you should still submit a single page indicating that you have opened the exam but not attempted any questions. Please make sure to write your candidate number on this single page.

1. (a) [5 marks] Compute the 61-adic expansions of $-\frac{11}{5}$ and $\frac{11}{5}$.

   (b) [8 marks] Find $x \in \mathbb{Q}$ with $|x^3 + 3x + 1|_5 \leqslant 5^{-4}$. Prove there does not exist $x \in \mathbb{Q}_5$ with $x^3 + 5x + 5 = 0$.

   (c) [5 marks] Let S be a set of prime numbers, and $\alpha \in \mathbb{Z}$. When S is finite, show that there exists a sequence $x_n \in \mathbb{Z}$ of *distinct* integers such that

$$x_n \to \alpha \text{ as } n \to \infty$$

   with respect to every valuation $|\cdot|_p$ for $p \in S$.

   Does the same result hold when S is infinite? Justify your answer.

   (d) [7 marks] Find the structure of the group $\mathcal{E}(\mathbb{F}_5)$ where $\mathcal{E} : y^2 = x^3 + x - 1$.

   [*You may use any results from lectures provided they are clearly stated.*]

2. (a) [10 marks] For $a \in \mathbb{Q}$ let $\mathcal{E}_a$ be the curve $y^2 = x^3 + ax - a$.

   (i) Find the discriminant $\Delta(a)$ of $x^3 + ax - a$.

   (ii) Assume now $\Delta(a) \neq 0$. Let $P = (1, 1) \in \mathcal{E}_a(\mathbb{Q})$. Show that

$$2P = \left(\frac{1}{4}(a^2 + 6a + 1), \frac{1}{8}(-a^3 - 9a^2 - 15a + 1) \right).$$

   Deduce that P is not of order 4.

   (iii) For $a \in \mathbb{Q}$ with $\Delta(a) = 0$, identify the singular points on $\mathcal{E}_a$ and say whether each is a cusp or a node.

   (b) [5 marks] Compute the torsion subgroup $\mathcal{E}(\mathbb{Q})_{\text{tors}}$ of the curve $\mathcal{E} : y^2 = x^3 - 15x + 22$.

   (c) [5 marks] Show that the equation $y^2 = x^3 - 4x^2 + 5x - 2$ has infinitely many solutions $(x, y) \in \mathbb{Z}^2$.

   (d) [5 marks] Let R be a commutative ring with a 1, and let F be a formal group over R. For m a non-negative integer define the multiplication by m map $[m](T) \in R[[T]]$ inductively by: $[0](T) = 0, [m + 1](T) := F([m](T), T)$. Prove that $[2](T)$ is a homomorphism from F to F.

   [*You may use any results from lectures provided they are clearly stated.*]

3. (a) [10 marks] Compute the rank of the curve $y^2 = x(x^2 + 3x + 5)$.

   (b) [15 marks] Compute the Mordell-Weil group of the curve $y^2 = x(x^2 + 10x + 8)$.

   [*You may use any results from lectures provided they are clearly stated.*]