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 2019

TUESDAY, 11 JUNE 2019, 9.30am to 11.15am

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:

- *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) [14 marks] (i) State the Hasse estimate.
   (ii) Prove that the equation $y^2 = x^3 + x - 3$ has a solution $(x, y) \in \mathbb{F}_p^2$ for every prime number p.
   (iii) Determine the structure of the group $\mathcal{E}(\mathbb{F}_5)$ where $\mathcal{E} : y^2 = x^3 + x - 3$.
   (iv) State Hensel's Lemma.
   (v) Prove that the equation $y^2 = x^3 + x - 3$ has a solution $(x, y) \in \mathbb{Q}_p^2$ for every prime number p.

   (b) [11 marks] (i) Find the 7-adic expansions of the rational numbers $\frac{1}{6}$ and $\frac{4}{21}$.
   (ii) For k a non-negative integer and p a prime number, define

$$a(k, p) := \sum_{n=0}^{\infty} n^k p^n \in \mathbb{Q}_p.$$

   Prove that $a(k, p) \in \mathbb{Q}$ for all such k and p. Furthermore, show that for any fixed k the set

$$\{a(k, p) : p \text{ a prime}\} \subset \mathbb{Q}$$

   is infinite.

2. (a) [8 marks] Let R be a ring (commutative with a multiplicative identity). Define what is meant by a *formal group* over R.
   When K is a field, complete with respect to a discrete non-Archimedean valuation, and R is its valuation ring with maximal ideal $\mathcal{M}$, explain how given a formal group over R one may give $\mathcal{M}$ the structure of a group. (In particular, you should explain carefully how inverses are constructed.)

   (b) [7 marks] Let $\mathcal{E} : y^2 = x^3 + Ax + B$ be an elliptic curve, where $A, B \in \mathbb{Z}$, and let p be an odd prime not dividing its discriminant. Show that the order $\#\mathcal{E}(\mathbb{Q})_{\text{tors}}$ of the torsion subgroup of $\mathcal{E}$ divides the order $\#\tilde{\mathcal{E}}(\mathbb{F}_p)$ of the group of points on the reduction $\tilde{\mathcal{E}}$ of the curve modulo p. [*Any results on formal groups proved in lectures may be assumed provided they are clearly stated.*]

   (c) [10 marks] Now let B be a positive integer and $\mathcal{E}$ be the elliptic curve $y^2 = x^3 + B$.
   (i) Prove carefully that the torsion subgroup of $\mathcal{E}$ always has order dividing 6. [*You may assume that given coprime integers a and n, there are infinitely many primes p with $p \equiv a \bmod n$.*]
   (ii) Explain why 2 divides the order of the torsion subgroup of $\mathcal{E}$ if and only if B is the cube of an integer.
   (iii) Show that 3 divides the order of the torsion subgroup of $\mathcal{E}$ if and only if B is the square of an integer.

3. Let p be an odd prime and $\mathcal{E}_p : y^2 = x(x^2 + p^3)$ be an elliptic curve.

   (a) [17 marks] When $p \equiv 1 \bmod 8$ prove that the rank of $\mathcal{E}_p$ is at most two, and when $p \not\equiv 1 \bmod 8$ prove that the rank of $\mathcal{E}_p$ is at most one.

   (b) [8 marks] Show further that when $p \equiv 3 \bmod 16$ or $p \equiv 7 \bmod 16$ then the rank of $\mathcal{E}_p$ is zero.

   [*You may use any results from lectures provided they are clearly stated. It may also help to recall that for an odd prime p we have that 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \bmod 8$.*]