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

Elliptic Curves
James Newton
Checked by: James Maynard

03/04/2024

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

1. (a) [6 marks] (i) State Hensel's lemma.

   (ii) Let $a \in \mathbb{Q}_7^\times$. Show that a has a cube root in $\mathbb{Q}_7$ if and only if $a = 7^n u$ with $n \in \mathbb{Z}$ divisible by 3, and $u \in \mathbb{Z}_7$ with $u \equiv \pm 1 \mod 7$.

   (b) [19 marks] Consider the elliptic curve with (projective) equation

$$\mathcal{C} : X^3 + Y^3 = 2Z^3$$

   and distinguished identity point $(1 : -1 : 0) \in \mathcal{C}(\mathbb{Q})$.

   (i) For a point $P = (x_1 : y_1 : 1)$ of $\mathcal{C}$, find a formula for the doubled point $2P$ in terms of rational functions in x_1 and y_1.
   [*You may find it useful to note that the tangent line to* $\mathcal{C}$ *at* $(1 : -1 : 0)$ *has equation* $X + Y = 0$.]

   (ii) What are the 2-torsion points of $\mathcal{C}(\mathbb{Q}_7)$?

   (iii) By considering your formula for $2P$, or otherwise, show that $\mathcal{C}(\mathbb{Q}_7)$ contains no point P of order 4.
   [*You may assume without proof that the points in* $\mathcal{C}(\mathbb{Q}_7) \cap \{Z = 0\}$ *do not have order* 4.]

2. Let p be a prime with $p > 5$, and consider the elliptic curve over $\mathbb{Q}$ with equation $\mathcal{E} : y^2 = x^3 + p$.

   [*Throughout this question, results on formal groups from lectures may be assumed provided they are clearly stated.*]

   (a) [7 marks] Let q be a prime with $q \nmid 6p$. Show that the order $\#\mathcal{E}(\mathbb{Q})_{\text{tors}}$ of the torsion subgroup of $\mathcal{E}$ divides the order $\#\widetilde{\mathcal{E}}_q(\mathbb{F}_q)$ of the group of points on the reduction $\widetilde{\mathcal{E}}_q$ of the curve modulo q.
   [*You may assume without proof that the reduction map modulo a prime of good reduction is a homomorphism.*]

   (b) [8 marks] (i) Compute the order $\#\widetilde{\mathcal{E}}_5(\mathbb{F}_5)$ of the group of points on the reduction $\widetilde{\mathcal{E}}_5$ of the curve modulo 5.

   (ii) Compute the number of points $\#\widetilde{\mathcal{E}}_p(\mathbb{F}_p)$ of the reduction $\widetilde{\mathcal{E}}_p$ of the curve modulo p.

   (c) [10 marks] (i) Show that there is no point of $\mathcal{E}(\mathbb{Q}_p)$ reducing to the singular point

$$(0, 0) \in \widetilde{\mathcal{E}}_p(\mathbb{F}_p).$$

   (ii) Deduce that $\#\mathcal{E}(\mathbb{Q})_{\text{tors}} = 1$.

3. (a) [10 marks] Consider an elliptic curve over $\mathbb{Q}$ defined by the equation

$$\mathcal{C} : y^2 = x(x^2 + B),$$

with B a non-zero integer, together with the 2-isogeny $\hat{\phi} : \mathcal{D} \to \mathcal{C}$ from the curve

$$\mathcal{D} : v^2 = u(u^2 - 4B)$$

given by

$$\hat{\phi}(u, v) = \left(\frac{1}{4} \left(\frac{v}{u} \right)^2 , \frac{1}{8} \left(v + \frac{4Bv}{u^2} \right) \right).$$

Show that if there is a point $(u, v) \in \mathcal{D}(\mathbb{Q})$ with $u = rt^2$, for r a squarefree integer and $t \in \mathbb{Q}^\times$, then r divides $4B$ and there are integers l, m, n, not all 0, with $\gcd(l, m) = 1$, satisfying the equation

$$rl^4 - \left(\frac{4B}{r} \right) m^4 = n^2.$$

(b) [10 marks] Suppose p is a prime with $p \equiv 3 \mod 8$. Show that the elliptic curve over $\mathbb{Q}$

$$\mathcal{E} : y^2 = x(x^2 - p^2)$$

has rank 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 $p \equiv \pm 1 \mod 8$ and -1 is a quadratic residue modulo p if and only if $p \equiv 1 \mod 4$.*]

(c) [5 marks] Find a point of infinite order on the curve with equation $y^2 = x(x^2 - 7^2)$, justifying why it has infinite order.

End of Last Page