MAST30035 Assignment 3

Due Friday 16 October at 23:59 on Canvas and GradeScope

Some guidelines:

- Your answers to this assignment can be handwritten (on physical paper and scanned, or on a tablet or other device), or typeset using a system that can produce professional-quality mathematical documents (e.g. LaTeX or Typst, but not Microsoft Word).

  If you are writing by hand, make sure that your writing can appear clearly enough on the document you upload to Gradescope. This is usually achieved by writing legibly with a very readable writing implement.

- Please indicate clearly which question you are writing about at the top of each page. (Ideally, start a new question on a new page.)

  When you upload your document to Gradescope, please mark which pages correspond to which questions.

- The quality of the exposition will be assessed alongside the correctness of the approach.

  There is no need to include your preparatory scratch work (do this on separate paper) but make sure that the solution you submit is a complete explanation.

  "Completeness" of the explanation is somewhat subjective, but: results from the lectures, tutorials, exercises can be used (without having to re-prove them). Make sure you say clearly what result(s) you are using, though.

- It is acceptable for students to discuss the questions on the assignments and strategies for solving them. However, each student must write down their solutions in their own words and notation (and make sure that they understand what they are writing).

- As a large language model, I do not have an opinion about your use of generative AI to complete this assignment.

  Actually… I do have an opinion.

  Whatever resource you tap into, use it in a smart way: know its limitations, and do the work of really understanding what it is that you are submitting. This is true of your mate who is smart but tends to make arithmetic mistakes, of your favourite linear algebra or analysis book that uses completely different notation to ours, or of the chatbot that sounds impressive but hallucinates references or gives you a proof that relies on lots of results we have not seen in the subject (and that's the best case scenario). Do your job: be paranoid, double-check everything, take it apart and put it back together until it makes sense to you.

  Why? (a) when you submit something as your own work, you assume responsibility for it; (b) see the next point.

- Assignments are a valuable learning tool in this subject, so strive to maximise their impact on your understanding of the material.

- No Chegg or anything similar. At all. Please.

This assignment consists of 3 questions. Please scan your answer pages and upload them to GradeScope in the correct order.

3.1. (10 marks)

Consider the family of elliptic curves E_n appearing in the congruent number problem:

$$E_n : \ y^2 = x^3 - n^2 x, \qquad n \in \mathbf{Z}_{\geqslant 1}.$$

In this question you will prove that the only torsion points on E_n are the points of order dividing 2:

$$E_{n,\mathrm{tors}}(\mathbf{Q}) = \{\mathcal{O}, (-n, 0), (0, 0), (n, 0)\}.$$

(a) Prove that for any $d \in \mathbf{Z}_{\geqslant 1}$, the elliptic curve $E_{d^2 n}$ is isomorphic to the elliptic curve E_n.

(b) By part (a), we may assume that n is squarefree. Let $P = (x, y) \in E_n(\mathbf{Q})$ be a point with $x, y \in \mathbf{Z}$, $y \neq 0$, and write $[2]P = (x_2, y_2)$. Prove that $x_2 \notin \mathbf{Z}$.

[**Hint**: Consider the parities of x and n.]

(c) Explain why part (b) implies that P has infinite order.

Solution.

(a) Letting $x = (d^{-1})^2 \hat{x}$ and $y = (d^{-1})^3 \hat{y}$ in E_n, we get an isomorphic elliptic curve with equation

$$d^{-6}\hat{y}^2 = d^{-6}\hat{x}^3 - n^2 d^{-2}\hat{x} \quad \Rightarrow \quad \hat{y}^2 = \hat{x}^3 - (d^2 n)^2 \hat{x},$$

which is precisely the equation of $E_{d^2 n}$.

(b) By the duplication formula we have

$$x_2 = \frac{x^4 + 2n^2x^2 + n^4}{(2y)^2} = \frac{(x^2 + n^2)^2}{4x(x^2 - n^2)}.$$

- If x and n have different parities, then the numerator of x_2 is odd, but its denominator is even, so $x_2 \notin \mathbf{Z}$.
- If x and n are both odd, then $x^2 \equiv 1 \pmod 4$ and $n^2 \equiv 1 \pmod 4$, so $x^2 + n^2 \equiv 2 \pmod 4$. This means that 2^1 is the highest power of 2 dividing $x^2 + n^2$, hence 2^2 is the highest power of 2 dividing the numerator of x_2. On the other hand, the denominator is at least divisible by 2^4, since $x^2 - n^2 \equiv 0 \pmod 4$. Hence $x_2 \notin \mathbf{Z}$.
- Suppose now that x and n are both even, $x = 2r$, $n = 2s$, so that

  $$x_2 = \frac{(r^2 + s^2)^2}{2r(r^2 - s^2)}.$$

  Since n is squarefree, we have that s is odd.
  If r is even, then the numerator is odd and the denominator is even, so $x_2 \notin \mathbf{Z}$.
  If r is odd, then as in the previous case $(r^2+s^2)^2$ is a multiple of 4 but not of 8, while $2r(r^2-s^2)$ is at least divisible by 8, so once again $x_2 \notin \mathbf{Z}$.

(c) Suppose P has finite order, then $[2]P$ also has finite order, so by the Lutz–Nagell Theorem its coordinates are integers, contradicting the fact that $x_2 \notin \mathbf{Z}$. □

3.2. (17 marks)

You are now asked to prove the same statement as in Assignment Question 3.1, but via a different approach.

(a) Suppose p is an odd prime that does not divide the discriminant of E_n. Prove that the cardinality of $\tilde{E}_n(\mathbf{F}_p)$ can be expressed as

$$\#\tilde{E}_n(\mathbf{F}_p) = 1 + \sum_{x \in \mathbf{F}_p} \left(1 + \left(\frac{f(x)}{p}\right)\right),$$

where $f(x) = x^3 - n^2 x$ and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol modulo p.

(b) Suppose p is an odd prime that does not divide the discriminant of E_n. Assume moreover that $p \equiv 3 \pmod 4$. Prove that $\#\tilde{E}_n(\mathbf{F}_p) = p + 1$.

[**Hint**: What can you say about $f(-x)$?]

(c) Fix a prime $p \equiv 3 \pmod 8$ and let $\ell_1, \dots, \ell_t$ be the odd prime divisors of $p + 1$.

Show that the set S of solutions of the system of congruences

$$\begin{aligned} x &\equiv 3 \pmod 8, \\ x &\equiv 1 \pmod{\ell_j} \quad \text{for all } j = 1, \dots, t \end{aligned}$$

is a primitive arithmetic progression.

(d) Show that if $q \in S$ is prime, then $\gcd(p + 1, q + 1) = 4$.

(e) Explain how you can put together the previous parts to show that the cardinality of the torsion subgroup of $E_n(\mathbf{Q})$ is 4.

Solution.

(a) We count the points in $\tilde{E}(\mathbf{F}_p)$ one $x \in \mathbf{F}_p$ at a time (plus the point at infinity).

- If x is such that $f(x) = 0$, so $\left(\frac{f(x)}{p}\right) = 0$, we get one point.
- If x is such that $f(x) \neq 0$ is a quadratic non-residue, so $\left(\frac{f(x)}{p}\right) = -1$, we get zero points.
- If x is such that $f(x) \neq 0$ is a quadratic residue, so $\left(\frac{f(x)}{p}\right) = 1$, we get two points.

In each case the number of points we get is precisely $1 + \left(\frac{f(x)}{p}\right)$. Putting it all together gives the desired expression.

(b) We rewrite the expression in part (a) as

$$\#\tilde{E}_n(\mathbf{F}_p) = 1 + \sum_{x \in \mathbf{F}_p} \left(1 + \left(\frac{f(x)}{p}\right)\right) = p + 1 + \sum_{x \in \mathbf{F}_p} \left(\frac{f(x)}{p}\right).$$

Observe that f is an odd function: $f(-x) = (-x)^3 - n^2(-x) = -(x^3 - n^2 x) = -f(x)$ for all x. Therefore

$$\left(\frac{f(-x)}{p}\right) = \left(\frac{-f(x)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{f(x)}{p}\right) = -\left(\frac{f(x)}{p}\right),$$

where we used the multiplicativity of the Legendre symbol and the assumption that $p \equiv 3 \pmod 4$.

So $x = 0$ contributes 0 to the sum above, and each $x \neq 0$ can be paired with $-x$ and together contribute

$$\left(\frac{f(x)}{p}\right) + \left(\frac{f(-x)}{p}\right) = \left(\frac{f(x)}{p}\right) - \left(\frac{f(x)}{p}\right) = 0.$$

We conclude that the whole sum is 0, so that $\#\tilde{E}_n(\mathbf{F}_p) = p + 1$.

(c) The solution set is an arithmetic progression by the Chinese Remainder Theorem. Moreover, there is a unique solution x with $0 \leqslant x < m$, and it is clear from the congruences that 0 is not a solution, so $0 < x < m$. In particular, $\gcd(x, m) = 1$ so the arithmetic progression is primitive.

(d) Let $g = \gcd(p + 1, q + 1)$; clearly g is divisible by 2.

Suppose an odd prime ℓ divides g, then $\ell \in \{\ell_1, \dots, \ell_t\}$ so $q + 1 \equiv 2 \pmod \ell$; since $\ell \mid (q + 1)$ this implies that $\ell \mid 2$, contradiction.

So g is a power of 2. But $p, q \equiv 3 \pmod 8$ means that $p + 1, q + 1 \equiv 4 \pmod 8$, so $p + 1$ and $q + 1$ are both divisible by 4 but no higher power of 2.

Hence $g = 4$.

(e) First we note that by Dirichlet's Theorem there are infinitely many primes in the primitive arithmetic progression $x \equiv 3 \pmod 8$, and since the discriminant Δ of E_n is only divisible by finitely many primes, we can find a prime $p \equiv 3 \pmod 8$ that does not divide Δ.

Since the set S of part (b) is a primitive arithmetic progression, it contains infinitely many primes q. We can therefore find a prime $q \in S$ that does not divide Δ.

Since both p, q are coprime to Δ, we can reduce E_n modulo p and modulo q. By part (a) we have $\#\tilde{E}_n(\mathbf{F}_p) = p+1$ and $\#\tilde{E}_n(\mathbf{F}_q) = q+1$. Therefore the number of torsion points of E_n divides both $p+1$ and $q+1$, so by part (c) it divides 4. But we already know 4 torsion points (the point at infinity and the three points of order 2). □

3.3. (13 marks)

We explore some consequences of Corollary 3.35.

(a) Suppose an elliptic curve E over $\mathbf{Q}$ has discriminant that is not divisible by 3. Identify which groups appearing in Theorem 3.12 **cannot** be isomorphic to the torsion subgroup of E. (Explain your answer, of course.)

(b) Let E be an elliptic curve over $\mathbf{Q}$ given by a Weierstrass equation

$$E: \ y^2 = x^3 + ax + b, \qquad a, b \in \mathbf{Z}.$$

Suppose that E has torsion subgroup isomorphic to $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}$. Prove that $4a^3 + 27b^2$ is divisible by 105.

(c) With the same assumptions as in part (b), find the congruence conditions modulo 3, 5, and 7 that a and b must satisfy.

Solution.

(a) Since 3 does not divide the discriminant of E, we can reduce E modulo 3. By Corollary 3.35 we have $\#E_{\text{tors}}(\mathbf{Q}) \mid \#\tilde{E}(\mathbf{F}_3)$.

The Hasse bound gives us

$$4 - 2\sqrt{3} \leqslant \#\tilde{E}(\mathbf{F}_3) \leqslant 4 + 2\sqrt{3},$$

which implies that $\#\tilde{E}(\mathbf{F}_3) \in \{1, 2, 3, 4, 5, 6, 7\}$. Checking against Mazur's list, the following **cannot** occur:

$$\mathbf{Z}/8\mathbf{Z}, \mathbf{Z}/9\mathbf{Z}, \mathbf{Z}/10\mathbf{Z}, \mathbf{Z}/12\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}, \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/8\mathbf{Z}.$$

(b) From part (a) we know that the discriminant $-16(4a^3+27b^2)$ must be divisible by 3. Hence $4a^3+27b^2$ must be divisible by 3.

By a similar argument, if 5 does not divide $4a^3 + 27b^2$ then by the Hasse bound

$$6 - 2\sqrt{5} \leqslant \#\tilde{E}(\mathbf{F}_5) \leqslant 6 + 2\sqrt{5} < 11,$$

contradicting the assumption that E has 16 torsion points. So 5 must divide $4a^3 + 27b^2$.

Finally, if 7 does not divide $4a^3 + 27b^2$ then

$$8 - 2\sqrt{7} \leqslant \#\tilde{E}(\mathbf{F}_7) \leqslant 8 + 2\sqrt{7} < 14,$$

contradicting the assumption that E has 16 torsion points. So 7 must divide $4a^3 + 27b^2$.

We conclude that $4a^3 + 27b^2$ is divisible by $3 \cdot 5 \cdot 7 = 105$.

(c) Since $3 \mid 4a^3 + 27b^2$ we get that $3 \mid a^3$ so $a \equiv 0 \pmod 3$. There are no modulo 3 conditions for b.

We have $4a^3 + 27b^2 \equiv 0 \pmod 5$ so $2b^2 \equiv a^3 \pmod 5$ or better yet $b^2 \equiv 3a^3 \pmod 5$.

Running through the possibilities for a modulo 5 we get $(a, b) = (0, 0), (2, \pm 2), (3, \pm 1)$ modulo 5.

We have $4a^3 + 27b^2 \equiv 0 \pmod 7$ so $27b^2 \equiv 3a^3 \pmod 7$ so $9b^2 \equiv a^3 \pmod 7$ so $2b^2 \equiv a^3 \pmod 7$ so $b^2 \equiv 4a^3 \pmod 7$.

Running through the possibilities for a modulo 7 we get $(a, b) = (0, 0), (1, \pm 2), (2, \pm 2), (4, \pm 2)$ modulo 7. □