

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. $\text{\LaTeX}$ 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:

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

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

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

- (a) Prove that for any $d \in \mathbf{Z}_{\geq 1}$, the elliptic curve E_{d^2n} 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.

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 $f(x) = x^3 - n^2x$ 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.

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

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

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.