MAST30035 Assignment 2

Due Friday 18 September 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.

2.1. (14 marks)

An integer t is called a *triangular number* if it is of the form

$$t = \frac{x(x-1)}{2} \qquad \text{for some } x \in \mathbf{Z}_{\geqslant 1}.$$

Note that 0 is considered a triangular number here.

In this question you will use triangular numbers to prove Lagrange's Four Square Theorem. In particular, you should not be relying on Lagrange's Theorem anywhere below.

Consider the statement

($*$) Every positive integer is the sum of three triangular numbers.

(a) Prove that if k is the sum of four squares, then so is $2k$.

(b) Prove that if $2k$ is the sum of four squares, then so is k.

[**Hint**: Writing $2k = x^2 + y^2 + z^2 + t^2$, what can the parities of x, y, z, t be?]

(c) Suppose that ($*$) is true. Prove that every positive integer m that is $\equiv 3 \pmod 8$ is the sum of three squares.

[**Hint**: Write $m = 8k + 3$ and write k as a sum of three triangular numbers.]

(d) Suppose that ($*$) is true. Prove Lagrange's Theorem: every positive integer n is the sum of four squares.

[**Hint**: What does part (c) tell you about $n \equiv 4 \pmod 8$? Then use the previous parts.]

(e) Prove that n is a sum of two triangular numbers if and only if $8n + 2$ is a sum of two squares.

2.2. (18 marks)

Let $p \geqslant 5$ be a prime number and consider the elliptic curve over $\mathbf{Q}$ given by

$$E_p : \; y^2 = x^3 + p^2.$$

(a) Show that E_p has no points of order 2.

(b) Show that the obvious point $Q = (0, p) \in E(\mathbf{Q})$ is torsion by finding its order.

(c) Let $P = (x_1, y_1) \in E(\mathbf{Q})$ be a torsion point. What possibilities for y_1 does the Lutz–Nagell Theorem give?

(d) Suppose that $P \neq \pm Q$. Use $P + Q$ and $P - Q$ to prove that $x_1 \mid 2p$.

(e) Using the previous parts, find all the torsion points of E_p.

(f) Allowing $p = 3$ now, we have $E_3 : \; y^2 = x^3 + 9$. Is the point $(-2, 1) \in E_3(\mathbf{Q})$ torsion?

2.3. (8 marks)

Alice and Bob use the Diffie–Hellman key exchange protocol in the group $G = (\mathbf{Z}/p\mathbf{Z})^\times$ with $p = 491$ and $g = 2$. They exchange publicly $A = 397$ and $B = 6$.

(a) Factor $p - 1$ and verify that g is a primitive root modulo p.

(b) Apply the Pohlig–Hellman method to find Alice's secret exponent a. (Find the discrete logarithm for each prime power ℓ^s dividing $p - 1$, then put them all together using the Chinese Remainder Theorem.)

(c) Verify that $g^a \equiv A \pmod p$ and find the shared secret key g^{ab}.

You may use technology for the calculations in $(\mathbf{Z}/p\mathbf{Z})^\times$, but follow the steps as indicated.