MAST30035 Assignment 1

Due Friday 21 August 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.

1.1. (18 marks) Recall the *Fibonacci numbers*, given by $F_0 = 0$, $F_1 = 1$ and recursively

$$F_{n+1} = F_n + F_{n-1} \qquad \text{for all } n \geqslant 1.$$

(a) Prove that $\mathsf{gcd}\,(F_{n+1}, F_n) = 1$ for all $n \geqslant 1$.

(b) What can you say about $\mathsf{gcd}\,(F_{n+2}, F_n)$ and $\mathsf{gcd}\,(F_{n+3}, F_n)$ as n varies? In this part, just state your observation(s), no need for a proof.

(c) Consider the matrix

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

Prove that

$$A^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} \qquad \text{for all } n \geqslant 1.$$

(d) Prove that $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$ for all $m, n \geqslant 1$. [**Hint**: $A^{m+n} = A^m A^n$.]

(e) Prove that if $m \mid n$ then $F_m \mid F_n$. [**Hint**: Induction on n/m.]

(f) Prove that for all $m, n \geqslant 1$, if $n = qm + r$ then $\mathsf{gcd}\,(F_n, F_m) = \mathsf{gcd}\,(F_m, F_r)$.

(g) Prove that $\mathsf{gcd}\,(F_n, F_m) = F_{\mathsf{gcd}\,(n,m)}$ for all $m, n \geqslant 1$.

(h) Conclude that: if $F_m \mid F_n$ then $m \mid n$.

1.2. (14 marks) We take a closer look at the efficiency of the Euclidean Algorithm for computing $\mathsf{gcd}\,(a, b)$. **Throughout the question we assume that $a > b \geqslant 1$.**

Let $E(a, b)$ denote the number of steps (that is, divisions) that the Euclidean Algorithm takes to compute $\mathsf{gcd}\,(a, b)$.

(a) Fix $n \geqslant 1$. We know from Assignment Question 1.1 that $\mathsf{gcd}\,(F_{n+1}, F_n) = 1$. What is $E(F_{n+1}, F_n)$?

(b) Use induction to prove that: for all $n \geqslant 1$, if $E(a, b) = n$, then $a \geqslant F_{n+2}$ and $b \geqslant F_{n+1}$.

(c) Use part (b) and the fact that

$$F_{n+1} \geqslant 10^{(n-1)/5} \qquad \text{for all } n \geqslant 1 \text{ (you are not asked to prove this)}$$

to show that $E(a, b) \leqslant 5 \log_{10}(b) + 1$.

(d) We now take a different approach. Let's set up the following notation for the Euclidean Algorithm: Define natural numbers r_n recursively as follows: let $r_0 = a$ and $r_1 = b$. If $n \geqslant 2$ and $r_{n-1} > 0$, define r_n by applying the Division Algorithm to r_{n-2} and r_{n-1}:

$$r_{n-2} = q_{n-2} r_{n-1} + r_n, \qquad 0 \leqslant r_n < r_{n-1}.$$

Prove that $2r_{n+2} < r_n$ for all n such that r_{n+2} is defined.

(e) Conclude that $E(a, b) \leqslant \log_2(b) + 1$.

(f) Compare briefly the results in parts (c) and (e).

1.3. (8 marks) My RSA private[1] key is (N, e), where $e = 65537$ and

$$N = 613741728013616690147699038703457766174721061233103055423658683990710518710554288157091$$

(a) Use this to encrypt your student ID number and send the ciphertext to: `aghitza.ntc@fastmail.fm`

In your assignment, describe how you obtained the ciphertext. (This can be short, and there's no wrong answer, I'm just curious to know how you went about it: SageMath? pen and paper? AI?)

(b) Given that N has 87 (decimal) digits, it is reasonable to assume that the two primes p and q such that $N = pq$ are roughly the size of $\sqrt{N}$; let's say, conservatively, that $10^{43} \leqslant p, q \leqslant 10^{45}$.

Estimate the probability that a randomly chosen m with $0 < m < N$ has $\mathsf{gcd}\,(m, N) > 1$.

(c) Recall that student ID numbers have at most 7 decimal digits; thus estimate the probability that your student ID m has $\mathsf{gcd}\,(m, N) > 1$.

[1] Just kidding, it's actually my public key.