Last/Family Name:
First/Given Name:
Student ID:

MATH 37181 FINAL PART B SPRING 2021

INSTRUCTIONS.
- If you don't have a printer or tablet:
  - write your declaration "I declare that: this is my own work ..." at the start of your blank page for Part B;
  - write your answers in the same order and format as this file on blank paper.
- Write your name and student ID on the top of your first page.
- Upload your scan to Canvas - Assignments - Final Exam Part B as a **single PDF file**.
- Name your file using your last-name, student ID number and -PartB, eg: Elder12345678-PartB.pdf
- Show all steps and working out. Clearly identify your answers for the multiple choice. (Eg write B1:F, B2:F, B3:F, B4:F, B5:F on your first page, or circle on a printed page.)
- You may use a basic scientific calculator for calculations. For Question B3 only you may also use the powermod website.

Part B has **5 multiple choice** and **2 long answer questions** worth a total of 15 marks. You should spend roughly 1 hour on this part.

I declare that: this is my own work, I have not used Discord/Wechat/Facebook etc or asked anyone anything during the exam, I have not posted screenshots or uploaded anything to an online site, I have not used any phone apps except a basic calculator app and Camscanner or other scanning app to scan my work, and I have not looked at any websites other than Canvas to download/upload, and powermod for Question B3.

(sign your name here) ____

Date: 16 November 2021.

B1. (1 mark) Let ϕ denote Euler's phi function. The value of $\phi(1739)$ is equal to

A. $1739 - 1$

B. $\phi(39)\phi(49)$

C. $\phi(37)\phi(49)$

D. $\phi(37)\phi(47)$

E. $37^2 - 37$

F. none of (A)–(E).

B2. (1 mark) Alice constructs an RSA system by choosing $n = 1739$ and $e = 35$. Alice's corresponding value for d is

A. $d = 757$

B. $d = 901$

C. $d = 899$

D. $d = 600$

E. $d = 897$

F. none of (A)–(E).

B3. (1 mark) Following on from the previous question (B2), suppose Bob sends Alice $c = 117$. Alice works out Bob's secret value of m to be [1]

A. $m = 366$

B. $m = 364$

C. $m = 175$

D. $m = 119$

E. $m = 370$

F. none of (A)–(E).

[1] You may use `https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html` instead of repeated squaring to save some time for this question.

B4. (1 mark) Let f_n denote the number of strings of $0, 1$ of length $n \in \mathbb{N}$ which avoid the factor[2] 000. Then for $n \geqslant 3$, f_n satisfies

A. $f_n = f_{n-1} + f_{n-2}$

B. $f_n = 3n$

C. $f_n = f_{n-1} + f_{n-2} + f_{n-3} + f_{n-4}$

D. $f_n = f_{n-1} + f_{n-2} + f_{n-3}$

E. $f_n = f_{n-1} + 2f_{n-2}$

F. none of the above.

B5. (1 mark) Define a relation $\mathscr{R}$ on the set of all finite length binary strings by $a\mathscr{R}b$ if

- the sum of the digits in a equal to the sum of the digits in b, **and**
- a is obtained from b by deleting zero or more digits from b.

Which of the following is false?

A. $\mathscr{R}$ is reflexive

B. $\mathscr{R}$ is antisymmetric

C. $\mathscr{R}$ is transitive

D. $\mathscr{R}$ is symmetric

E. $11\mathscr{R}0110$

F. none of (A)–(E).

[2] if w is a string, u is a factor means $w = u_0uu_1$ where u_0, u, u_1 are strings. For example the string 010 is a factor of 001010 ($u_0 = 0$, $u_1 = 10$ or $u_0 = 001$, $u_1 =$ empty), and 010 is not a factor of 001100.

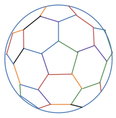
B6. (5 marks) Let $x, y, n \in \mathbb{N}_+$.

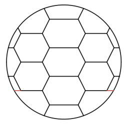
(a) Prove that if $\exists \lambda, \mu \in \mathbb{Z}$ so that $1 = \lambda x + \mu y$, then $\gcd(x, y) = 1$.

(b) Prove that if $\gcd(x, n) = 1$ and $\gcd(y, n) = 1$ then $\gcd(xy, n) = 1$.

B7. (5 marks)

(a) A soccer ball has a pattern on it made up of pentagons (5-sided shape) and hexagons (6-sided shape). Three faces (pentagons or hexagons) meet at each vertex.





Using theorems proved in Weeks 11-12, how many pentagons can a soccer ball have? Show all working.

(b) Prove that every connected graph with $n \in \mathbb{N}_+$ vertices has a spanning tree with $n-1$ edges.

State clearly which proof method(s) you are using and set out correctly.

END OF PART B