EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2022	MATH2617-WE01

Title:
Elementary Number Theory II

Time:	2 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	No	Models Permitted: Use of electronic calculators is forbidden.

Instructions to Candidates:	Answer all questions. Section A is worth 40% and Section B is worth 60%. Within each section, all questions carry equal marks. Students must use the mathematics specific answer book.

Revision:	

ED01/2022

SECTION A

Q1 (a) Find the remainder $r \in \mathbb{N}$, $r < 41$, when $7^{7^{101}}$ is divided by 41.

(b) Find all the integer solutions to the equation

$$153x - 34y = 68.$$

Q2 (a) Let p be a prime number such that $q = 4p + 1$ is also a prime number. Prove that 2 is a primitive root mod q. *(Hint: Use Euler's criterion.)*

(b) You are given that the continued fraction expansion of $\sqrt{22}$ is

$$[4; \overline{1, 2, 4, 2, 1, 8}].$$

Find a solution $(x, y) \in \mathbb{N}^2$ to the equation $x^2 - 22y^2 = 1$.

SECTION B

Q3 (a) Find an $x \in \mathbb{N}$ such that

$$x^7 \equiv 2 \pmod{79}.$$

(b) Let p be an odd prime. You are given the fact that any primitive root mod p is a quadratic non-residue (NR). Find the number of NRs mod 83 that are not primitive roots mod 83.

(c) Let $g, m \in \mathbb{N}$ be such that $\gcd(g, m) = 1$. Show that g is a primitive root modulo m if and only if

$$g^{\varphi(m)/p} \not\equiv 1 \pmod{m}$$

for every prime divisor p of $\varphi(m)$. (Here φ is the Euler φ-function.)

Q4 Let p be a prime such that $p \equiv 4 \pmod 7$.

(a) Prove that there exists an $\alpha \in \mathbb{Z}$ such that $\alpha^2 \equiv -7 \pmod p$.

(b) Prove that we can choose $x, y \in \mathbb{Z}$, $(x, y) \neq (0, 0)$, such that $x^2 + 7y^2 \equiv 0 \pmod p$ and such that $|x|, |y| < \sqrt{p}$.

(c) Prove that

$$x^2 + 7y^2 = p$$

has a solution $(x, y) \in \mathbb{Z}^2$.