Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2024	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:	

ED01/2024

SECTION A

Q1 Let ϕ denote the Euler ϕ function.

1.1 Compute $\phi(2500)$.

1.2 Find a solution $0 \leq x < 2500$ such that

$$7^{5004} \equiv x \pmod{2500}.$$

1.3 Show that 884 can be written as a sum of two squares, and find $a, b \in \mathbb{Z}$ such that $884 = a^2 + b^2$.

Q2 **2.1** Find the smallest solution $x \in \mathbb{N}$ to the system of congruences

$$x \equiv 13 \pmod{16}$$
$$x \equiv 2 \pmod{11}.$$

2.2 Find the smallest solution $x \in \mathbb{N}$ such that

$$365x \equiv 4 \pmod{337}.$$

Show all work involved.

SECTION B

Q3 **3.1** Determine $\mathrm{ord}_{17}(2)$. Justify your answer.

3.2 Show that if $a \in \mathbb{N}$ is such that $2^a + 2$ is divisible by 17 then $a \equiv 5 \pmod{8}$.

3.3 Find all $m \in \mathbb{N}$ such that $2^{2^m+1} + 2$ is divisible by 17.

Q4 **4.1** Determine whether the congruence $x^2 + 10x - 19 \equiv 0 \pmod{101}$ is solvable.

4.2 Determine all the primes p such that $\left(\frac{3}{p}\right) = +1$. (This should be expressed as one or more congruence conditions for p.)

4.3 Let $p \equiv 3 \pmod{4}$ be a prime. Let $a \in \mathbb{Z}$ satisfy $\mathrm{ord}_p(a) = (p-1)/2$. Show that $-a$ is a primitive root modulo p.
(*Hint:* Consider separately the cases that $\mathrm{ord}_p(-a)$ is odd and even. Note that $(p-1)/2$ is the largest positive divisor of $p-1$, besides $p-1$ itself; you should prove this.)