Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2023	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:	

ED01/2023

SECTION A

Q1 **1.1** Solve the congruence $458z \equiv 3 \pmod{129}$. (Show all steps involved.)

1.2 Find a solution $x \in \mathbb{Z}$, $0 \le x < 132$ to the system of congruences

$$x \equiv 7 \pmod{12}$$
$$x \equiv 5 \pmod{11}.$$

1.3 Let $a, b \in \mathbb{N}$, satisfying $\gcd(a, b) = 1$. Let d denote $\gcd(2a + b, a - b)$. Show that $d|3$. Give an example of a pair (a, b) with $d = 1$, and an example of a pair with $d = 3$.

Q2 **2.1** Can 1666 be represented as a sum of two squares $a^2 + b^2$, with $a, b \in \mathbb{Z}$? Justify your answer.

2.2 Find two different representations $c^2 + d^2 = a^2 + b^2 = 325$, where a, b, c, d are non-negative integers, and $\{a, b\}$ is not the same set as $\{c, d\}$.

2.3 Show that 105 is a quadratic residue modulo 991. You may use without proof that 991 is a prime. (Show all steps involved.)

SECTION B

Q3 Given $n \in \mathbb{N}$, let $\phi(n)$ denote the value of Euler's ϕ function at n, i.e., $\phi(n)$ is the number of elements in the set $\{1 \leq a \leq n : \gcd(a, n) = 1\}$.

3.1 Compute $\phi(1260)$. (Show all steps involved.)

3.2 Let $a, b \in \mathbb{N}$. Show that if $a|b$ then $\phi(a)|\phi(b)$.

3.3 Find the last digit of $3^{7^{101}}$. (Show all steps involved.)

3.4 Show that $x^{92} \equiv 6 \pmod{31}$ has no solutions.
(*Hint*: Use a similar argument as for the previous part to reduce the problem to solving a quadratic congruence.)

Q4 **4.1** Determine the number of primitive roots modulo 101.

4.2 Show that for any $1 \leq a \leq 100$ that is *not* a primitive root, the order $\text{ord}_{101}(a)$ of a modulo 101 either divides 50 or divides 20.

4.3 Show that 2 is a primitive root modulo 101.
(*Hint*: Compute $2^{50} \pmod{101}$ using Euler's criterion. Use that calculation to show that $2^{20} \not\equiv 1 \pmod{101}$ also.)

4.4 Show that $2^a \equiv 2^b \pmod{101}$ if, and only if, $a \equiv b \pmod{100}$. Note that there are two directions to prove here.