Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2021	MATH2617-WE01

Title:

Elementary Number Theory II

Time (for guidance only):	2 hours	
Additional Material provided:		
Materials Permitted:		
Calculators Permitted:	Yes	Models Permitted: There is no restriction on the model of calculator which may be used.

Instructions to Candidates:	Credit will be given for your answers to all questions. All questions carry the same marks. Please start each question on a new page. Please write your CIS username at the top of each page. To receive credit, your answers must show your working and explain your reasoning.

Revision:	

ED01/2021

Q1 **1.1** Prove that 11 divides $467^{754} + 134^{421}$. *(You must use only pen and paper calculations.)*

1.2 Determine whether the number 2021^{2021} is the sum of two squares.

1.3 Find all natural numbers n such that $\varphi(17n) = 17\varphi(n)$, where φ is the Euler φ-function. *(You must prove that all of the integers you find are solutions and that there are no other solutions.)*

Q2 **2.1** Let $m, n, i \in \mathbb{N}$ be such that $\gcd(m, n) = 1$. Show that the set

$$R = \{km + i \mid k = 0, 1, \dots, n-1\}$$

is a complete set of residues mod n.

2.2 Find all the solutions $x \in \mathbb{N}$ with $x < 77$ of the congruence $x^2 \equiv 64 \pmod{77}$. *(Your solution should at some point use the Chinese Remainder Theorem. Just trying all $x = 1, 2, \dots, 76$ will not count.)*

2.3 Prove that for all solutions $x, y \in \mathbb{N}$ of the Pell equation $x^2 - 22y^2 = 1$, we have

$$\left| x - y\sqrt{22} \right| < 0.003.$$

Q3 In this question φ is the Euler φ-function, as usual.

3.1 Let $a, m \in \mathbb{N}$ be such that $\gcd(a, m) = 1$. Show that m divides $\varphi(a^m - 1)$ for $a > 1$. *(Hint: Think about the order of the number a modulo some other number.)*

3.2 Suppose that r is a primitive root mod m. Let $e, f \in \mathbb{N}$. Show that $r^e \equiv r^f \pmod{m}$ if and only if $e \equiv f \pmod{\varphi(m)}$.

3.3 Find all the solutions $x \in \mathbb{N}$ to the congruence $6^x \equiv 11 \pmod{17}$. *(You must use a method. Simply using trial and error with $x = 1, 2, \dots$ will not count.)*

3.4 Let $a, m \in \mathbb{N}$ be such that $\gcd(a, m) = 1$. Suppose that a primitive root mod m exists. Let $n \in \mathbb{N}$. Show that $x^n \equiv a \pmod{m}$ has a solution if and only if

$$a^{\varphi(m)/d} \equiv 1 \pmod{m},$$

where $d = \gcd(n, \varphi(m))$.

Q4 **4.1** Let p and q be two distinct primes such that $p \equiv q \equiv 3 \pmod{4}$. Show that if $x^2 \equiv p \pmod{q}$ has no solutions, then $x^2 \equiv q \pmod{p}$ has exactly two distinct solutions mod p.

4.2 Let p be an odd prime and let $a, b \in \mathbb{Z}$ be such that $a^2 - 4b \not\equiv 0 \pmod{p}$. Prove that the congruence

$$x^2 + ax + b \equiv 0 \pmod{p}$$

has either no solutions or two distinct solutions mod p. *(Note: No square roots or non-integers are allowed in congruences.)*

4.3 Let p be a prime such that $p \equiv 1 \pmod{6}$ and let $a \in \mathbb{N}$ be such that $\gcd(p, a) = 1$. Show that the congruence $x^3 \equiv a \pmod{p}$ has either no solutions or three distinct solutions mod p.