Durham University

EXAMINATION PAPER

Examination Session:	Year:	Exam Code:
May/June	2026	MATH2617-WE01

Title: Elementary Number Theory II

Time:	2 hours	
Additional Material provided:	None	
Materials Permitted:	None	
Calculators Permitted:	No	Models Permitted: Use of electronic calculators is forbidden.

Instructions to Candidates:	Answer all questions. The indicative marks shown in brackets for the main parts of each question are given as a guide to the weighting the markers expect to apply. Write your answer in the white-covered answer booklet with barcodes. Begin your answer to each question on a new page.

Revision:	

ED01/2026

SECTION A

1. (a) Use the Euclidean algorithm to find the greatest common divisor d of 618 and 479, and determine $x, y \in \mathbb{Z}$ such that $618x + 479y = d$. **[4]**

(b) Determine the number of positive integers $1 \leq k \leq 245$ that are coprime to 245. **[3]**

(c) Determine whether or not the congruence $x^2 \equiv 125 \pmod{73}$ has a solution. **[3]**

---

2. (a) Find the least positive integer in the residue class of 3^{1999} modulo 17. State any results you use. **[3]**

(b) Show that for any odd integer n there are no primitive Pythagorean triples (x, y, z) where $y = 2n$. **[3]**

(c) Find two representations of the integer $85 = a^2 + b^2 = c^2 + d^2$, such that a, b, c and d are positive integers, and $\{a, b\}$ and $\{c, d\}$ are distinct sets. **[4]**

SECTION B

3. Throughout this problem, let p be an odd prime.

(a) State the definition of a primitive root modulo p. **[2]**

(b) Show that if a is a primitive root modulo p then it must be a quadratic non-residue modulo p. **[4]**

(c) Show that g is a primitive root modulo p if and only if, whenever q is a prime factor of $p-1$, $g^{(p-1)/q} \not\equiv 1 \pmod{p}$. **[6]**

(d) Show that 3 is a primitive root modulo $p = 17$. **[3]**

---

4. We define the *Möbius function* to be the function defined on positive integers via $\mu(1) = 1$, and for $n > 1$,

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by } p^2 \text{ for some prime } p \\ (-1)^k & \text{if } n = p_1 \cdots p_k \text{ with all } p_i \text{ distinct.} \end{cases}$$

(a) Compute the following values: i) $\mu(12)$; ii) $\mu(6)$; iii) $\mu(102)$. **[3]**

(b) Show that for every prime p we have $\mu(p) = -1$ and $\mu(p^k) = 0$ for all $k \geq 2$. **[2]**

(c) Show that for every $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$ we have $\mu(mn) = \mu(m)\mu(n)$. Furthermore, find an example to show that this condition fails when $\gcd(m,n) \neq 1$. **[3]**

(d) Let $n > 1$ and write its prime factorisation as $n = p_1^{a_1} \cdots p_k^{a_k}$. Show that if $d|n$ and $\mu(d) \neq 0$ then $d|p_1 \cdots p_k$. **[2]**

(e) Prove that if $n > 1$ then $\sum_{d|n} \mu(d) = 0$.
(Hint: If $p_1, \ldots, p_k$ are the prime divisors of n then note that the subsets S of $\{1, \ldots, k\}$ are in bijection with divisors $d|n$ via $S \mapsto d(S) := \prod_{j \in S} p_j$.) **[5]**
