UNIVERSITY COLLEGE LONDON

University of London

EXAMINATION FOR INTERNAL STUDENTS

For The Following Qualifications:-

B.Sc. *M.Sci.*

Mathematics C333: Theory Of Numbers I

COURSE CODE	:	**MATHC333**
UNIT VALUE	:	**0.50**
DATE	:	**07-MAY-03**
TIME	:	**10.00**
TIME ALLOWED	:	**2 Hours**

03-C0915-3-90

TURN OVER

All questions may be attempted but only marks obtained on the best **four** *solutions will count.*
The use of an electronic calculator is **not** *permitted in this examination.*

1. (a) Show that the greatest common divisor of two integers a and b (not both 0) is the smallest positive integer of the form $ax + by$ where x and y are integers.

   (b) Find two integers x and y such that $571x + 111y = 1$.

   (c) State the theorem about division with remainder. What is the input, and the output, of the division with remainder algorithm? What is the size of the input?

   (d) Assume a, b are natural numbers. Determine which of the conditions $a^2|b^2$ and $a^2|b^3$ imply $a|b$.

2. (a) State and prove the fundamental theorem of arithmetic.

   (b) Assume a, b, c are positive integers with $ab = 284$ and $bc = 497$. What are the possible values of abc?

   (c) Show that there are arbitrarily large gaps between consecutive primes.

   (d) Give the definition of the least common multiple of two natural numbers a, b. Show that the least common multiple divides every common multiple.

3. (a) What is a reduced residue system mod m where m is a positive integer? Define Euler's φ function and determine $\varphi(1998)$.

   (b) State and prove Wilson's theorem.

   (c) Let Q denote the set of integers that can be written as sum of two squares. State the characterization theorem for Q. Is $2002 \in Q$?

   (d) What are the last two digits of the number 2^{300}?

4. (a) Let a, b, m be positive integers. State the theorem on the solutions of the congruence $ax \equiv b \bmod m$.

   (b) Find all solutions to the system of congruences

$$x \equiv 5 \bmod 7, \ x \equiv 7 \bmod 11.$$

   (c) Assume p is a prime and $(a, p) = 1$. State the theorem on the number of solutions to the congruence $x^n \equiv a \bmod p$.

   (d) Show that 5 is a primitive root mod 23. Solve the congruence $x^7 \equiv 2\ (23)$.

5. (a) Define the order of a mod m. Show that if $a^k \equiv 1 \bmod m$, then k is divisible by the order of a mod m.

   (b) Define the Legendre symbol $(\frac{a}{p})$. Show that $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$ provided p is a prime and a, b are integers.

   (c) State the law of quadratic reciprocity. How many solutions are there to the congruence $2x^2 \equiv 56 \bmod 101$?

   (d) Give the definition of a multiplicative function. For $n \in N$ let $f(n)$ be equal to the product of the primes that appear in the canonical representation of n. Show that $f(n)$ is multiplicative.