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	:	**15-MAY-02**
TIME	:	**10.00**
TIME ALLOWED	:	**2 hours**

02-C0913-3-90

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) State and prove the theorem about division with remainder.

   (b) Assume a, b are positive integers with $a > b$. Show that when dividing a by b the remainder is less than $a/2$.

   (c) Find two integers x and y such that $3273x + 527y = 1$.

   (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.

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

   (b) Assume a, b, c are positive integers with $ab = 171$ and $bc = 495$. What are the possible values of abc?

   (c) Show that the number of primes in $\{1, 2, \ldots, n\}$ is at least $\frac{1}{2} \ln n$.

   (d) Define the Legendre symbol $(\frac{a}{p})$. Determine whether the congruence

$$x^2 + 2x \equiv 12 \bmod 101$$

   has a solution or not.

3. (a) Define the inverse of $a \bmod m$. Show that the inverse exists and is unique if $(a, m) = 1$. What is the inverse of the inverse of $a \bmod m$?

   (b) Assume p is a prime which is congruent to $3 \bmod 4$ and a, b are integers. Show that if p divides $a^2 + b^2$, then p divides both a and b.

   (c) Let Q denote the set of integers that can be written as sum of two squares. State the characterization theorem for Q. Is $999 \in Q$?

   (d) Use the strong prime test base 2 to show that 341 is not a prime.

4. (a) State and prove the Chinese remainder theorem.
   (b) Find all solutions to the system of congruences

$$x \equiv 3 \bmod 10, \; x \equiv 5 \bmod 14.$$

   (c) Define Euler's φ function. State and prove the formula for $\varphi(n)$ when $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is the canonical representation of n assuming that φ is multiplicative.
   (d) Show that $n^7 - n$ is divisible by 42 for every integer n.

5. (a) Let $f(x)$ be a polynomial with integral coefficients. Assume p is a prime. Define the degree, d, of the congruence $f(x) \equiv 0 \bmod p$. Show that the congruence has at most d solutions $\bmod p$.
   (b) Assume a, b, m are natural numbers with $(a, m) = 1$ and $(b, m) = 1$. Assume the order of $a \bmod m$ is h and the order of $b \bmod m$ is k, and $(h, k) = 1$. Show that the order of $ab \bmod m$ is hk.
   (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) How many primitive roots are there $\bmod 37$? Is 5 a primitive root $\bmod 23$?