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	:	**25-MAY-04**
TIME	:	**14.30**
TIME ALLOWED	:	**2 Hours**

04-C0923-3-100

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 fundamental theorem of arithmetic.
   (b) Letting $\pi(x)$ denote the number of primes $p \leqslant x$, prove that $\pi(x) \geqslant \log(x) - 1$.
   (c) Show that there can be arbitrarily large gaps between consecutive primes.

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

$$\begin{aligned} x &\equiv 2 \pmod 5, \\ x &\equiv 5 \pmod 7, \\ x &\equiv 3 \pmod 8. \end{aligned}$$

   (c) Find all solutions to the congruence $x^2 + 4x + 3 \equiv 0 \pmod{15}$.

3. (a) Let $f(x)$ be a polynomial with integer coefficients, and let p be a prime. Show that there exists a polynomial $g(x)$, with integer coefficients and of degree at most $p-1$, such that $f(x) \equiv 0 \pmod p$ and $g(x) \equiv 0 \pmod p$ have exactly the same solutions.
   (b) Define the term *primitive root* modulo a prime p. Show that $3^8 \equiv -1 \pmod{17}$, and hence that 3 is a primitive root modulo 17.
   (c) Solve, if possible, the congruences $x^{12} \equiv 16 \pmod{17}$ and $x^{11} \equiv 9 \pmod{17}$.

4. (a) Define Euler's *totient function* φ. What does it mean to say that φ is multiplicative?

   (b) If

$$n = \prod_{i=1}^{k} p_i^{\alpha_i},$$

   where the p_i are distinct primes and the α_i are positive integers, state and prove a formula for $\varphi(n)$ in terms of the p_i and α_i. (It may be assumed that φ is multiplicative.)

   (c) Show that, if $(a,n) = 1$ and $\{x_1, \ldots, x_r\}$ is a reduced residue system modulo n, then so is $\{ax_1, \ldots, ax_r\}$. Hence prove Euler's theorem.

5. (a) Let p be a prime. Show that $x^2 \equiv -1 \pmod p$ is soluble if $p \equiv 1 \pmod 4$, but is insoluble if $p \equiv 3 \pmod 4$. (Any results assumed must be clearly stated.)

   (b) Let $p \equiv 1 \pmod 4$ be a prime. Show that p can be expressed in the form $p = a^2 + b^2$, with a and b integers.

   (c) Define the *Legendre symbol* $(\frac{a}{p})$. Determine whether or not the congruence $x^2 + 4x \equiv 7 \pmod{101}$ has a solution. (Any results assumed must be clearly stated.)