UNIVERSITY COLLEGE LONDON

EXAMINATION FOR INTERNAL STUDENTS

MODULE CODE : **MATH3701**

ASSESSMENT PATTERN : **MATH3701A**

MODULE NAME : **Theory Of Numbers I**

DATE : **25-May-10**

TIME : **10:00**

TIME ALLOWED : **2 Hours 0 Minutes**

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) What is the input, what is the output of the division with remainder algorithm? What is the size of the input? Assume $a, b \in \mathbb{N}$ and $a > b$. Show that when dividing a by b the remainder is smaller than $a/2$.
   (b) Show that the number of primes in $\{1, 2, \ldots, n\}$ is at least $\frac{1}{2} \log n$.
   (c) Define Euler's ϕ function. For which values of $n \in \mathbb{N}$ is $\phi(3n) = 3\phi(n)$?

2. (a) Assume $x, y, z \in \mathbb{N}$ and $xy = 124$ and $yz = 292$. What are the possible values of xyz?
   (b) Give the definition of a reduced residue system mod m. Show that if $(a, m) = 1$ and $r_1, \ldots, r_s$ is a reduced residue system mod m, then so is $ar_1, \ldots, ar_s$. Is $a + r_1, \ldots, a + r_s$ a reduced residue system mod m, too?
   (c) Let a, b, m be positive integers. State and prove the theorem on the solutions of the congruence $ax \equiv b \bmod m$.

3. (a) Let Q denote the set of integers that can be written as the sum of two squares. State the characterization theorem for Q. Show that if p is a prime with $p \equiv 3 \bmod 4$ and $p | a^2 + b^2$ with $a, b \in \mathbb{Z}$, then $p|a$ and $p|b$.
   (b) Let $f(x)$ be a polynomial with integral coefficients. Define the degree of the congruence $f(x) \equiv 0 \bmod m$. Show that if p is a prime and $d|p - 1$ ($d \in \mathbb{N}$), then $x^d - 1 \equiv 0 \bmod p$ has exactly d solutions.
   (c) Find all solutions to the congruence $x^3 + x^2 + 29 \equiv 0 \bmod 5^3$.

4. (a) Define the Legendre symbol $\left(\frac{a}{p}\right)$. Assume p is a prime with $p \equiv 3 \bmod 4$. Show that for all $a \in \mathbb{N}$ the congruence $x^2 \equiv a \bmod p$ has either no solution or its solutions are $\pm a^{(p+1)/4}$.

   (b) Give the definition of the order of $a \bmod m$ and the definition of a primitive root $\bmod m$. Is 2 or 5 a primitive root mod 19? Show that if the order of $a \bmod m$ is h, and the order of $b \bmod m$ is k, then the order of $ab \bmod m$ divides hk.

   (c) Give the definition of a multiplicative function. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ be the canonical representation of $n \in N$ with all $\alpha_i \geq 1$. Show that the function $f(n) = p_1 p_2 \dots p_k$ is multiplicative.

5. (a) State the law of quadratic reciprocity. How many solutions are there to the congruence $3x^2 \equiv 66 \bmod 107$?

   (b) Give the definition of the simple finite continued fraction. Find the value of the infinite continued fraction $[1; 2, 3, 2, 3, 2, 3, ...] = [1, \overline{2, 3}]$.

   (c) State Dirichlet's theorem on Diophantine approximation and use it to show that every prime p with $p \equiv 1 \bmod 4$ can be written as sum of two squares.