UNIVERSITY COLLEGE LONDON

EXAMINATION FOR INTERNAL STUDENTS

MODULE CODE : **MATH3701**

ASSESSMENT PATTERN : **MATH3701A**

MODULE NAME : **Theory Of Numbers I**

DATE : **15-May-08**

TIME : **14:30**

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) Show that there are arbitrarily large gaps between consecutive primes.
   (b) Suppose $k, n \in \mathbb{N}$ and $k \geq 2$. Show that if $\sqrt[k]{n}$ is rational, then n is the kth power of an integer.
   (c) What is the input and the output of the squaring and reducing algorithm? What is the size of the input? Give an upper bound, as a function of the size of the input, on the number of iterations this algorithm can take. Determine the last two digits of 11^{201}.

2. (a) Give the definition of a reduced residue system $\bmod m$. Show that if $(a, m) = 1$ and $r_1, \ldots, r_s$ is a reduced residue system $\bmod m$, then so is $ar_1, \ldots, ar_s$.
   (b) State and prove Wilson's theorem.
   (c) Assume p is a prime. Show that there are integers a, b such that $a^2 + b^2 \equiv 2 \bmod p$.

3. (a) Define the Möbius function $\mu : \mathbb{N} \to \{-1, 0, 1\}$. Using the fact that $\sum_{d|n} \mu(d) = 0$ for all $n \geq 2$, $n \in \mathbb{N}$, prove that $\left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2}\right)\left(\sum_{k=1}^{\infty} \frac{1}{k^2}\right) = 1$.
   (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, then $f(x) \equiv 0 \bmod p$ cannot have more solutions $\bmod p$ than its congruence degree.
   (c) Let Q denote the set of integers that can be written as sum of two squares. Assume $n \in \mathbb{N}$. Does $n \equiv 1 \bmod 4$ imply that $n \in Q$? Does $n \equiv -1 \bmod 4$ imply that $n \notin Q$?

4. (a) Define the Legendre symbol $\left(\frac{a}{p}\right)$. Show that the congruence $x^2 \equiv 3 \bmod 47$ has two solutions. Can you find these solutions explicitly?

   (b) Give the definition of the order of $a \bmod m$. Show that $a^k \equiv 1 \bmod m$ if and only if k is a multiple of the order of $a \bmod m$. What is the order of 3 and $5 \bmod 23$?

   (c) State and prove the theorem on the number of solutions to the congruence $x^n \equiv a \bmod p$ where $a, n, p \in \mathbb{N}$, p is a prime and $(a, p) = 1$.

5. (a) Solve the congruence $x^3 - x^2 \equiv 4 \bmod 7^3$.

   (b) State the key lemma to the RSA public key cryptosystem. Explain how authentification works.

   (c) State Dirichlet's theorem on Diophantine approximation. Find the value of the infinite continued fraction $[0; 1, 2, 1, 2, 1, 2, ...] = [0; \overline{1, 2}]$.