UNIVERSITY COLLEGE LONDON

University of London

EXAMINATION FOR INTERNAL STUDENTS

For The Following Qualifications:-

B.Sc. *M.Eng.* *M.Sci.*

Mathematics C333: Theory Of Numbers I

COURSE CODE	:	**MATHC333**
UNIT VALUE	:	**0.50**
DATE	:	**22-MAY-06**
TIME	:	**14.30**
TIME ALLOWED	:	**2 Hours**

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 divison with remainder algorithm? What is the size of the input? Prove an upper bound on the number of elementary operations taken by the algorithm.

   (b) Give the definition of the least common multiple, $[a, b]$, of two numbers $a, b \in \mathbb{N}$. Show that $(a, b)[a, b] = ab$ where (a, b) denotes the greatest common divisor of a and b.

   (c) Assume $x, y, z \in \mathbb{N}$ and $xy = 124$, $xz = 292$. What are the possible values of xyz?

2. (a) Assume p is a prime, $a_1, \dots, a_k \in \mathbb{N}$, and $p|a_1 \dots a_k$. Show that $p|a_i$ for some i.

   (b) State and prove the fundamental theorem of arithmetic.

   (c) Use the sequence $F(n) = 2^{2^n} + 1$, $(n = 0, 1, 2, \dots)$ to show that there are infinitely many primes.

3. (a) Define the inverse of a mod m. Prove that the inverse exists and is unique if $(a, m) = 1$. What is the inverse of 17 mod 105?

   (b) 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 q is a prime which is congruent to 3 mod 4, then $q \notin Q$.

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

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

   $$x \equiv 7 \bmod 12, \ \mathrm{x} \equiv 4 \bmod 15.$$

   (b) Determine the last two digits of the number 2^{300}.

   (c) Assume $f(x)$ is a polynomial with integral coefficients, and for $m \in \mathbb{N}$ let $N_m(f)$ denote the number of solutions to the congruence $f(x) \equiv 0$ mod m. Show that $N_m(f)$ is a multiplicative function.

5. (a) Define the order of a mod m. Show that if the order of a mod m is h and $k \in \mathbb{N}$, then the order of a^k is $h/(h,k)$.

(b) State and prove Euler's criterion. How many solutions are there to the congruence $2x^2 \equiv 46 \bmod 103$?

(c) State and prove the Lemma of Gauss on quadratic residues.

END OF PAPER