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-05**
TIME	:	**10.00**
TIME ALLOWED	:	**2 Hours**

05-C0926-3-120
© 2005 University College London

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. What is the input, and the output, of the division with remainder algorithm? What is the size of the input?

   (b) Give the definition of the least common multiple of two natural numbers a and b. Show that it divides every common multiple of a and b.

   (c) State and prove the fundamental theorem of arithmetic. Determine which of the conditions $a^3|b^2$ and $a^2|b^3$ imply $a|b$, assuming that a, b are natural numbers.

2. (a) Define the inverse of $a \bmod m$. Prove that the inverse exists and is unique if $(a, m) = 1$. What is the inverse of $23 \bmod 82$?

   (b) State and prove Wilson's theorem.

   (c) Define Euler's φ function. State and prove the formula for $\varphi(n)$ in terms of the canonical representation of n assuming that φ is multiplicative. Determine $\varphi(2004)$.

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

   (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 a and b.

   (c) Let Q denote the set of integers that can be written as the sum of two squares. State the characterization theorem for Q. Is $2004 \in Q$?

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

$$x \equiv 5 \bmod 12, \ x \equiv 2 \bmod 9.$$

(b) Solve the congruence $x^3 + x + 57 \equiv 0 \bmod 125$.

(c) State and prove the key lemma of the RSA cryptosystem.

5. (a) Give the definition of the order of $a \bmod m$. Show that the order of $a \bmod m$ divides $\phi(m)$ if $(a, m) = 1$. Is 5 a primitive root mod 23?

(b) Define the Legendre symbol $(\frac{a}{p})$. State and prove Euler's criterion. Use it to show that $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$ provided p is a prime and a, b are integers.

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