EASTERN UNIVERSITY, SRI LANKA

THIRD EXAMINATION IN SCIENCE 2003/2004

SECOND SEMESTER (JUNE/JULY' 2005)

(Repeat)

MT 309 - NUMBER THEORY

Answer all questions

Time: Two hours

1. (a) Define the greatest common divisor, $\gcd(a, b)$, of two integers a and b, not both zero.

   (b) Use the Euclidean algorithm to find the greatest common divisor d of 198, 288 and 512. Hence find the integers x, y and z which satisfy the equation $d = 198x + 288y + 512z$.

   (c) Prove that for any nonzero integers a and b, $\text{lcm}(a, b) \times \gcd(a, b) = ab$.

   (d) Define the greatest integer $[x]$ of a real number x and show that $[x] + 1 = [x + 1]$.

2. (a) Prove that if a, b and c are three nonnegative integers, where a and c are relatively prime and if $c \mid ab$ then $c \mid b$.

   (b) Show that the linear Diophantine equation $ax + by = c$ has solutions if and only if $\gcd(a, b)$ divides c.

   Further, let x_0, y_0 be any particular solution of this equation. Show that all other solutions are given by $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$ for each integer t, where $d = \gcd(a, b)$.

   (c) A certain number of sixes and nines are added to give a sum of 126; if the number of sixes and nines are interchanged, the new sum is 114. How many of each were there originally?

3. Define Euler's $\phi-$ function for any nonnegative integer n.

(a) State Euler's theorem and use it to prove $n^p \equiv n(\text{mod } p)$ for any integer n and any prime p.

(b) If $\gcd(a, m) = \gcd(a-1, m) = 1$ then prove that $1 + a + a^2 + \ldots + a^{\phi(m)-1} \equiv 0(\text{mod } m)$.

(c) If p is a prime number such that $p \equiv 1(\text{mod } 4)$ then using Wilson's theorem prove that $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1(\text{mod } p)$.

(d) Prove that the linear congruence $ax \equiv b(\text{mod } m)$ has solutions if and only if $d \mid b$, where $d = \gcd(a, m)$.

Further, show that if $d \mid b$ it has d mutually incongruent solutions modulo m.

(e) Find a complete set of mutually incongruent solutions of $3x \equiv 6(\text{mod } 15)$.

4. (a) If $a \equiv b(\text{mod } m_1)$ and $a \equiv b(\text{mod } m_2)$ then show that $a \equiv b(\text{mod } m_1 m_2)$, where $\gcd(m_1, m_2) = 1$.

(b) Define a *pseudoprime* and show that there are infinitely many pseudoprimes to the base 2.

(You may use the result that if d and n are natural numbers and $d \mid n$ then $(2^d - 1) \mid (2^n - 1)$).

(c) Define Carmichael numbers and show that 6601 is a Carmichael number.

(d) If a belongs to the exponent h modulo m and if $a^r \equiv 1(\text{mod } m)$ then show that $h \mid r$.

(e) If a belongs to the exponent h modulo m and if $\gcd(k, h) = d$ then show that a^k belongs to the exponent $\frac{h}{d}$ modulo m.