EASTERN UNIVERSITY, SRI LANKA

THIRD EXAMINATION IN SCIENCE 2005/2006

March/April' 2008

SECOND SEMESTER

MT 309 - NUMBER THEORY

(Proper)

Time:Two hours

Answer all questions

Q1. Define the greatest common divisor $\gcd(a,b)$ of two non zero integers a and b.

(a) Use the Euclidean algorithm to find the greatest common divisor d of 42823 and 6409. Hence find a pair of integers which satisfy $42823x + 6409y = d$.

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

(c) The least common multiple of two positive integers a and b,denoted by $\text{lcm}(a,b)$, is defined to be the smallest positive integer that is divisible by both a and b.

Prove that:

i. $\text{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$,

ii. if a and b are non negative integers then $\gcd(a,b)$ divides $\text{lcm}(a,b)$.

(d) Explain whether it is possible to have 100 coins made of c cents, d dimes and q quarters, be worth exactly 5 rupees.

(Here 1 dime=10 cents, 1 quarter=25 cents).

Q2. (a) State and prove the Euler's theorem.

(b) Show that if $\gcd(m,n) = 1$ then $m^{\phi(n)} + n^{\phi(m)} \equiv 1(\text{mod } mn)$.

(c) If $a \equiv b(\text{mod } m_1)$ and $a \equiv b(\text{mod } m_2)$ then show that $a \equiv b(\text{mod } m_1m_2)$, where $\gcd(m_1,m_2) = 1$.

(d) Show that if p is prime then $(p-1)! \equiv (p-1)(\text{mod } 1+2+3+....(p-1))$.

Q3. (a) Prove that if p is odd prime, then

i. $1^p + 2^p + 3^p + ...(p-1)^p \equiv 0(\text{mod } p)$,

ii. $1^{p-1} + 2^{p-1} + 3^{p-1} + ...(p-1)^{p-1} \equiv -1(\text{mod } p)$.

(b) Using Wilson's theorem, prove that $1^2 3^2 5^2 ....(p-2)^2 \equiv (-1)^{\frac{p+1}{2}}(\text{mod } p)$ for any odd prime.

(c) If p is prime and congruent to 1 modulo 4, then show that $\left(\frac{(p-1)!}{2}\right)^2 \equiv -1(\text{mod } p)$.

Q4. Define the following:

- Pseudo Prime,
- Carmichael number.

(a) Prove that if $n = q_1 q_2 .... q_k$, where q_j's are distinct primes that satisfy $q_j - 1$ divides $(n-1)$ for all j, then n is carmichael number.

(b) Show that $2821 = 7 \times 13 \times 31$ is a carmichael number using

i. the definition;

ii. the above part.

(c) Show that $645 = 3 \times 5 \times 43$ is a pseudo prime to the base 2.

(d) Define the term "Primitive Root".

If a belongs to the exponent h modulo m and suppose that $a^r \equiv 1(\text{mod } m)$ then prove that h divides r.

(e) Prove that, if $a^b \equiv 1(\text{mod } m)$ for some integer b it is necessary and sufficient that $\gcd(a, m)$=1.