28|2

06 NOV 2015
EASTERN UNIVERSITY, SRI LANKA

EASTERN UNIVERSITY, SRI LANKA

DEPARTMENT OF MATHEMATICS

EXTERNAL DEGREE

THIRD EXAMINATION IN SCIENCE - 2008/2009

SECOND SEMESTER (Feb./Apr., 2015)

EXTMT 309 - NUMBER THEORY

Answer all questions **Time : Two hours**

---

1. (a) Define what is meant by the *greatest common divisor*, $gcd(a, b)$, of two integers a and b, not both zero.

   Find the $gcd(119, 272)$.

   (b) For any positive integers a, b and c prove that

   i. $lcm(a, b)\ gcd(a, b) = ab$.

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

   iii. If a abd b are two odd integers. Prove that $8|(a^2 - b^2)$.

   (c) A man buys horses and cows for a total amount of Rs. 17,700. If a horse cost Rs. 310 and a cow cost Rs. 200 then find the number of horses and cows that can be bought.

2. Define what is meant by the *Euler's ϕ - function* for any non-negative integer n.

   (a) State and prove the *Euler's Theorem.*

   (b) State and prove the *Fermat Little Theorem.*

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

   (d) State the *Willson's Theorem*, and use it to prove that if p is prime and $p \equiv 1(\text{mod } 4)$ then $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (-1)(\text{mod } p)$.

3. Define what it means by the following terms:

   - *Pseudo Prime*;
   - *Carmichael number.*

   (a) If $d, n \in \mathbb{N}$ and $d|n$ then show that $(2^d - 1)|(2^n - 1)$.

   (b) 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, the n is Carmichael number.

   (c) Show that $6601 = 7 \times 23 \times 41$ is a Carmichael number by using

      i. the definition;

      ii. the part(b).

   (d) Show that 645 is a psedo prime to the base 2.

4. Define what is meant by the following:

   - an integer a belongs to the exponent h modulo m;
   - a primitive root.

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

   (b) If g is a primitive root modulo m then $g, g^2, ..., g^{\phi(m)}$ are mutually incongruent and form reduced residue system mod m.

   (c) If a belongs to the exponent h modulo m and $\gcd(k, h) = d$ then a^k belongs to the exponent h/d modulo m.