EASTERN UNIVERSITY, SRI LANKA

DEPARTMENT OF MATHEMATICS

EXTERNAL DEGREE EXAMINATION IN SCIENCE - 2008/2009

THIRD YEAR SECOND SEMESTER (April/May, 2016)

EXTMT 309 - NUMBER THEORY

(REPEAT)

Answer all Questions Time: Two hours

Q1. (a) Define what it means by the *greatest common divisor* gcd(a, b) of two integers a and b, not both zero.

Find the gcd$(3270, 729)$.

(b) Show that the square of any odd integer is of the form $8k + 1$, where k is an integer.

(c) A customer bought a dozen piece of fruit apple and orange for Rs 1.32. If an apple cost 3 cents more than an orange and more apples than oranges purchased, then determine how many pieces of each kind were bought.

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

(b) State and prove the *Fermat's Little theorem.*

(c) Prove that if n is relatively prime to 72, then n^{12}=1(mod 72).

(d) Prove that $1 + a + a^2 + ... + a^{\phi(m)-1} \equiv 0 (\text{mod } m)$ if $gcd(a, m) = 1$, $gcd(a - 1, m) = 1$.

Q3. Define what are meant 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) Show that 561=3.11.17 is a pseudo prime to the base 2 and a car number.

(c) If $n = q_1 q_2, ..., q_k$, where q_js are distinct primes that satisfy $(q_j - 1)|(n$ all j, then prove that n is a Carmichael number.

Q4. (a) State what are meant by saying

(i) an integer a belongs to the exponent h modulo m;

(ii) an integer g is called a primitive root modulo m.

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

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