EASTERN UNIVERSITY, SRI LANKA
DEPARTMENT OF MATHEMATICS
THIRD EXAMINATION IN SCIENCE - 2011/2012
SECOND SEMESTER (June, 2016)
PM 309 - NUMBER THEORY
(SPECIAL 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 $\gcd(42823, 6409)$.

(b) Prove that $[x] + 1 = [x + 1]$ for any real number x.

(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 $n^{12} \equiv 1 (\text{mod } 72)$.

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

Q3. (a) Define what are meant by the following terms:

Pseudo Prime;

Carmichael Number;

Show that 561 is a pseudo prime to the base 2 and carmichael number.

(b) Show that there are infinitely many pseudo primes to the base 2.

(c) If p is a prime≥ 5, then show that $p^2 \equiv 1 (\text{mod } 12)$.

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 mu 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.