# EASTERN UNIVERSITY, SRI LANKA
## DEPARTMENT OF MATHEMATICS
## THIRD EXAMINATION IN SCIENCE - 2012/2013
## SECOND SEMESTER (Sep./Oct., 2015)
## PM 309 - NUMBER THEORY
## (PROPER & 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 $\gcd(1071, 462)$.

(b) Prove that if $k$ is odd, then $2^{n+2}$ divides $k^{2^n} - 1$ for all natural numbers $n$.

(c) A customer bought a dozen piece of fruits 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 $n^{12} \equiv 1 (mod\ 72)$.

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

Q3. Define what is meant by the following terms:

* *Pseudo Prime*;
* *Carmichael Number.*

Show that 561=3.11.17 is a Carmichael number and pseudo prime to the base 2.

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

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

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

Q4. (a) State what is 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 mutually incongruent and form reduced residue system modulo $m$.

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