# EASTERN UNIVERSITY, SRI LANKA

## DEPARTMENT OF MATHEMATICS

## THIRD EXAMINATION IN SCIENCE - 2014/2015

## SECOND SEMESTER (Dec., 2017/Jan., 2018)

## PM 309 - NUMBER THEORY

---

**Answer all questions** **Time : Two hours**

---

1. (a) i. Show that the linear Diophantine equation $ax + by = c$ has a solution if and only if $d|c$, where $d = gcd(a, b)$.

   Let $x_0, y_0$ be any particular solution of this equation then show that all the other solutions are given by $x = x_0 + \frac{b}{d}t$, $y = y_0 - \frac{a}{d}t$ for each $t \in \mathbb{Z}$.

   ii. Clara wants to buy pizza and cola to her family for Rs. 4000. If she know that each pizza cost Rs. 570 and each bottle of cola cost Rs. 220, how many pizzas and bottles of cola she can buy?

   (b) Let $a$ and $n$ be positive integers with $a > 1$. Prove that, if $a^n + 1$ is prime, then $a$ is even and $n$ is a power of 2.

2. (a) Let $a, b, a_i, b_i \in \mathbb{Z}$ and $m, k \in \mathbb{N}$. Prove the following:

   i. if $a \equiv b(\text{mod } m)$ then $a^k \equiv b^k(\text{mod } m)$;

   ii. if $a_i \equiv b_i(\text{mod } m)$ $\forall\ i$ then $\sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i(\text{mod } m)$.

   (b) i. If $P(x) = \sum_{i=0}^{n} c_i x^i$ is a polynomial, where $c_i \in \mathbb{Z}$ and $a \equiv b(\text{mod } m)$ then prove that $P(a) \equiv P(b)(\text{mod } m)$.

   ii. If an integer $M$ is formed by reversing the order of digits of another number $N$ then show that $N - M$ is divisible by 9.

(c) A band of 17 pirates stole a sack of gold coins and agreed to share the coins equally. Unfortunately, it was found that there is a remainder of 3 coins when all had equal shares. In the fight for extra coins one of them was killed. When they tried to divide the coins among the rest, there ware 10 extra coins. Again another pirate got killed in the fight for these extra coins. Now the remaining members were able to have equal shares. What was the least number of coins that would have been given to each pirates.

3. (a) State the Euler's theorem.

Hence, prove the Fermat's little theorem: if $p$ is a prime then $n^p \equiv n(\text{mod } p)$ for any integer $n$.

(b) i. Show that $a^{p-1} - b^{p-1}$ is divisible by the prime $p$.

ii. Find the remainder when $314^{160}$ is divided by 165.

iii. Solve the congruence $x^{103} \equiv 4(mod\ 11)$.

4. (a) Define the following:

i. pseudoprime;

ii. Carmichael number;

iii. primitive root.

(b) Show that 341 is a psedoprime to the base 2.

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

(d) Show that 6601 is a Carmichael number using:

i. the definition;

ii. the above part (c).