EASTERN UNIVERSITY, SRI LANKA

DEPARTMENT OF MATHEMATICS

THIRD EXAMINATION IN SCIENCE - 2008/2009

SECOND SEMESTER (Sep./Nov., 2010)

MT 309 - NUMBER THEORY

Answer all questions **Time : Two hours**

---

1. State the *division algorithm.*

   (a) For any integer a, show that:

   i. $3 \mid a(a+1)(a+2)$;

   ii. $3 \mid a(2a^2+7)$;

   iii. if a and b are both odd integers then $16 \mid (a^4+b^4-2)$.

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

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

   ii. A certain number of sixes and nines are added to give the sum of 126; if the number of sixes and nines are interchanged, the new sum is 114. How many of each were there originally?

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

   i. if $a \equiv b (\text{mod } m)$ and $c \equiv d (\text{mod } m)$ then $ac \equiv bd (\text{mod } m)$;

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

(b) i. If $P(x) = \sum_{k=0}^{n} c_k x^k$ be a polynomial, where $c_k \in \mathbb{Z}$ 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 $9 \mid (N - M)$.

(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 equally among the rest, there were 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 pirate.

3. (a) State and prove 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) If p is a prime grater than equal to 5 then show that $p^2 \equiv 1(\text{mod } 12)$.

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

(d) State Wilson's theorem.

Let p be a prime such that $p \equiv 1(\text{mod } 4)$. Prove that

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv (\text{mod } p).$$

4. (a) Define the following:

i. pseudoprime;

ii. Carmichael number.

(b) If $n = q_1 q_2 q_3 ... q_k$, where q_j's are distinct prime such that $(q_j - 1) \mid (n - 1)$ for all j then prove that n is a Carmichael number.

(c) Show that 2821 is a Carmichael number by using:

i. the definition;

ii. the above part (b).

(d) Find the remainder when 314^{160} is divide by 165.