EASTERN UNIVERSITY, SRI LANKA

THIRD EXAMINATION IN SCIENCE - 2013/2014

SECOND SEMESTER (October, 2017)

PM 309 - NUMBER THEORY

(SPECIAL REPEAT)

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. Write 100 as the sum two summands one of which is divisible by 7 and the other by 11.

   (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. Prove that any palindrome with even number of digits is divisible by 11.

(c) Solve the following simultaneous system of linear congruences:

$$\begin{aligned} x &\equiv 1 (\text{mod } 3) \\ x &\equiv 3 (\text{mod } 5) \\ x &\equiv 5 (\text{mod } 7). \end{aligned}$$

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. Find the remainder when $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ is divided by 7.

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

4. (a) Define the following:

   i. pseudoprime;

   ii. Carmichael number;

   iii. primitive root.

   (b) 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.

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

   i. the definition;

   ii. the above part (b).

   (d) Find all primitive roots modulo 8.