EASTERN UNIVERSITY, SRI LANKA

DEPARTMENT OF MATHEMATICS

SPECIAL REPEAT EXAMINATION IN SCIENCE - 2007/2008

THIRD YEAR, FIRST AND SECOND SEMESTER (Feb., 2010)

MT 309 - NUMBER THEORY

Answer all Questions | Time: Two hours

---

1. (a) Define the **greatest common divisor**, $gcd(a, b)$, of two integers a and b, not both zero.

   Find the $gcd(341, 527)$.

   (b) Show that the square of any odd integer is of the form $8k + 1$, where k is an integer.

   (c) 1000 glasses are packed in two types of boxes. There are 172 boxes in first type and 20 in second type. If each type contains a fixed number of glasses, find the number of glasses in each type.

2. (a) State and prove the **Euler's theorem**.

   (b) State and prove the **Fermat's Little theorem**.

   (c) Varify that $5^{38} \equiv 4(mod\ 11)$.

   (d) If $a \equiv 2(mod\ 17)$, $b \equiv 4(mod\ 17)$ and $c \equiv 5(mod\ 17)$, then find the least positive residue of $a^2 + b^2 + c^2$ modulo 17.

3. (a) Define the following:

   (i) pseudoprime;

   (ii) carmichael number.

   (b) Show that if $n = q_1 q_2 \dots q_k$ where the q_j's are distinct primes that satisf
   $(q_j - 1) \mid (n-1)$ for all j, then n is a carmichael number.

   (c) Show that $2821 = 7 \times 13 \times 31$ is a carmichael number using

   (i) Fermat's Little theorem,

   (ii) part (b).

   (d) Show that $561 = 3 \times 11 \times 17$ is a pseudoprime to the base 2.

4. (a) Define the following:

   (i) an integer a belongs to the exponent h modulo m;

   (ii) an integer g is called a primitive root modulo m.

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

   (c) Let a be any odd integer. Prove that $a^{2n-2} \equiv 1 (mod\ 2^n)$ for all $n \geq 3$.

   (d) Show that if $F_n = 2^{2^n} + 1$, $n > 1$, is prime, then 2 is not a primitive root
   F_n. Discuss the case when $n = 1$.