EASTERN UNIVERSITY, SRI LANKA
THIRD EXAMINATION IN SCIENCE (2007/2008)
SECOND SEMESTER(December/January, 2008)
MT 309 - NUMBER THEORY
(SPECIAL REPEAT)

Answer all Questions **Time: Two hours**

Q1. (a) State the *Euclid's Lemma.*

(b) If a and b are two integers. Prove that $8/a^2 - b^2$.

(c) If p is a prime and a is an integer such that p does not divide a, then prove that p and a are relatively prime.

(d) If p is prime, show that $\sqrt{p}$ is irrational.

(e) If $n \geq 3$, prove that $f_n > \alpha^{n-2}$.

Q2. (a) If $n = q_1 q_2 \ldots\ldots q_r$ with q_i distinct primes that satisfy $(q_i - 1)/(n-1)$ for all i, then prove that n is a carmichael number.

(b) Prove that the quadratic congruence $x^2 + 1 \equiv 0(mod\ p)$. where p is an odd prime, has a solution if and only if $p \equiv 1(mod 4)$.

(c) Solve that $6x \equiv 15(mod 21)$.

(d) What is the remainder when 5^{48} is divided by 12.

(e) Find the general solution $39x - 56y = 11$.

Q3. (a) State and prove the *Euler's Theorem.*

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

(c) If $a \equiv b(mod\ m_1)$ and $a \equiv (mod\ m_2)$, where $gcd(m_1, m_2) = 1$ then show th $a \equiv b(mod\ m_1 m_2$.

(d) Show that if p is prime then$(p-1)! \equiv (p-1)(mod\ ! + 2 + ...(p-1))$.
Use : $(p-1)! \equiv -1(mod\ p)$.

Q4. (a) Prove that if p is an odd prime, then

i $1^p + 2^p + ... + (p-1)^p \equiv 0(mod\ p)$.

ii $1^{p-1} + 2^{p-1} + ... + (p-1)^{p-1} \equiv -1(mod\ p)$.

(b) Using *Wilson's Theorem*,prove that $1^2 3^2 5^2 .....(p-2)^2 = (-1)^{\frac{p-1}{2}}(mod\ p)$ f any odd prime.
Use : $k = -(p-k)(mod\ p)$.

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