

EASTERN UNIVERSITY, SRI LANKA

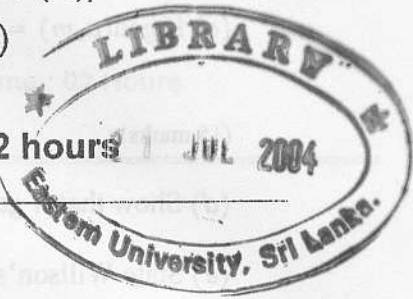
THIRD EXAMINATION IN SCIENCE (2002/03 & 2002/03 (A))

(Second Semester - February / March 2004)

Number Theory - MT 309

Answer all questions

Time allowed: 2 hours



Q1.

(a) Define the greatest integer $[x]$ of a real number x and show that $0 \leq [2x] - 2[x] \leq 1$. (25 marks)

(b) If p ($1 \leq p \leq n$) and n (> 2) are relatively prime then prove that $\gcd(n-p, n) = 1$. (20 marks)

(c) Prove that the Linear Diophantine Equation $ax + by = c$ has a solution if and only if $d \mid c$ where $d = \gcd(a, b)$. Further show that if (x_0, y_0) is a solution then the set of all solutions are given by $(x_0 + \frac{bt}{d}, y_0 - \frac{at}{d})$, $t \in \mathbb{Z}$ [35 marks]
(You may assume that if $d = \gcd(a, b)$ then $\gcd(\frac{a}{d}, \frac{b}{d}) = 1$)

(d) Find the shortest possible distance between two lattice points on the line defined by $ax - by = c$ [20 marks]

Q2.

(a) If $a = t_1^{g_1} t_2^{g_2} \dots t_r^{g_r}$ and $b = t_1^{h_1} t_2^{h_2} \dots t_r^{h_r}$ then $\gcd(a, b) = t_1^{c_1} t_2^{c_2} \dots t_r^{c_r}$ and $\text{lcm}(a, b) = t_1^{d_1} t_2^{d_2} \dots t_r^{d_r}$, where each c_i and d_i are the minimum and maximum of g_i and h_i respectively. Use this result (without proof) to show that

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}$$

(30 marks)

(b) If p and q are two distinct primes, then show that \sqrt{pq} is irrational. (20 marks)

(c) Define the Fibonacci sequence f_n (10 marks) and prove that

(i) $f_n > \alpha^{n-2}$ for $n \geq 2$, where $\alpha = \frac{1 + \sqrt{5}}{2}$, (20 marks)

(ii) $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$, for $n \geq 1$. (20 marks)

Q3.

(a) Define Euler's ϕ function $\phi(n)$ for any nonnegative integer n and show that

$\omega(n) < \phi(n)$, where $\omega(n)$ denotes the number of primes $\leq n$ that does not divide n . (20 marks)

(b) State Euler's Theorem and use it to prove $n^p \equiv n \pmod{p}$ for any integer n , any prime p . (20 marks)

(c) If $\gcd(a, m) = \gcd(a - 1, m) = 1$ then prove that

$$1 + a + a^2 + \dots + a^{\phi(m)-1} \equiv 0 \pmod{m}.$$

(15 marks)

(d) Show that if $\gcd(m, n) = 1$ then $m^{\phi(n)} + n^{\phi(m)} \equiv 1 \pmod{mn}$. (20 marks)

(e) State Willson's Theorem and use it to prove if $p \equiv 1 \pmod{4}$ then

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

(25 marks)

Q4.

(a) If $a \equiv b \pmod{m_1}$ and $a \equiv b \pmod{m_2}$ then show that $a \equiv b \pmod{m_1 m_2}$, where $\gcd(m_1, m_2) = 1$. (20 marks)

(b) Define a *pseudoprime* and show that there are infinitely many pseudoprimes to the base 2.

(You may use the result that if d and n are natural numbers and $d \mid n$ then $(2^d - 1) \mid (2^n - 1)$). (30 marks)

(c) Define Carmichael numbers and show that 2821 is a Carmichael number (20 marks)

(d) If a belongs to the exponent h modulo m and if $a^r \equiv 1 \pmod{m}$ then show that $h \mid r$. (15 marks)

(e) If a belongs to the exponent h modulo m and if $\gcd(k, h) = d$ then show that a^k belongs to the exponent $\frac{h}{d}$ modulo m . (15 marks)