MAS3008

UNIVERSITY OF EXETER

SCHOOL OF ENGINEERING, COMPUTER SCIENCE AND MATHEMATICS

MATHEMATICAL SCIENCES

NUMBER THEORY

May/June 2006

Time allowed: 2 HOURS.

Examiner: Dr M.J. Craven

This is a CLOSED BOOK examination.

The mark for this module is calculated from 75% of the percentage mark for this paper plus 25% of the percentage mark for associated coursework.

Answer Section A (50%) and any TWO of the three questions in Section B (25% for each).

Marks shown in questions are merely a guideline. Candidates are permitted to use approved portable electronic calculators in this examination.

SECTION A

1. (a) State (without proof) the *Chinese Remainder Theorem.* Find the general solution of each of the following systems of simultaneous congruences:

$$(i)\begin{cases} x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases};\ (ii)\begin{cases} x \equiv 10 \pmod{33} \\ x \equiv 8 \pmod{46} \end{cases}.$$

(12)

(b) State (without proof) the *Law of Quadratic Reciprocity.* Write down the values of the Legendre symbols $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ for an odd prime p. Compute the following Legendre symbols, showing all working:

(i) $\left(\frac{32}{199}\right)$; (ii) $\left(\frac{1066}{2011}\right)$.

(Note: $1066 = 2 \times 13 \times 41$.) (9)

(c) Prove there are infinitely many primes p satisfying $p \equiv -1 \pmod{6}$. (8)

(d) Find four essentially distinct representations of $9805 = 5 \times 37 \times 53$ as a sum of two squares of natural numbers.

(Recall that representations $n = a^2 + b^2 = c^2 + d^2$ where $a, b, c, d \in \mathbb{N}$ are essentially distinct unless $a = c$ and $b = d$, or $a = d$ and $b = c$.) (11)

(e) Find all solutions of the congruence

$$x^2 + x + 7 \equiv 0 \pmod{3^3}.$$

(10)

[50]

SECTION B

2. Let p be a prime and let a be an integer such that $a \not\equiv 0 \pmod{p}$.

   (a) Prove *Fermat's Little Theorem*; in other words, under the above assumptions
   $$a^{p-1} \equiv 1 \pmod{p}.$$
   (7)

   (b) Give the definition of Euler's *totient function* ϕ. Suppose that m, n are coprime and show that a is coprime to mn if and only if a is coprime to both m and n. (8)

   (c) Write down a formula giving $\phi(n)$ in terms of the prime factorisation of n. Hence find all solutions of the following equations (where any solutions exist):
   (i) $\phi(n) = 10$; (ii) $\phi(n) = 3$; (iii) $\phi(n) = 8$. (10)

   [25]

3. (a) Describe Pollard's Rho method for factorising a given integer n. Your description should include a clear step-by-step description of the algorithm, together with a brief explanation of why it works. The algorithm may be expressed in pseudocode, as MAPLE code or some other computer language if you wish. (Assume that a subroutine is available to compute the greatest common divisor of two integers.) Explain the roles of the input parameters and how the algorithm may terminate. (9)

   (b) Let an iteration function be $f(x) = x^2+1$ and the seed be $x_0 = 1$. Apply Pollard's Rho method to find a proper factor of $n = 9287$. [It should take four steps.] (6)

   (c) Change the seed to $x_0 = 24$ and otherwise apply Pollard's Rho method as in part (b). How many steps does the algorithm take to find a proper factor of n? Does the proper factor found by the algorithm change? If it does, then what proper factor is found? (6)

   (d) Explain why Pollard's Rho method fails when the iteration function $f(x) = x^2 - 2$ and the seed $x_0 = 1$ are chosen.
   [Take n to be as in part (b) of this question.] (4)

   [25]

4. (a) Let $S_2 = \{a^2+b^2 : a, b \in \mathbb{Z}\}$ be the set of all sums of two squares. Prove that if $m, n \in S_2$ then $mn \in S_2$. (6)

(b) State (without proof) a necessary and sufficient condition for a number $n \in \mathbb{N}$ to be expressible as the sum of two squares, $n = a^2 + b^2$ where $a, b \in \mathbb{Z}$.

Hence which of the numbers $n = 8, 41, 42, 45, 77$ are expressible as the sum of two squares? For each n that is, express it as a sum of two squares. (10)

(c) Let p be a prime such that $p \equiv 3 \pmod 4$. Prove there exist $u, v \in \mathbb{Z}$ such that $u^2 + v^2 + 1 \equiv 0 \pmod p$.

Hence find appropriate $u, v \in \mathbb{Z}$ such that $u^2 + v^2 + 1 \equiv 0 \pmod p$ for each of $p = 7$ and $p = 19$. (9)

[25]