MAS3008

UNIVERSITY OF EXETER

SCHOOL OF ENGINEERING, COMPUTER SCIENCE & MATHEMATICS

DEPARTMENT OF MATHEMATICAL SCIENCES

NUMBER THEORY

8 June 2005

9:30 a.m. – 11:30 a.m.
Duration: 2 hours

Examiner: Dr R.J. Chapman

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.

Calculators labelled as approved by the Department of Mathematical Sciences may be used.

SECTION A

1. (a) Find the general solution of the following system of simultaneous congruences:

$$\begin{cases} 10x & \equiv & 51 \pmod{91}, \\ 111x & \equiv & 63 \pmod{195}. \end{cases}$$

(10)

(b) Prove that there infinitely many primes p satisfying $p \equiv 5 \pmod{6}$. (10)

(c) Calculate $\varphi(1925)$ and find the least positive residue of 6^{6006} modulo 1925.
(NB $1925 = 5^2 \times 7 \times 11$). (8)

(d) Find all solutions of the congruence

$$x^3 \equiv 1 \pmod{169}.$$

(NB $169 = 13^2$). (10)

(e) Evaluate the following Legendre symbol

$$\left(\frac{1066}{2011}\right).$$

(4)

(f) Find four essentially distinct representations of $3445 = 5 \times 13 \times 53$ 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, $d \in \mathbf{N}$ are essentially distinct unless $a = c$ and $b = d$, or $a = d$ and $b = c$.) (8)

[**50**]

SECTION B

2. (a) Define Euler's phi-function φ. Prove Euler's generalization of Fermat's theorem, namely that if a is coprime to the natural number n then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

(You may assume this consequence of the Euclidean algorithm: if m and n are coprime integers then there exist integers r and s with $rm + sn = 1$.) (9)

(b) Let $n = pq$, where p and q are distinct primes, and suppose that r is a positive integer coprime to $\varphi(n)$. Show that there is a positive integer s such that

$$b \equiv a^r \pmod{n} \qquad \text{implies} \qquad a \equiv b^s \pmod{n}$$

for all a coprime to n. Prove that this implication also holds when a is an integer divisible by p.

(You may assume the formula expressing $\varphi(n)$ in terms of the prime factorization of n.) (9)

(c) Let t be a positive integer with the property that $6t + 1$, $12t + 1$ and $18t + 1$ are all prime. Prove that

$$m = (6t + 1)(12t + 1)(18t + 1)$$

is a Carmichael number, that is, $a^{m-1} \equiv 1 \pmod{m}$ for all integers a which are coprime to m. (7)

[25]

3. (a) Let p be an odd prime. Euler's criterion for the Legendre symbol states that

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Using Euler's criterion, prove Gauss's Lemma: this states that if a is not divisible by p then

$$\left(\frac{a}{p}\right) = (-1)^r$$

where r is the number of integers j in the interval $(0, p/2)$ such that aj is congruent modulo p to an integer in the interval $(p/2, p)$. (10)

(b) Using Gauss's Lemma prove that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Deduce that if q is a prime factor of $12m^2 - 1$ then $q \equiv \pm 1 \pmod{12}$ and hence prove that there are infinitely many primes q with $q \equiv \pm 1 \pmod{12}$. (15)

[25]

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

(b) Let p be a prime with $p \equiv 1 \pmod{4}$ and u be a number with $u^2 \equiv -1 \pmod{p}$. By applying the pigeonhole principle to the set

$$A = \{(a, b) : a, b \in \mathbf{Z}, 0 \leq a, b < \sqrt{p}\}$$

and the function $(a, b) \mapsto ua + b$, prove that there are integers c and d with $p = c^2 + d^2$. (10)

(c) Let $S_3 = \{a^2 + b^2 + c^2 : a, b, c \in \mathbf{Z}\}$ be the set of sums of three squares. Find $m \in S_3$ and $n \in S_3$ with $mn \notin S_3$. Prove that $4^k r \notin S_3$ whenever k is a nonnegative integer and $r \equiv 7 \pmod{8}$. (9)

[25]