MAS3008

UNIVERSITY OF EXETER

SCHOOL OF MATHEMATICAL SCIENCES

NUMBER THEORY

11 June 2002

9:30 a.m. – 12:30 p.m.
Duration: 3 hours

Examiner: Dr N.P. Byott

The marks from Section A (40%) and the best THREE questions in Section B (20% for each) will be recorded.

Marks shown in questions are merely a guideline.

Approved calculators of the following type may be used Casio fx82 series, Sharp EL521 or EL531 Series and Texas TI-30X or TI-36X.

SECTION A

1. (a) Find all solutions of each of the following congruences, or show that none exist:

   (i) $5x \equiv 12 \pmod{37}$;
   (ii) $5x \equiv 12 \pmod{35}$;
   (iii) $5x \equiv 15 \pmod{35}$;
   (iv) $x^2 \equiv -1 \pmod{221}$;
   (v) $x^2 \equiv 2 \pmod{265}$;
   (vi) $x^5 \equiv 2 \pmod{31}$.

   [Hint for part (iv): $221 = 13 \cdot 17$.] (15)

   (b) State (without proof) the Law of Quadratic Reciprocity, including the values of the Legendre symbols $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ for an odd prime number p. Evaluate the following Legendre symbols, showing your working and justifying each intermediate step:

   $$\text{(i)}\ \left(\frac{7}{53}\right); \qquad \text{(ii)}\ \left(\frac{19}{59}\right); \qquad \text{(iii)}\ \left(\frac{-39}{97}\right).$$

   (9)

   (c) Show that 3 is a primitive root modulo 43, but that 2 is not. How many incongruent primitive roots are there modulo 43? How many are there modulo 43^2? Find one of the primitive roots modulo 43^2. (9)

   (d) Find all integer solutions to the following Diophantine equations:

   (i) $x^2 + 17y = -2$;
   (ii) $x^2 - y^2 = 35$.

   (7)

   [**40**]

SECTION B

2. (a) Give an account of the Miller-Rabin primality test. Your account should include a clear step-by-step description of the algorithm, together with a brief explanation of why it works. You may express the algorithm in pseudocode, or as a procedure in MAPLE or some other computer language, if you wish. [Assume that subroutines are available to compute the greatest common divisor of two integers, and to compute $a^k \bmod n$ for given integers a, k, n with $k, n \geq 1$.] Explain the roles of the various input parameters, and the various ways in which the algorithm may terminate, indicating what conclusions may be drawn in each case. (10)

   (b) Illustrate your answer to part (a) by applying the Miller-Rabin test to $n = 1729$ using base $a = 2$. What conclusion can you draw? (4)

   (c) What does it mean to say that a number n is a *Carmichael number*? Show that the number $561 = 3 \cdot 11 \cdot 17$ is a Carmichael number. Show also that if n is any Carmichael number and p is a prime dividing n then $p - 1$ must divide $n - 1$. [Any general results you use should be clearly stated, but need not be proved.] (6)

[**20**]

3. (a) Define Euler's totient function φ. Given that $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $\gcd(m, n) = 1$, derive a formula for $\varphi(n)$ in terms of the prime factorisation of n. (4)

   (b) In each of the following cases, find all natural numbers n (if there are any) such that:

   (i) $\varphi(n) = 22$;
   (ii) $\varphi(n) = 23$;
   (iii) $\varphi(n) = 24$. (8)

   (c) Now let $\tau(n)$ denote the number of positive divisors of n. Show that $\tau(mn) = \tau(m)\tau(n)$ whenever $\gcd(m, n) = 1$. Hence obtain a formula for $\tau(n)$ in terms of the prime factorisation of n, and prove that

   (i) for any $k \geq 2$ there are infinitely many natural numbers n with $\tau(n) = k$;
   (ii) if $\tau(n)$ is prime then n must be a prime power. (7)

[**20**]

4. (a) Let p be an odd prime. Give the definitions of the terms *quadratic residue* and *quadratic non-residue mod* p, and define the Legendre symbol $\left(\frac{a}{p}\right)$. (4)

(b) State and prove Euler's Criterion which gives the value of $\left(\frac{a}{p}\right)$. Deduce that

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

for any integers a, b. (8)

(c) Use Euler's Criterion to deduce the value of $\left(\frac{-1}{p}\right)$ for an odd prime p. (3)

(d) Let $p_1, p_2, \ldots, p_r$ be primes of the form $8k+5$, and set $N = (p_1 p_2 \ldots p_r)^2 + 4$. Show that every prime factor of N is congruent mod 8 to either 1 or 5. Hence show that there are infinitely many primes of the form $8k+5$. (7)

[**20**]

5. (a) State without proof a necessary and sufficient condition for a prime number p to be a sum of two squares. (2)

(b) Using the result of part (a), prove that a natural number n is a sum of two squares if and only if $v_q(n)$ is even for every prime $q \equiv 3 \pmod 4$. [Here $v_q(n)$ is the exponent of the largest power of q dividing n; thus $v_q(n) = e$ if q^e divides n but q^{e+1} does not.] (9)

(c) The number $12325 = 5^2 \cdot 17 \cdot 29$ has exactly 6 inequivalent representations as a sum of 2 squares. Find them all. [If $n = a^2 + b^2$ then the 8 expressions $(\pm a)^2 + (\pm b)^2$ and $(\pm b)^2 + (\pm a)^2$ for n are considered to be equivalent.] (6)

(d) Deduce from the result of part (a) that if p is prime and $p \equiv 1 \pmod 4$ then p can be written in the form $p = 4a^2 + b^2$. (3)

[**20**]