MAT3434

UNIVERSITY OF EXETER

SCHOOL OF MATHEMATICAL SCIENCES

NUMBER THEORY

26 May 1999

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. Find all solutions to each of the following congruences, or show that none exist:

   (a) $x^2 \equiv -1 \pmod{77}$; (2)

   (b) $x^2 \equiv -1 \pmod{185}$; (3)

   (c) $x^2 \equiv 3 \pmod{13^3}$; (5)

   (d) $x^3 + 2x \equiv 2 \pmod{7^2}$; (6)

   (e) $x^8 \equiv -1 \pmod{41}$; (2)

   (f) $x^{21} \equiv 7 \pmod{41}$. (2)

   [**20**]

2. (a) Show that there are infinitely many primes p such that $p \equiv 3 \pmod{4}$. (4)

   (b) Let p be an odd prime. Define the terms *quadratic residue* modulo p and *quadratic non-residue* modulo p. Show that, among the integers a with $1 \leq a \leq p-1$, there are the same number of quadratic residues and quadratic non-residues modulo p. (5)

   (c) Define the Legendre symbol $\left(\dfrac{a}{p}\right)$, where p is an odd prime and a is any integer. State (without proof) the values of the Legendre symbols $\left(\dfrac{-1}{p}\right)$ and $\left(\dfrac{2}{p}\right)$. Use the law of quadratic reciprocity to evaluate the following Legendre symbols, showing your working and justifying each intermediate step:

   $$\text{(i) } \left(\frac{6}{29}\right); \qquad \text{(ii) } \left(\frac{21}{41}\right); \qquad \text{(iii) } \left(\frac{-22}{59}\right); \qquad \text{(iv) } \left(\frac{101}{103}\right).$$

   (11)

   [**20**]

SECTION B

3. (a) Let a be a fixed integer, and let $n > 1$ be a composite integer. What does it mean to say that n is:

   (i) a *pseudoprime* to base a;

   (ii) a *Carmichael number.*

   Show that if n is a pseudoprime both to base a and to base b, then it is also a pseudoprime to base ab. Deduce that n is a Carmichael number if and only if n is a pseudoprime to base p for every prime $p < n$ which does not divide n. (7)

   (b) Give an account of the Miller-Rabin primality test for an integer n using a given base a. This should include a clear step-by-step account of the algorithm, together with a brief outline of why the test works. You may express the algorithm in pseudocode, or as a procedure in MAPLE or some other computer language, if you wish. Indicate the various points at which the algorithm may terminate, and what can be deduced in each case (in particular, whether a proper factor of n can be obtained). You may assume that subroutines are available to compute $a^k \pmod{n}$ for $k \geq 0$, and to compute the gcd of two integers. (10)

   (c) Illustrate your answer to part (b) by applying the Miller-Rabin test to $n = 449$ with base $a = 2$. What conclusion can you draw? (3)

   [20]

4. (a) Define Euler's totient function φ, and show that $\varphi(p^e) = p^{e-1}(p-1)$ when p is prime and $e \geq 1$. Write down (without proof) a formula giving $\varphi(n)$ in terms of the prime factorization of n. Hence find all solutions of each of the following equations:

   (i) $\varphi(n) = 46$;

   (ii) $\varphi(n) = 8$;

   (iii) $\varphi(n) = \frac{1}{2}n$. (10)

   (b) Let g be an integer, and let p be a prime not dividing g. What does it mean to say that g is a *primitive root* modulo p?

   Let $n \geq 1$ and let a be an integer such that $\gcd(a, p) = 1$, where again p is a prime. Using the fact that a primitive root modulo p exists, show that the congruence $x^n \equiv a \pmod{p}$ can be solved for x if and only if $a^{(p-1)/d} \equiv 1 \pmod{p}$ with $d = \gcd(n, p-1)$. (5)

   (c) Let p be a prime such that $p \equiv 2 \pmod{3}$. Show that for every integer a, the congruence $x^3 \equiv a \pmod{p}$ has exactly one solution modulo p. Given that 2 is a primitive root modulo 59, and that $10 \equiv 2^7 \pmod{59}$, solve the congruence $x^3 \equiv 10 \pmod{59}$. (5)

   [20]

5. (a) State and prove Euler's criterion on the Legendre symbol $\left(\dfrac{a}{p}\right)$, where p is an odd prime. [Any standard facts you use should be clearly stated, but need not be proved.] Apply Euler's criterion to evaluate $\left(\dfrac{-1}{p}\right)$ for all odd primes p. (7)

(b) State the law of quadratic reciprocity relating the Legendre symbols $\left(\dfrac{p}{q}\right)$ and $\left(\dfrac{q}{p}\right)$ for distinct odd primes p, q. Use it to evaluate $\left(\dfrac{3}{p}\right)$ for all odd primes p. (4)

(c) For $n \geq 1$, let $F_n = 2^{2^n} + 1$ be the nth Fermat number. Show that if F_n is prime then

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}. \qquad (*)$$

(5)

(d) Prove conversely that if $(*)$ holds then F_n is prime, by first showing that the order of 3 mod F_n is precisely $F_n - 1$. [Standard facts about the order of an integer a modulo m may be used without proof.] (4)

[20]

6. (a) Let p be an odd prime. Prove that $(p-1)! \equiv -1 \pmod{p}$. Deduce that for $r = \left(\frac{1}{2}(p-1)\right)!$ we have $r^2 \equiv -1 \pmod{p}$ if $p \equiv 1 \pmod{4}$, and $r \equiv \pm 1$ if $p \equiv 3 \pmod{4}$. (7)

(b) Prove that a prime p can be written as the sum of two squares if and only if either $p = 2$ or $p \equiv 1 \pmod{4}$. (7)

(c) Let p be a prime. Show that p^2 can be written in the form $a^2 + b^2$ for *positive* integers a, b if and only if $p \equiv 1 \pmod{4}$. Express $5329 = 73^2$ in this form. (6)

[20]