MAS3008

UNIVERSITY OF EXETER

SCHOOL OF MATHEMATICAL SCIENCES

NUMBER THEORY

15 June 2000

2:15 p.m. – 5:15 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) $x^2 \equiv -1 \pmod{65}$;

   (ii) $x^2 \equiv 4 \pmod{57}$;

   (iii) $x^2 \equiv 2 \pmod{11^3}$;

   (iv) $x^2 \equiv 3 \pmod{13^3}$. (11)

   (b) Write down a formula for $\varphi(n)$ in terms of the prime factorization of n, where n is Euler's totient function. Hence find all natural numbers n (if there are any) such that:

   (i) $\varphi(n) = 28$;

   (ii) $\varphi(n) = 26$;

   (iii) $\varphi(n) = 20$. (10)

   (c) 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:

   $$\text{(i)}\ \left(\frac{7}{23}\right); \qquad \text{(ii)}\ \left(\frac{-15}{47}\right); \qquad \text{(iii)}\ \left(\frac{26}{61}\right).$$

   (8)

   (d) Find all integer solutions to the following Diophantine equations, or show that none exist:

   (i) $17x + 29y = 8$;

   (ii) $x^2 + 7y = 2$;

   (iii) $2x^2 + 4xy + 6y^2 = 11$;

   (iv) $x^2 - 4x + y^2 - 2y = 29$. (11)

[40]

SECTION B

2. (a) Give an account of Pollard's $p-1$ method for factorizing a given integer n using a given base a. This should include a clear step-by-step account 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. Explain the roles of the various input parameters, and indicate the various ways in which the algorithm may terminate. State the likely effect of changing the parameters in the cases when the algorithm fails to find a proper factor of n.

   [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)

   (b) Illustrate your answer to part (a) by applying Pollard's $p-1$ method to $n = 2263$ with base $a = 2$ and with maximum number of iterations $k_{\max} = 6$. (5)

   (c) Without actually carrying out the algorithm, determine how many steps of the $p-1$ method would be needed to factorize $n = 71977 = 167 \times 431$.

   What would happen if you applied this method to $n = 74563 = 173 \times 431$?

   [The numbers 167, 173, 431 are all prime.] (5)

   [20]

3. (a) Define Euler's totient function φ, and show that $a^{\varphi(n)} \equiv 1 \pmod{n}$ for any natural number n and any integer a with $\gcd(a, n) = 1$.

   Briefly explain why $\varphi(mn) = \varphi(m)\varphi(n)$ whenever $\gcd(m, n) = 1$.

   Let p and q be distinct prime numbers, and let a be an integer such that $\gcd(a, p) = \gcd(a, q) = 1$. Show that

$$a^{pq-1} \equiv a^{p-1}a^{q-1} \pmod{pq}.$$

   (9)

   (b) Let p be a prime number. What does it mean to say that an integer g is a *primitive root* mod p? Show that if $\gcd(g, p) = 1$ then g is a primitive root mod p if and only if $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ for every prime factor q of $p-1$. (4)

   (c) Show that 2 is not a primitive root mod 89, but that 3 is a primitive root mod 89. Hence find all solutions (if any exist) to the following congruences:

   (i) $x^6 \equiv 9 \pmod{89}$;

   (ii) $x^{11} \equiv 27 \pmod{89}$. (7)

   [20]

4. (a) Prove that there are infinitely many prime numbers l with $l \equiv 3 \pmod 4$. (3)

(b) Let p be an odd prime number and let a be any integer. Show that if l is a prime factor of $a^{p-1} + a^{p-2} + \cdots + a + 1$ then the order of a mod l is either 1 or p. Deduce that either $l = p$ or $l \equiv 1 \pmod p$. Hence show that there are infinitely many prime numbers l such that $l \equiv 1 \pmod p$. (9)

(c) Let p be an odd prime number. By choosing an appropriate even value for a in part (b), prove that there are infinitely many prime numbers l satisfying both of the conditions

(i) $l \equiv 1 \pmod p$;

(ii) $l \equiv 3 \pmod 4$. (5)

(d) Let p be a prime number such that $p \equiv 3 \pmod 4$. Use part (c), together with the Law of Quadratic Reciprocity, to show that there are infinitely many prime numbers l such that p is a quadratic non-residue mod l. (3)

[**20**]

5. (a) State (without proof) a necessary and sufficient condition, in terms of the prime factorization, for a natural number n to be expressible as the sum of two squares, $n = a^2 + b^2$ where a, b are integers.

For each of the numbers $n = 41, 47, 49, 53, 77$, determine whether n is the sum of two squares, and if so, express n in this form.

Find two inequivalent expressions for $2173 = 41 \times 53$ as the sum of two squares. [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.] (8)

(b) Define the term *Pythagorean triple*. What does it mean to say that a Pythagorean triple is *primitive*?

Show that if (x, y, z) is a primitive Pythagorean triple then, possibly after interchanging x and y, we have

$$x = r^2 - s^2, \qquad y = 2rs, \qquad z = r^2 + s^2$$

for some natural numbers r, s, where $r > s$, $\gcd(r, s) = 1$, and exactly one of r, s is odd. (8)

(c) Deduce that, if (x, y, z) is *any* Pythagorean triple, then the product xyz is divisible by 60. (4)

[**20**]