

MAS3008

UNIVERSITY OF EXETER

SCHOOL OF MATHEMATICAL SCIENCES

NUMBER THEORY

6 June 2003

9:30 a.m. – 12:30 p.m.

Duration: 3 hours

Examiner: Dr N.P. Byott

Answer Section A (40%) and any THREE of the four questions in Section B (20% for each).

Marks shown in questions are merely a guideline.

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

SECTION A

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

(i) $7x \equiv 10 \pmod{27}$;

(ii) $7x \equiv 10 \pmod{28}$;

(iii) $9x \equiv 15 \pmod{39}$;

(iv) $x^2 \equiv 1 \pmod{91}$;

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

(16)

- (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 p . Evaluate the following Legendre symbols, showing your working and justifying each intermediate step:

(i) $\left(\frac{5}{79}\right)$; (ii) $\left(\frac{-23}{83}\right)$; (iii) $\left(\frac{21}{97}\right)$.

(9)

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

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

(ii) $\varphi(n) = 30$;

(iii) $\varphi(n) = 32$.

(9)

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

Write 53 and 89 as sums of two squares, and find two inequivalent expressions for $4717 = 53 \times 89$ as a 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.]

(6)

[40]

SECTION B

2. (a) Give an account of Pollard's Rho method for factorizing a given integer n . 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 a subroutine is available to compute the greatest common divisor of two integers.] Explain the roles of the various input parameters, and indicate the various ways in which the algorithm may terminate. (8)
- (b) Illustrate your answer to part (a) by applying Pollard's Rho method, with iteration function $f(x) = x^2 + 1$ and with initial value $x_0 = 1$, in order to find a proper factor of $n = 3293$. [You should find a factor at the 4th step.] (6)
- (c) Suppose we try to implement Pollard's Rho method, but instead of iterating a quadratic function we use the linear function $f(x) = ax + b \pmod n$, where a is chosen so that both a and $a - 1$ are invertible mod n . Show by induction on r that

$$f^{(r)}(x) = a^r x + (a^r - 1)cb \pmod n \quad \text{for } r \geq 0,$$

where $ac \equiv c + 1 \pmod n$. How many iterations would be needed to detect a prime factor p of n ? Explain why this choice of f is not a sensible one. (6)

[20]

3. (a) Show that there are infinitely many primes $l \equiv -1 \pmod 6$. (4)
- (b) Show that, for any $n \geq 3$, there are infinitely many primes $l \not\equiv 1 \pmod n$. (4)
- (c) Let p be a prime, let a be any integer, and let l be a prime factor of $a^{p-1} + a^{p-2} + \cdots + a + 1$. By considering the order of $a \pmod l$, show that either $l = p$ or $l \equiv 1 \pmod p$. Hence show that there are infinitely many primes $l \equiv 1 \pmod p$. (10)
- (d) Deduce from part (c) that, for any odd prime p , there are infinitely many primes $l \equiv 1 \pmod{2p}$. (2)
- [20]

-
4. (a) Define the term *primitive root modulo n* . Show that if a primitive root modulo n exists, then there are exactly d incongruent solutions to $x^d \equiv 1 \pmod{n}$ for each d dividing $\varphi(n)$, and that exactly $\varphi(d)$ of these have order $d \bmod n$. (Here φ denotes Euler's totient function.) (8)

- (b) Let $n \geq 3$ be a natural number such that primitive roots modulo n exist. Use the result of part (a) to find the number of incongruent primitive roots modulo n . Show that at most half of the integers a with $1 \leq a \leq n$ and $\gcd(a, n) = 1$ are primitive roots modulo n .

[You may use without proof the formula for $\varphi(m)$ in terms of the prime factorisation of m .] (8)

- (c) Find the number of incongruent solutions to each of the following congruences:

(i) $x^{15} \equiv -3 \pmod{41}$;

(ii) $x^{10} \equiv 2 \pmod{41}$.

[You are not required to find the solutions themselves. You may assume without proof that a primitive root modulo 41 exists.] (4)

[20]

5. (a) Let $n \geq 2$, and let u, v, y be nonzero integers with $y^n = uv$ and $\gcd(u, v) = 1$. By considering the powers of each prime p which occur in the prime factorisations of u and v , show that there are integers r and s such that $u = \pm r^n$ and $v = \pm s^n$. (4)

- (b) Let $x^2 + y^2 = z^2$ where x, y, z are natural numbers with x and z both odd and $\gcd(x, z) = 1$. Show that, for some natural numbers r, s we have

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

Does the same conclusion hold if $\gcd(x, z) > 1$? Justify your answer. (8)

- (c) Using part (a), show that the Diophantine equation $y^3 = 4x^2 - 1$ has a unique solution in integers, and find that solution. (8)

[20]