**MAS3008**

UNIVERSITY OF EXETER

**SCHOOL OF MATHEMATICAL SCIENCES**

# NUMBER THEORY

12 June 2001

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) $6x \equiv 17 \pmod{65}$;

   (ii) $6x \equiv 21 \pmod{69}$;

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

   (iv) $x^2 \equiv 2 \pmod{55}$;

   (v) $x^2 \equiv 2 \pmod{7^3}$;

   (vi) $x^2 + 4x \equiv 6 \pmod{13^2}$. (14)

   (b) Use the Binary Powering Algorithm to evaluate $3^{45} \bmod 577$. Show your working. (6)

   (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:

   $$\text{(i)} \left(\frac{5}{41}\right); \qquad \text{(ii)} \left(\frac{39}{79}\right); \qquad \text{(iii)} \left(\frac{-34}{109}\right).$$

   (9)

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

   (i) $15x + 23y = 7$;

   (ii) $x^2 + 11y = 5$;

   (iii) $3x^2 + 6xy^2 - 6y^4 = 1$;

   (iv) $x^2 - 4y^2 = 21$. (11)

**[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.

   If $p$ is a prime factor of $n$, roughly how many steps (on average) of the Rho method would be needed to detect it? (10)

   (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 $x_0 = 2$, in order to find a proper factor of $n = 4661$. [You should find a factor at the 4th step.] (6)

   (c) Show that if $p$ is prime then the only solution to the congruence $x^2 \equiv 1 \pmod{p}$ is $x \equiv \pm 1 \pmod{p}$. Use the fact that $748^2 \equiv 1 \pmod{8881}$ to find a proper factor of 8881. (4)

   **[20]**

3. (a) Define Euler's totient function $\varphi$, and state, without proof, a formula for $\varphi(n)$ in terms of the prime factorisation of $n$. Show that, if $m$ is a factor of $n$, then $\varphi(m)$ is a factor of $\varphi(n)$. (5)

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

   (i) $\varphi(n) = 10$;

   (ii) $\varphi(n) = 18$;

   (iii) $\varphi(n) = 26$. (9)

   (c) Now consider the following property for a natural number $n$:

$$\gcd(n, \varphi(n)) = 1. \qquad (*)$$

   Show that if $n$ is prime then $n$ satisfies property $(*)$, but that if $n = p^e$ is a prime power with $e > 1$ then $n$ does not satisfy property $(*)$. Show further that if $n$ is a composite number satisfying property $(*)$ then $n$ is a product of distinct odd primes. Is the converse true? (6)

   **[20]**

4. (a) Let $n$ be a natural number and let $a$ be an integer with $\gcd(a, n) = 1$. What does it mean to say that $a$ is a *primitive root* modulo $n$? Show that $a$ is a primitive root modulo $n$ if and only if $a^{\varphi(n)/q} \not\equiv 1 \pmod{n}$ for every prime factor $q$ of $\varphi(n)$, where $\varphi$ denotes Euler's totient function (4)

(b) Show that 2 is a primitive root modulo 19. Make a table of the powers $2^i$ mod 19 for $0 \leq i \leq 17$, and use your table to find all solutions to each of the following congruences (or to show that no solutions exist):

(i) $x^7 \equiv 5 \pmod{19}$;

(ii) $x^4 \equiv 8 \pmod{19}$;

(iii) $x^3 \equiv 11 \pmod{19}$;

(iv) $5x^{11} \equiv 13 \pmod{19}$. (10)

(c) Let $p$ be prime and let $g$ be a primitive root mod $p$. Show that either $g$ or $g + p$ is a primitive root mod $p^2$. (6)

**[20]**

5. (a) Let $p$ be an odd prime, and let $a$ be an integer not divisible by $p$. State Gauss' Lemma concerning the Legendre symbols $\left(\frac{a}{p}\right)$, and use it to evaluate the Legendre symbols $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$. (6)

(b) Let $p$ be a prime such that $p \equiv 1 \pmod{4}$. Prove that $p$ can be written as the sum of two integer squares.

Express 53 and 97 as sums of two squares, and hence find two inequivalent expressions for $5141 = 53 \times 97$ 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.] (9)

(c) Let $p$ be a prime such that $p \equiv \pm 1 \pmod{8}$. Show that $p = 2a^2 - b^2$ for some integers $a$ and $b$. (5)

**[20]**