

MAS3008

UNIVERSITY OF EXETER

**SCHOOL OF ENGINEERING, COMPUTER SCIENCE &
MATHEMATICS**

DEPARTMENT OF MATHEMATICAL SCIENCES

NUMBER THEORY

June 2004

9:30 a.m. – 11:30 p.m.
Duration: 2 hours

Examiner: Robin Chapman

*Answer Section A (50%) and any TWO of the three
questions in Section B (25% for each).*

Marks shown in questions are merely a guideline.

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

SECTION A

1. (a) Find the general solution of the following system of simultaneous congruences:

$$\begin{cases} 6x \equiv 90 \pmod{99} \\ 2x \equiv 129 \pmod{187}. \end{cases} \quad (10)$$

- (b) Find the least positive residue of

(i) 5^{2003} modulo 101;

(ii) 3^{10020} modulo 2003.

(NB 101 and 2003 are both prime.) (7)

- (c) Find all solutions of the congruence

$$x^2 \equiv 1 \pmod{1001}.$$

(NB $1001 = 7 \times 11 \times 13$) (12)

- (d) Evaluate the following Legendre symbols using the Law of Quadratic Reciprocity:

$$(i) \left(\frac{77}{101}\right); (ii) \left(\frac{277}{401}\right); (iii) \left(\frac{1215}{2003}\right). \quad (9)$$

- (e) Find four essentially distinct representations of $3145 = 5 \times 17 \times 37$ as a sum of two squares of natural numbers.

(Recall that representations $n = a^2 + b^2 = c^2 + d^2$ where $a, b, c, d \in \mathbf{N}$ are essentially distinct unless $a = c$ and $b = d$, or $a = d$ and $b = c$.) (12)

[50]

SECTION B

2. Let p be a prime, and let a be an integer with $a \not\equiv 0 \pmod{p}$.

(a) Prove *Fermat's Little Theorem*:

$$\text{under these hypotheses, } a^{p-1} \equiv 1 \pmod{p}. \quad (6)$$

(b) What is the *order* of a modulo p ? Prove that if k is the order of a modulo p and $a^m \equiv 1 \pmod{p}$ then $k \mid m$. (6)

(c) Find a number a having order 72 modulo 73. (7)

(d) Let p be a prime factor of $2^q - 1$, where q is prime. Prove that $p \equiv 1 \pmod{q}$. (6)

[25]

3. (a) Define the *Legendre symbol* and state *Euler's criterion* characterizing its value. Using Euler's criterion prove that

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ -1 & \text{if } p \equiv 3 \pmod{4}. \end{cases} \quad (6)$$

(b) Let $n \geq 2$ be an integer and let p be a prime factor of $(n!)^2 + 1$. Prove that $p > n$ and that $p \equiv 1 \pmod{4}$. Deduce that there are infinitely many primes congruent to 1 modulo 4. (8)

(c) Assuming the theorem that states

Let $a \in \mathbf{N}$ and let p and q be odd primes. If $p \equiv \pm q \pmod{4a}$ then

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

prove the Law of Quadratic Reciprocity. (11)

[25]

4. (a) What is a *primitive Pythagorean triple*? Prove that if (x, y, z) is a primitive Pythagorean triple with x odd, then there are integers r and s with $x = r^2 - s^2$, $y = 2rs$ and $z = r^2 + s^2$. (11)

(b) Find all primitive Pythagorean triples (x, y, z) with $y = 60$. (8)

(c) Prove that the equation

$$x^3 + y^3 = z^3$$

has no solutions in integers with $xyz \not\equiv 0 \pmod{3}$. (6)

[25]