

EXAMINATION FOR INTERNAL STUDENTS

MODULE CODE : MATH3701

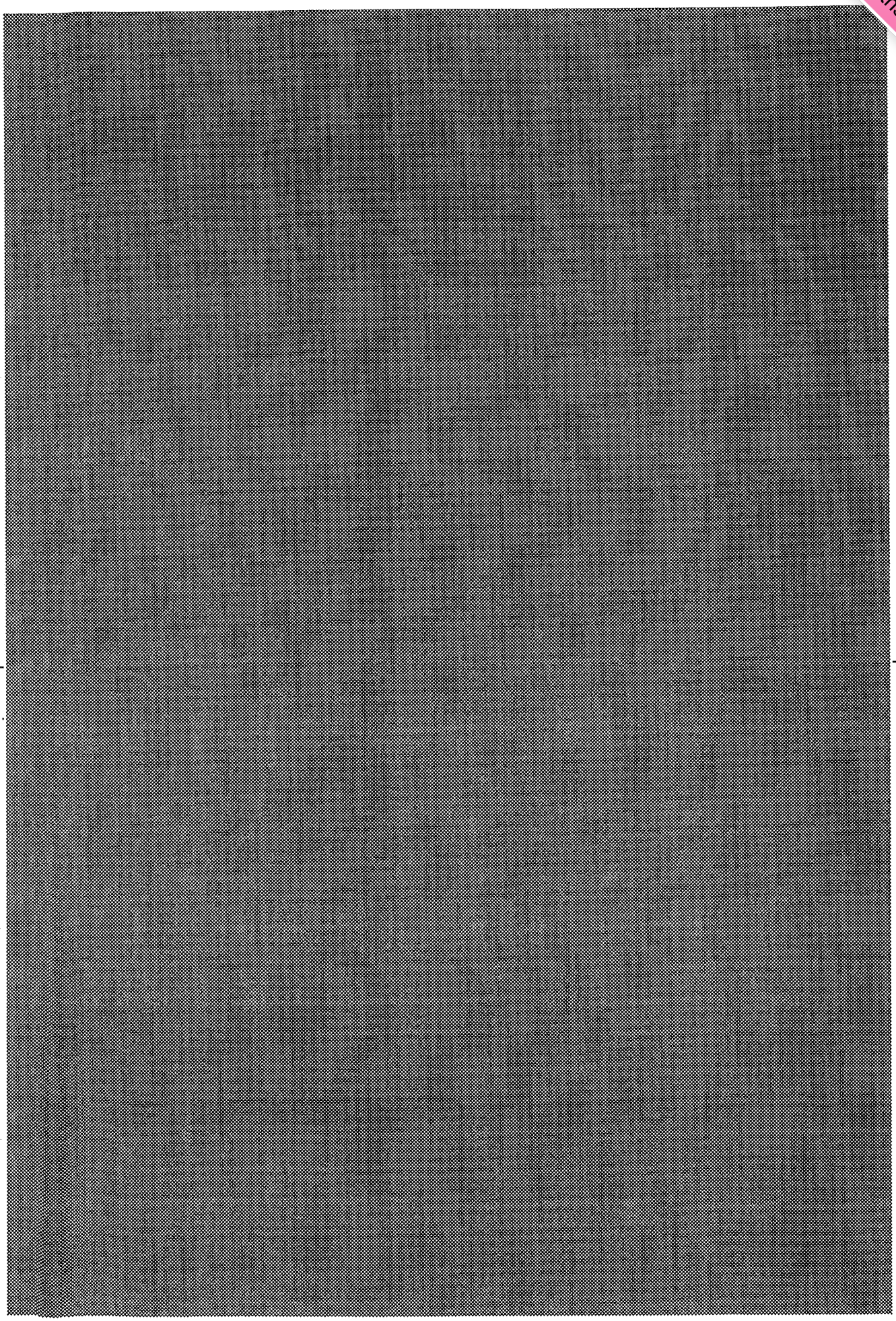
ASSESSMENT : MATH3701A
PATTERN

MODULE NAME : Theory of Numbers I

DATE : 08-May-12

TIME : 14:30

TIME ALLOWED : 2 Hours 0 Minutes



All questions may be attempted, but only marks obtained on the best four solutions will count.

The use of an electronic calculator is **not** permitted in this examination.

1. (a) Let p be a prime number, and a, b, c be integers, such that a is not congruent to 0 modulo p .

Prove that:

(i) If $bc \equiv 0 \pmod{p}$, then $b \equiv 0 \pmod{p}$ or $c \equiv 0 \pmod{p}$.

(ii) If $ab \equiv ac \pmod{p}$, then $b \equiv c \pmod{p}$.

(You may assume that, for natural numbers m, n , the greatest common divisor of m and n can be written in the form $k_1m + k_2n$, for integers k_1, k_2 .)

- (b) Prove that, if a is not congruent to 0 modulo p , then:

$$a^{p-1} \equiv 1 \pmod{p}$$

- (c) (i) Suppose that m and n are natural numbers, and that m is coprime to n . State what it means for n to be a pseudoprime for the base m .
(ii) Determine all bases (modulo 15) for which 15 is a pseudoprime.

2. (a) Define Euler's ϕ -function, $\phi : \mathbb{N} \rightarrow \mathbb{N}$.

(b) (i) Let p be a prime number, and k a natural number. Determine $\phi(p^k)$.

(ii) Hence, show that the following holds:

$$\sum_{d|p^k} \phi(d) = p^k$$

For parts (c) and (d), you may assume that, if a, b are coprime natural numbers, then $\phi(ab) = \phi(a)\phi(b)$.

- (c) Prove that, for any natural number n :

$$\sum_{d|n} \phi(d) = n$$

- (d) Determine the value of $\phi(504)$.

3. (a) (i) Let p be a prime number and m be an integer that is not congruent to 0 modulo p .
State what it means to say that m is a quadratic residue modulo p .
- (ii) Define the Legendre symbol $\left(\frac{m}{p}\right)$, for any integer m and prime number p .
- (b) (i) State the theorem of Euler for quadratic residues modulo an odd prime number p .
- (ii) Deduce that, for an odd prime number p , and integers m, n :

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right)$$

- (c) State the law of quadratic reciprocity.
- (d) Determine whether or not the following congruence is solvable:

$$x^2 + 4x + 7 \equiv 0 \pmod{137}$$

(You may assume that 137 is a prime number.)

4. (a) Give the definition of a regular continued fraction.
- (b) Describe a process that may be used to generate a regular continued fraction representation for any nonnegative real number r .
- (c) Show that, if r is a nonnegative rational number, then the process described in part (b) terminates.
- (d) Consider the following infinite regular continued fraction:

$$\theta = 4 + \frac{1}{2 + \frac{1}{8 + \frac{1}{2 + \frac{1}{8 + \frac{1}{2 + \dots}}}}}$$

Determine the value of θ^2 .

5. (a) Show that, if each of the natural numbers m, n , can be represented as a sum of two squares, then the product mn can also be represented as a sum of two squares.
- (b) Suppose that p is a prime number that is congruent to 3 modulo 4, and that n is a natural number that can be written in the form $p^{2k+1}m$, where the natural number m is not divisible by p . Show that n cannot be represented as a sum of two squares.
(You may assume any relevant results on quadratic residues and modular arithmetic modulo p .)
- (c) Describe the natural numbers that can be represented as sums of two squares.
- (d) By factorising 725, find three distinct representations of 725 as a sum of two squares.