MATH-304401

Only approved basic scientific calculators may be used.

This question paper consists of 2 printed pages, each of which is identified by the reference MATH-304401.

Examination for the Module MATH-3044
(May/June 2004)

Number Theory

Time allowed : 3 hours

Do not answer more than **four** questions
All questions carry equal marks

1. **(a)** Use the arithmetic of congruences to show that $2^{67} - 3$ is divisible by 97.

(b) Prove that $2^{2^n} - 3$ is divisible by 13 whenever n is an even integer with $n \geq 2$.

(c) State Fermat's little theorem and use it to show that $2^{q-1} \equiv 1 \pmod{pq}$ whenever p and $q = 2p - 1$ are both odd primes.

(d) Define *Euler's ϕ function.* Give a formula for $\phi(n)$ if n has the prime factorization $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, where $p_1, p_2, \dots, p_m$ are the distinct prime numbers dividing n.

Hence calculate $\phi(880)$.

(e) State a theorem of Euler that generalizes Fermat's little theorem, and use it to show that if $x > 10$ and $(x, 10) = 1$ then the last two decimal digits of x and x^{201} are the same.

2. **(a)** State a result that says exactly which numbers can be written as the sum of two integer squares.

Prove directly that no number of the form $4k + 3$ can be written as the sum of two squares.

(b) Suppose that $m = a^2 + b^2$ and $n = c^2 + d^2$ are two integers expressible as a sum of two squares. Write down an expression for mn as the sum of two squares. Hence express the number 5353 as the sum of two squares in two different ways.

(c) What is a *primitive Pythagorean triple*? Show that, if a and b are two coprime integers of which one is even, then $(a^2 - b^2, 2ab, a^2 + b^2)$ is a primitive Pythagorean triple.

Conversely, given a primitive Pythagorean triple (x, y, z), show how to find a and b such that, after exchanging x and y if necessary, (x, y, z) has the form $(a^2 - b^2, 2ab, a^2 + b^2)$.

Find two primitive Pythagorean triples that include 15 as a member.

continued . . .

3. **(a)** Let n be an integer with $n \geq 2$. Define the term *primitive root of* n.

Find all the primitive roots of 13, and show directly that 12 has no primitive roots.

(b) Let p be an odd prime and suppose that a is a primitive root of p. Prove that $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Deduce that 9 is not a primitive root of any odd prime.

(c) Which of the numbers 48, 49, 50 and 51 have primitive roots? Give brief reasons.

(d) Let p be a prime with $p > 3$, and suppose that p divides $2^{29} + 1$. What is the smallest $m > 1$ such that $2^m \equiv 1 \pmod{p}$? Deduce that $p \equiv 1 \pmod{58}$.

(e) Let r be a primitive root of the odd prime p. Show that, modulo p, the powers $r, r^2, \ldots, r^{p-1}$ are congruent to the integers $1, 2, \ldots, p-1$ in some order. Deduce Wilson's theorem.

4. **(a)** Suppose that $a,\ b > 1$ and $(a, b) = 1$. What is meant by saying that a is a *quadratic residue modulo* b? List all the quadratic residues modulo 18.

(b) Let p be an odd prime number. Show that the numbers $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are pairwise incongruent modulo p, and deduce that exactly half of the numbers $1, 2, \ldots, p-1$ are quadratic residues modulo p.

(c) For p an odd prime number and a an integer coprime to p define the *Legendre symbol* $\left(\frac{a}{p}\right)$, and state the law of quadratic reciprocity.

Using without proof the fact that p has a primitive root, prove Euler's criterion that if $(a, p) = 1$ then $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

(d) Determine whether or not the congruence $x^2 \equiv 111 \pmod{2011}$ has a solution. (You may assume the fact that 2011 is a prime number.)

(e) Let p be a prime of the form $12k + r$, where $r = 1, 5, 7$ or 11. For which values of r is 3 a quadratic residue modulo p?

5. **(a)** Define the set of *Gaussian integers*, $\mathbb{Z}[i]$.

What is the *norm*, $N(\alpha)$, of a Gaussian integer α? Show that $N(\alpha\beta) = N(\alpha)N(\beta)$ when α and β are Gaussian integers.

Deduce that $4 + i$ is a prime in $\mathbb{Z}[i]$.

Prove that the number 5 is not a prime in $\mathbb{Z}[i]$.

(b) Find the value of the finite continued fraction $[3; 2, 7]$.

Show that $\sqrt{27} = [5; \overline{5, 10}]$, and hence derive two solutions in positive integers to the Pell equation $x^2 - 27y^2 = 1$.

END