MATH-304401

Only approved basic scientific calculators may be used.

This question paper consists of 3 printed pages, each of which is identified by the reference MATH-304401.

Examination for the Module MATH-3044
(May/June 2005)

Number Theory

Time allowed : 3 hours

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

1. **(a)** Find the gcd $(3278, 4321)$, and write it in the form $3278s + 4321t$, where s and t are integers.

(b) Use the arithmetic of congruences to show that $2^{68} + 5$ is divisible by 83.

(c) Beginning with the identity $641 = 5 \times 2^7 + 1$, show that 641 is a factor of $2^{32} + 1$.

(d) Show that the number $n^5 + 1$ is never prime for $n > 1$.

(e) State Fermat's little theorem, and use it to show that if p is a prime divisor of $a^r - 1$, where $a, r \in \mathbb{Z}$, $a > 1$ and $r > 1$, then $p | a^d - 1$, where $d = (p-1, r)$.

Now suppose that an odd prime p divides $3^{53} - 1$; by listing the possibilities for d show that $p \geq 107$.

2. **(a)** State the results which describe exactly which numbers n can be written as the sum of m integer squares for $m = 2$, 3 and 4.

Show that all perfect squares are congruent to 0, 1 or 4 mod 8, and hence prove directly that no number of the form $8k + 7$ is the sum of three squares.

For each of the following numbers, find the least m for which it is the sum of m squares:

(i) 3×2^{10}; (ii) 7^{15}; (iii) 5^{15}.

(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 1517 $(= 37 \times 41)$ as the sum of two squares of positive integers in two different ways.

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

Find two primitive Pythagorean triples that include 20 as a member.

3. **(a)** Define *Euler's ϕ function.* Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$, where $p_1, p_2, \ldots, p_m$ are the distinct prime numbers dividing n. Give a formula for $\phi(n)$ in terms of the p_i.

Hence calculate $\phi(600)$.

(b) State the theorem of Euler that generalizes Fermat's little theorem, and use it to calculate the last two decimal digits of 109^{129}.

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

Find all the primitive roots of 14.

State a theorem of Gauss that describes which numbers have primitive roots, and use it to determine which of the numbers 26, 27 and 28 have primitive roots.

Question 3 continues . . .

(d) Prove that $\phi(n)$ is even whenever $n > 2$.

Suppose that $n = uv$, where $(u, v) = 1$ and $u, v > 2$. Show that, for all a with $(a, n) = 1$, we have $a^{\phi(n)/2} \equiv 1 \bmod n$, and deduce that n has no primitive roots.

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 19.

(b) 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.

Show that 5 is a quadratic residue modulo a prime $p > 5$ if and only if $p \equiv 1$ or 4 mod 5.

By considering an expression of the form $4(p_1p_2 \dots p_n)^2 - 5$, or otherwise, deduce that there are infinitely many primes congruent to 4 mod 5.

(c) Determine whether or not the congruence $x^2 \equiv 35 \pmod{1237}$ has a solution. (You may assume the fact that 1237 is a prime number.)

(d) State Euler's criterion, and use it to show that if $q = 2n+1$ is prime and 2 is a quadratic residue modulo q, then $q|2^n - 1$. Deduce that $2^{23} - 1$ is composite.

5. **(a)** Define the set of *Gaussian integers*, $\mathbb{Z}[i]$. Explain the terms *unit* and *prime* as applied to the elements of $\mathbb{Z}[i]$.

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. Prove that there are just four units in $\mathbb{Z}[i]$.

Suppose that a positive integer p is a prime in the usual sense but is not a prime in $\mathbb{Z}[i]$. Show that there is an element $\alpha \in \mathbb{Z}[i]$ with $N(\alpha) = p$. Deduce that p can be written as the sum of two integer squares.

(b) Show that $\sqrt{18} = [4; \overline{4, 8}]$, and hence derive two solutions in positive integers to the Pell equation $x^2 - 18y^2 = 1$.

(c) Let p and q be distinct odd primes, and let e be a positive integer with $(e, (p-1)(q-1)) = 1$. A number x with $(x, pq) = 1$ is encoded by the formula $E(x) \equiv x^e \bmod pq$. Explain how to find a positive integer d such that, when a number is decoded by the formula $D(y) \equiv y^d \bmod pq$, then $D(E(x)) \equiv x \bmod pq$. Justify your answer using a theorem of Euler.

END