MATH–304401

This question paper consists of 2 printed pages, each of which is identified by the reference MATH–3044

Only approved basic scientific calculators may be used.

Examination for the Module MATH–3044
(May 2006)

Number theory
Time allowed : 3 hours

Answer not more than **four** questions. All questions carry equal marks.

1. (i) State the fundamental theorem of arithmetic, and use it to show that if a and b are coprime positive integers such that ab is a square, then a and b are both squares.

(ii) Prove that if x and y are positive integers such that $x^2 = y^2 - 9y$, then $x = 6$ or 20.

(iii) By using Fermat's Little Theorem, show that for any distinct primes p and q,

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

(iv) Determine how many zeroes there are at the end of 230!, explaining your reasoning.

2. (i) Define Euler's 'totient' function $\phi(n)$, and assuming that $\phi(ab) = \phi(a)\phi(b)$ whenever a and b are coprime, derive the formula

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k})$$

where $p_1, p_2, \ldots, p_k$ are the distinct prime factors of n.

(ii) Prove that for coprime positive integers a and n, $a^{\phi(n)} \equiv 1 \bmod n$.

(iii) Describe all numbers n such that $\phi(n) = \frac{2n}{5}$.

(iv) Calculate $\phi(100)$, and hence determine the last two digits of 1781^{1781}.

3. (i) Find all Pythagorean triples that have 10 as a member.

(ii) Find the least positive multiples of 28 which may be written as a sum of 2, 3, and 4 squares, explaining your reasoning, and quoting any relevant results.

(iii) Define *primitive root* of a positive integer n. Prove by induction that $n = 2^k$ has no primitive root for $k \geq 3$.

(iv) Find which of the following have primitive roots: 54, 64, 75, 121. Show that 2 is a primitive root of 27, and find all primitive roots of 27 expressed as powers (mod 27) of 2.

4. (i) Define the *Legendre symbol* $\left(\dfrac{a}{p}\right)$ where p is an odd prime not dividing a.

(ii) State Gauss's Lemma, which characterizes $\left(\dfrac{a}{p}\right)$ as a certain power of -1, and use it to determine $\left(\dfrac{5}{17}\right)$ and $\left(\dfrac{8}{17}\right)$.

(iii) State the law of quadratic reciprocity, and give a formula for $\left(\dfrac{2}{p}\right)$. Hence evaluate $\left(\dfrac{770}{2003}\right)$. (You may assume that 2003 is prime.)

(iv) For which odd primes p is 13 a quadratic residue mod p?

5. (i) Define the set of *Gaussian integers* $\mathbb{Z}[\mathrm{i}]$. Define the *norm* $N(\alpha)$ of a Gaussian integer α. Prove that if α and β are Gaussian integers with $\beta \neq 0$, then there are Gaussian integers q and r such that $\alpha = q\alpha + r$ and $N(r) < N(\beta)$. If $\alpha = 14 + 2\mathrm{i}$ and $\beta = 3 + 2\mathrm{i}$, find suitable values for q and r.

(ii) Define the terms *unit*, *prime* and *irreducible* as applied to Gaussian integers. State, with reasons, which primes of $\mathbb{Z}$ remain primes in $\mathbb{Z}[\mathrm{i}]$, and which ones factorize as the product of other primes. [You may assume without proof that in $\mathbb{Z}[\mathrm{i}]$ an element is prime if and only if it is irreducible.]

Factorize the number 60 into primes in $\mathbb{Z}[\mathrm{i}]$.

(iii) Find the values of the finite continued fraction $2 + \dfrac{1}{4 + \frac{1}{4 + \frac{1}{4}}}$ and the infinite recurring continued fraction $2 + \dfrac{1}{4 + \frac{1}{4 + \frac{1}{4 + \dots}}}$. Deduce two solutions of Pell's equation $x^2 - 5y^2 = 1$.

END