A17855 No Calculator

UNIVERSITY OF BIRMINGHAM

School of Mathematics

Programmes in the School of Mathematics — Final Examination

Programmes including Mathematics — Final Examination

06 22498

MSM 3P05: Number Theory

Summer Examinations 2010

Time allowed: 3 hours

Full marks may be obtained with complete answers to FOUR questions (each worth 25%) out of SIX. Only the FOUR best answers will be credited.

No calculator is permitted in this examination.

1. (a) (i) Write down the definitions of $\mathbb{Z}[i]$ and the norm $N : \mathbb{Z}[i] \longrightarrow \mathbb{Z}$.

(ii) Determine the factors of $1+8i$ in $\mathbb{Z}[i]$.

(b) (i) Let $\alpha \in \mathbb{Z}[i]$. Prove that if $N(\alpha)$ is irreducible in $\mathbb{Z}$, then α is irreducible in $\mathbb{Z}[i]$.

(ii) Let $\alpha \in \mathbb{Z}[i]$ and suppose that $N(\alpha)$ is prime in $\mathbb{Z}$. What can you say about α? [A few sentences at most.]

(c) (i) Let x be an odd natural number. Show that $x^2+2 \equiv 3 \bmod 4$ and deduce that there exists a prime p with

$$p \mid x^2+2 \quad \text{and} \quad p \equiv 3 \bmod 4.$$

(ii) Use (i) to show that there are infinitely many prime numbers p with $p \equiv 3 \bmod 4$. [Hint: Let x be the product of certain primes.]

(iii) Deduce that there are infinitely many counterexamples to the converse of (b)(i).

2. (a) Use the Euclidean Algorithm to determine all the solutions to

$$33x \equiv 6 \bmod 108.$$

(b) (i) State and prove the theorem of Lagrange concerning the number of roots of a polynomial modulo a prime.

(ii) Let p be a prime and d a natural number with $d \mid p-1$. Prove that

$$x^d \equiv 1 \bmod p$$

has exactly d distinct solutions modulo p.

(c) Let p be a prime and d a natural number with $d \mid p-1$. Investigate the number of solutions to

$$x^d \equiv 1 \bmod p^2.$$

[Hint: Consider integers of the form $s+yp$, where s is a solution to $x^d \equiv 1 \bmod p$.]

3. (a) State Gauss' Law of Quadratic Reciprocity and use it to evaluate the following Legendre symbols.

$$\left(\frac{5}{23}\right), \quad \left(\frac{20}{31}\right) \quad \text{and} \quad \left(\frac{35}{43}\right).$$

(b) Let p be an odd prime. Prove that there are the same number of quadratic residues modulo p as there are nonresidues. Clearly indicate where you use the fact that p is prime.

(c) For each $n \in \mathbb{N}$ define the n^{th} Mersenne number by $M_n = 2^n - 1$.
Let p and q be primes. Assume that $p \equiv 3 \bmod 4$ and $q = 2p+1$.
By considering the Legendre symbol $\left(\frac{2}{q}\right)$, or otherwise, prove that $q \mid M_p$. Deduce that M_{23} is not prime.

4. In parts (a) and (b) we assume that $x, y \in \mathbb{Z}$ satisfy

$$y^3 = x^2 + 4.$$

(a) (i) Write down the units of $\mathbb{Z}[i]$ and verify that each unit is the cube of a unit.

(ii) Let d be a highest common factor of $x+2i$ and $x-2i$. Prove that d is an associate of π^t for some $t \geq 0$, where $\pi = 1+i$.

(b) (i) Prove that t is a multiple of 3 and deduce that y^3/π^{2t} is associate to the cube of a Gaussian integer.

(ii) Show that $x+2i$ is the cube of a Gaussian integer.

(iii) Determine the possibilities for x and y.

(c) Let k be a natural number. Obtain an upper bound for the number of integer solutions to

$$y^3 = x^2 + 4^k.$$

Where appropriate, you may merely indicate modifications to, or re-use, your previous answers.

5. Write an essay which discusses the Method of Descent and illustrates its use by discussing the special case

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

of Fermat's Last Theorem. Your essay should demonstrate that you have knowledge of the necessary background material and contain a significant amount of mathematical detail.

6. For each $n \in \mathbb{N}$ define the n^{th} Mersenne number by

$$M_n = 2^n - 1.$$

Define a sequence $r_0, r_1, \dots$ by

$$r_0 = 4 \quad \text{and} \quad r_{i+1} = r_i^2 - 2.$$

Let

$$\tau = 2 + \sqrt{3}.$$

We will work in the ring $\mathbb{Z}[\sqrt{3}]$, which possesses a conjugate function defined by $\overline{a + b\sqrt{3}} = a - b\sqrt{3}$ for all $a, b \in \mathbb{Z}$.

(a) (i) Let $n \in \mathbb{N}$. Prove that if M_n is prime, then so is n.

(ii) Prove that $\tau\overline{\tau} = 1$.

(iii) Prove that $r_i = \tau^{2^i} + \overline{\tau}^{2^i}$ for all $i \geq 0$.

(b) (i) Let $\alpha \in \mathbb{Z}[\sqrt{3}]$ and let p be an ordinary prime number. Prove that

$$\alpha^p \equiv \left\{ \begin{array}{ll} \alpha & \text{if } p \equiv \pm 1 \bmod 12 \\ \overline{\alpha} & \text{if } p \equiv \pm 5 \bmod 12. \end{array} \right\} \bmod p.$$

Any significant results that your proof requires should be clearly stated. You may assume without proof that

$$\left(\frac{3}{p}\right) = \left\{ \begin{array}{ll} 1 & \text{if } p \equiv \pm 1 \bmod 12 \\ -1 & \text{if } p \equiv \pm 5 \bmod 12. \end{array} \right.$$

(ii) Let a and q be elements of a ring R. What is the order of a modulo q?

(iii) Let a and d be elements of a ring R, let d be the order of a modulo q, and let $k \in \mathbb{N}$. Prove that $a^k \equiv 1 \bmod q$ if and only if k is a multiple of d.

(c) Let $n \in \mathbb{N}$, $n \geq 3$, and assume that

$$r_{n-2} \equiv 0 \bmod M_n.$$

Let q be a prime factor of M_n.

(i) Show that $\tau^{2^{n-1}} \equiv -1 \bmod q$ and that $\tau^{2^n} \equiv 1 \bmod q$.

(ii) Deduce that the order of τ modulo q is 2^n.

(iii) Suppose that $q \equiv \pm 1 \bmod 12$. Apply (b)(i) to obtain a contradiction.

(iv) Apply (b)(i) to prove that $M_n = q$ and deduce that M_n is prime.