A99999 No Calculator

THE UNIVERSITY OF BIRMINGHAM

Refer to www.exampapers.bham.ac.uk for the definitive version.

99 99999

MSMP05: Number Theory

2006 3 hours

Full marks to this examination may be obtained with complete answers to FOUR questions out of SIX. Credit will be given to the best FOUR answers only. Calculators may not be used in this examination.

Turn over

1. (a) Determine the factors of $5 - 2\sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}]$.

(b) Let $p \in \mathbb{Z}, p > 0$, be irreducible in $\mathbb{Z}$. Suppose that p is not irreducible in $\mathbb{Z}[\sqrt{-2}]$.

(i) Prove that

$$p = \pi\pi^*$$

for some $\pi \in \mathbb{Z}[\sqrt{-2}]$.

(ii) Deduce that there are integers a and b such that $p = a^2 + 2b^2$ and then that

$$\left(\frac{-2}{p}\right) = 1.$$

(c) State and prove the converse to the result proved in (b).

[Standard properties of $\mathbb{Z}[\sqrt{-2}]$ may be used without proof provided that they are stated clearly.]

2. (a) (i) Define the term *multiplicative function*.

(ii) Define $\mu : \mathbb{N} \longrightarrow \mathbb{C}$ by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 \mid n \text{ for some prime } p \\ (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes.} \end{cases}$$

Prove that μ is multiplicative.

(b) For any function $f : \mathbb{N} \longrightarrow \mathbb{C}$ define $\widehat{f} : \mathbb{N} \longrightarrow \mathbb{C}$ by

$$\widehat{f}(n) = \sum_{d|n} f(d).$$

(i) Prove that $\widehat{\mu}(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1. \end{cases}$

(ii) State and prove the Möbius Inversion Formula.

(c) Let ϕ denote the Euler ϕ-function.

(i) Prove that $\widehat{\phi}(n) = n$ for all $n \in \mathbb{N}$ and deduce that ϕ is multiplicative.

(ii) Where in your answer to (c)(i) have you used, implicitly or explicitly, the fact that $\mathbb{Z}$ is a Euclidean ring?

[Standard properties of multiplicative functions may be used without proof provided that they are stated clearly.]

3. (a) (i) Use the Euclidean Algorithm to determine the solutions to

$$48x \equiv 45 \bmod 69.$$

(ii) Suppose that $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Prove that if $\text{hcf}(a, n) \mid b$ then

$$ax \equiv b \bmod n$$

has at least one solution.

(b) Suppose that p is a prime and that a is an integer with $a \not\equiv 0 \bmod p$.

(i) What is *the order of a modulo p?*

(ii) Let d be the order of a modulo p and let $k \in \mathbb{N}$. Prove that $a^k \equiv 1 \bmod p$ if and only if $d \mid k$.

(iii) Use Fermat's Little Theorem to deduce that $d \mid p - 1$. [Two lines at most.]

(iv) Let $k \in \mathbb{N}$ with $\text{hcf}(k, p-1) = 1$. Use (b)(ii),(iii) to prove that the only solution to

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

is $x \equiv 1 \bmod p$.

(c) Let p be a prime and $k \in \mathbb{N}$ with $\text{hcf}(k, p-1) = 1$. Prove that every integer has a k^{th} root modulo p.

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

$$\left(\frac{19}{37}\right) \quad \text{and} \quad \left(\frac{15}{89}\right).$$

(b) Determine the primes p for which 3 is a quadratic residue modulo p.

(c) State and prove Gauss' Lemma.

5. Let $\omega = e^{2\pi i/3}$ and $\mathbb{Z}[\,\omega\,] = \{\ a + b\omega \mid a, b \in \mathbb{Z}\ \}$.

(a) (i) Show that $\omega^3 = 1$, that $\omega^* = \omega^2$, that $\omega^2 + \omega + 1 = 0$ and deduce that $\omega = \frac{1}{2}(-1 + \sqrt{-3})$.

(ii) Define $N : \mathbb{Z}[\,\omega\,] \longrightarrow \mathbb{Z}$ by $N(\alpha) = \alpha\alpha^*$. Show that

$$N(a + b\omega) = a^2 - ab + b^2$$

for all $a, b \in \mathbb{Z}$.

(iii) By completing the square, or otherwise, show that the units of $\mathbb{Z}[\,\omega\,]$ are $\pm 1, \pm\omega$ and $\pm\omega^2$. [You may assume, without proof, that α is a unit if and only if $N(\alpha) = 1$.]

(b) Let $\lambda = 1 - \omega$.

(i) Show that λ^2 is associate to 3.

(ii) Show that every member of $\mathbb{Z}[\,\omega\,]$ can be written in the form $a + b\lambda$, for some $a, b \in \mathbb{Z}$.

(iii) Show that if $\alpha \in \mathbb{Z}[\,\omega\,]$ then $\alpha^3 \equiv n \bmod \lambda^3$ for some $n \in \mathbb{Z}$.

(iv) Suppose that u is a unit of $\mathbb{Z}[\,\omega\,]$ such that

$$u \equiv \alpha^3 \bmod \lambda^3$$

for some $\alpha \in \mathbb{Z}[\,\omega\,]$. Prove that u is a cube of a unit.

(c) Give an outline of the proof of Fermat's Last Theorem in the case $n = 3$. Pay particular attention to how the conclusion of (b) is used.

6. In this question we consider the ring

$$\mathbb{Z}[\sqrt{5}] = \{ a + b\sqrt{5} \mid a, b, \in \mathbb{Z} \}$$

and the conjugate function $\overline{} : \mathbb{Z}[\sqrt{5}] \longrightarrow \mathbb{Z}[\sqrt{5}]$ defined by $\overline{a + b\sqrt{5}} = a - b\sqrt{5}$ for all $a, b \in \mathbb{Z}$.

(a) Let $p \in \mathbb{Z}$, $p > 0$, be irreducible in $\mathbb{Z}$. In other words, p is an ordinary prime number.

(i) Use the Binomial Theorem to prove that

$$(\alpha + \beta)^p \equiv \alpha^p + \beta^p \bmod p$$

for all $\alpha, \beta \in \mathbb{Z}[\sqrt{5}]$. You may use any property of binomial coefficients provided that it is stated clearly.

(ii) Prove that

$$\alpha^p \equiv \left\{ \begin{array}{ll} \alpha & \text{if } p \equiv \pm 1 \bmod 5 \\ \overline{\alpha} & \text{if } p \equiv \pm 2 \bmod 5 \end{array} \right\} \bmod p$$

for all $\alpha \in \mathbb{Z}[\sqrt{5}]$.

You may use, without proof, the fact that $\left(\frac{5}{p}\right) = \left\{ \begin{array}{ll} 1 & \text{if } p \equiv \pm 1 \bmod 5 \\ -1 & \text{if } p \equiv \pm 2 \bmod 5 \end{array} \right.$.

(b) Let $\tau = 2 + \sqrt{5}$ and define a sequence $r_1, r_2, \ldots,$ by

$$r_1 = 18 \quad \text{and} \quad r_{k+1} = r_k^2 - 2.$$

(i) Prove that $\tau\overline{\tau} = -1$. [One line.]

(ii) Prove that $r_k = \tau^{2^k} + \overline{\tau}^{2^k}$ for all $k \in \mathbb{N}$.

Let $n \in \mathbb{N}$ and put $p = 2^n - 1$. Assume that p is irreducible in $\mathbb{Z}$ and that $p \equiv 2 \bmod 5$.

(iii) Use(a)(ii) to prove that $\tau^{2^n} \equiv -1 \bmod p$.

(iv) Deduce that $r_n \equiv -2 \bmod p$ and then that

$$r_{n-1} \equiv 0 \bmod p.$$

(c) Let $n \in \mathbb{N}, n \geq 3$ and put $M = 2^n - 1$. Assume that M has a prime factor q with $q \equiv \pm 2 \bmod 5$ and that

$$r_{n-1} \equiv 0 \bmod M.$$

(i) Use(b)(ii) to show that $\tau^{2^n} \equiv -1 \bmod q$. Deduce that the order of τ modulo q is 2^{n+1}.

(ii) Use (a)(ii) to show that $\tau^{2(q+1)} \equiv 1 \bmod q$. Deduce that $M = q$, so that M is prime.