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 2011

Time allowed: 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.
An indication of the number of marks allocated to parts of questions is shown in square brackets.
No calculator is permitted in this examination.

1. (a) Determine the factors of $6 - 7i$ in $\mathbb{Z}[\,i\,]$.

   (i) Prove that for each $z \in \mathbb{C}$ there exists $q \in \mathbb{Z}[\,i\,]$ such that

$$|z - q|^2 < 1.$$

   (ii) Which very important property of $\mathbb{Z}[\,i\,]$ is (i) used to prove?

   (b) Suppose α is a nonzero Gaussian integer. Prove that there are only finitely many congruence classes modulo α. Obtain an upper bound for the number of such classes in terms of α.

[25]

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

   (ii) Let $\sigma(n)$ denote the sum of the positive factors of n. Using the fact that σ is multiplicative, evaluate $\sigma(100)$.

   (b) The Möbius function $\mu : \mathbb{N} \longrightarrow \mathbb{C}$ is defined by

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

   Given a function $f : \mathbb{N} \longrightarrow \mathbb{C}$ the function
   $\widehat{f} : \mathbb{N} \longrightarrow \mathbb{C}$ is defined 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) Prove the Möbius Inversion Formula, namely that if $f : \mathbb{N} \longrightarrow \mathbb{C}$ is any function then

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

   (c) Suppose that p is a prime number.

   (i) Write down, without proof, the number of solutions to

$$X^n \equiv 1 \bmod p$$

   where n is a positive factor of $p - 1$.

(ii) Use the Möbius Inversion Formula to prove that there exists a primitive root modulo p.
[You may assume without proof that $\widehat{\phi}(n) = n$ for all n, where ϕ is the Euler ϕ–function.]

[25]

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

$$15x \equiv 9 \bmod 159.$$

(b) State and prove Fermat's Little Theorem.

(c) A *near-prime* is an odd number $p > 1$ with the properties:

- p is not prime.
- $2^{p-1} \equiv 1 \bmod p$.

Suppose that p is a near-prime.

(i) Prove that $2^p - 1$ is not prime.

(ii) Prove that $2^p - 1$ is a near-prime.

[25]

4. (a) (i) State Gauss' Law of Quadratic Reciprocity.

(ii) Evaluate the following Legendre Symbols:

$$\left(\frac{5}{19}\right) \quad \text{and} \quad \left(\frac{15}{19}\right).$$

(iii) Determine the primes p for which 5 is a quadratic residue.

(b) State and prove Euler's Criterion.

(c) Establish an analogue of Fermat's Little Theorem for the ring $\mathbb{Z}[\sqrt{5}]$.

[25]

5. Suppose that x, y and z are positive integers that satisfy

$$x^2 + y^2 = z^2$$

and that x and y are coprime in the integers.

(a) By considering congruences modulo 4, or otherwise, prove that z is odd.

(b) (i) Write down a factorization of $x^2 + y^2$ in the Gaussian integers and show that the two factors are coprime.
[Hint: Show that the norm of any common factor is a factor of $2x^2$ and also of $2y^2$.]

(ii) Prove that there exist positive integers a and b such that

$$(x, y, z) = (a^2 - b^2, 2ab, a^2 + b^2)$$

or

$$(x, y, z) = (2ab, a^2 - b^2, a^2 + b^2).$$

[You may assume any results related to unique factorization provided they are stated clearly.]

(c) Investigate to what extent the integers a and b in (b)(ii) are uniquely determined.

[25]

6. 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 $\mathbb{Z}[\omega]$ is a ring.

(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) Outline of the proof of Fermat's Last Theorem in the case $n = 3$ and describe in detail how the conclusion of (b) is used.

[25]