# UNIVERSITY OF BIRMINGHAM

## School of Mathematics

Programmes in the School of Mathematics Final Examination

Programmes including Mathematics Final Examination

**06 22498 MSM3P05 Level H**

**Number Theory**

**06 16214 MSM4P05 Level M**

**Number Theory**

Summer Examinations 2012

Three Hours

Full marks will be obtained with complete answers to FOUR out of SIX questions. If more than FOUR questions are attempted then only the best FOUR will count towards the final mark. No calculator is permitted in this examination.

**1.** (a) (i) Write down the definition of $\mathbb{Z}[i]$.

(ii) Let $\alpha \in \mathbb{Z}[i]$. Prove that $\alpha$ is a unit if and only if the norm $N(\alpha) = 1$.

(b) Determine the factors of $9 + 2i$ in $\mathbb{Z}[i]$.

(c) (i) Let $\pi = a + bi$ with $a, b \in \mathbb{Z}$ and $a, b \neq 0$. Suppose that $\pi$ is associate to $\pi^*$, where $\pi^*$ is the complex conjugate of $\pi$. Prove that $a = b$ or $a = -b$.

(ii) Let $\pi = a + bi$ with $a, b \in \mathbb{Z}$ and $a, b \neq 0$. Suppose that $\pi$ is irreducible in $\mathbb{Z}[i]$ and that $\pi$ is not associate to $1 + i$. Prove that $\pi$ and $\pi^*$ are coprime.

(iii) Prove that there exist infinitely many Gaussian integers $\alpha$ with the following properties:

- $N(\alpha)$ is the product of two prime numbers.
- At least one of the potential factors of $\alpha$, as discovered by the "norm method" for determining factors, is not actually a factor.

[Hint: you may assume without proof the fact that there are infinitely many prime numbers that are congruent to $1$ modulo $4$.]

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

$$51x \equiv 6 \bmod 87.$$

(b) Suppose that $a$ and $b$ are integers and that $n$ is a natural number. Consider the equation

$$aX \equiv b \bmod n. \qquad (*)$$

Let $h = \text{hcf}(a,n)$.

(i) Prove that $(*)$ has a solution if and only if $h \mid b$.

Now suppose that $x_0$ is a solution to $(*)$.

(ii) Prove that $x_0 + k\dfrac{n}{h}$ is also a solution to $(*)$ for each $k \in \mathbb{Z}$.
[This should take no more than three lines.]

(iii) Suppose that $y$ is a solution to $(*)$. Prove that there exists $k \in \mathbb{Z}$ such that

$$y \equiv x_0 + k\frac{n}{h} \bmod n \quad \text{and} \quad 0 \leq k < h.$$

(c) Let $p$ be an odd prime number.

(i) Using (b) or otherwise, show that if $a \in \mathbb{Z}$ with $a \not\equiv 0 \bmod p$ then there exists a *unique* $a'$ with $aa' \equiv 1 \bmod p$.

(ii) Referring to (c)(i), determine the values of $a$ for which $a' \equiv a \bmod p$.

(iii) Deduce that $(p-1)! \equiv -1 \bmod p$.

**3.** (a) (i) Define the terms *quadratic residue* and *quadratic nonresidue*.

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

$$\left(\frac{5}{29}\right), \quad \left(\frac{14}{29}\right), \quad \left(\frac{19}{29}\right).$$

(b) (i) State Gauss' Lemma.

(ii) Use Gauss' Lemma to evaluate $\left(\frac{3}{11}\right)$.

(iii) Prove Gauss' Lemma.

(c) Let $p$ be an odd prime.

(i) Define the term *primitive root modulo* $p$.

(ii) Suppose that $\omega$ is a primitive root modulo $p$. What is $\left(\frac{\omega}{p}\right)$?

(iii) Using primitive roots, prove that there are as many quadratic residues modulo $p$ as there are nonresidues.

**4.** Let $\tau = \frac{1}{2}(-1+\sqrt{-11})$ and $R = \{\, a+b\tau \mid a,b \in \mathbb{Z} \,\}$.

Define a norm $N : R \longrightarrow \{0,1,2,\ldots\}$ by

$$N(\alpha) = \alpha\alpha^*$$

where $\alpha^*$ is the complex conjugate of $\alpha$.

(a) (i) Show that $\tau^2 + \tau + 3 = 0$ and briefly explain why this implies that $R$ is a ring.

(ii) If $a,b \in \mathbb{Z}$, show that

$$N(a+b\tau) = a^2 - ab + 3b^2.$$

(iii) By completing the square, or otherwise, show that the units of $R$ are $1$ and $-1$.

[Standard properties of norms may be used without proof.
WARNING: $(a+b\tau)^* \neq a - b\tau$.]

(b) Suppose that $p \in \mathbb{Z}$ is an odd positive prime number and that $p$ is not irreducible in $R$.

(i) Prove that there exists an irreducible $\pi \in R$ such that

$$p = \pi\pi^* \text{ and } N(\pi) = p.$$

(ii) Deduce that there exist integers $a$ and $b$ such that

$$a^2 - ab + 3b^2 = p$$

and then that the Legendre symbol

$$\left(\frac{-11}{p}\right) = 1.$$

(c) Throughout the remainder of this question, you may assume that $R$ is a Euclidean Ring.

(i) State the relationship between irreducibles and primes in a Euclidean Ring.

(ii) State and prove the converse of the result proved in (b).

**5.** Throughout this question, $\omega = e^{2\pi i/3}$, $\mathbb{Z}[\omega] = \{ a+b\omega \mid a,b \in \mathbb{Z} \}$ and $\lambda = 1-\omega$.

You may assume without proof that $N(\lambda) = 3$.

(a) (i) Show that $\omega^3 = 1$ and that $\omega^2 + \omega + 1 = 0$.

(ii) Write down, without proof, the units of $\mathbb{Z}[\omega]$.

(iii) Show that $\lambda^2$ is associate to 3.

(iv) Show that $\{ 0,1,2 \}$ is a complete set of residues mod $\lambda$ in $\mathbb{Z}[\omega]$.

(b) Let $x,y,z \in \mathbb{Z}[\omega] - \{ 0 \}$, let $u$ be a unit of $\mathbb{Z}[\omega]$ and suppose that

- $x^3 + y^3 = uz^3$,
- $x$ and $y$ are coprime in $\mathbb{Z}[\omega]$, and
- $\lambda \mid z,\ \lambda \nmid x$ and $\lambda \nmid y$.

Set

$$\mathscr{A} = \{ x+y,\ x+\omega y,\ x+\omega^2 y \ \}.$$

(i) Show that the difference of any two distinct members of $\mathscr{A}$ is associate to $\lambda y$. Deduce that $\lambda$ is a factor of every member of $\mathscr{A}$.

(ii) Show that $\lambda$ is a highest common factor of any two distinct members of $\mathscr{A}$.

(iii) Show that exactly one member of $\mathscr{A}$ is a multiple of $\lambda^2$.

(c) In approximately a page, outline the proof of Fermat's Last Theorem for exponent 3. Indicate how the conclusion of (b) is used.

**6.** Write an essay on Mersenne primes and analogues of Fermat's Little Theorem.

You may wish to refer to the numbers

$$\mu = 1+\sqrt{3} \text{ and } \tau = 2+\sqrt{3}.$$

You may use the fact that the Legendre symbol

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1,11 \mod 12 \\ -1 & \text{if } p \equiv 5,7 \mod 12 \end{cases}$$

provided that you give a brief indication of how it is proved.