UNIVERSITY OF BIRMINGHAM

School of Mathematics

Programmes in the School of Mathematics Final Examination

Programmes involving Mathematics Final Examination

MSM3P05 06 22498 Level H

Number Theory

MSM4P05 06 16214 Level M

Number Theory

Summer examinations 2013-14

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.

Each question carries equal weight. No calculator is permitted in this examination.

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

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

(b) Determine the factors of $-8+9i$ in $\mathbb{Z}[i]$.

(c) Let $\alpha \in \mathbb{Z}[i]$ and suppose that $N(\alpha) = pq$ where p and q are distinct prime numbers.

(i) Prove that α is the product of at most two irreducible Gaussian integers.

(ii) State the relationship between irreducibles and primes in $\mathbb{Z}[i]$. Prove that α is the product of exactly two irreducible Gaussian integers.

[25]

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

$$100x \equiv 12 \bmod 144.$$

Throughout the remainder of the question, p is a prime and a is an integer with $a \not\equiv 0 \bmod p$.

(b) (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) State Fermat's Little Theorem and use it to deduce that $d \mid p-1$.

(c) Assume that k is a natural number with hcf$(k, p-1) = 1$.

(i) Using (b), show that the only solution to $x^k \equiv 1 \bmod p$ is $x \equiv 1 \bmod p$.

(ii) Let l be an integer. Show that $x^k \equiv l \bmod p$ has at most one solution.

[25]

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

$$\left(\frac{5}{19}\right),\ \left(\frac{15}{37}\right) \quad \text{and} \quad \left(\frac{14}{23}\right).$$

(b) (i) What can you say about the number of quadratic residues and quadratic non residues modulo a prime p. (Proof not required.)

(ii) State and prove Euler's Criterion.

(c) Establish an analogue of Fermat's Little Theorem for the ring $\mathbb{Z}[\sqrt{-7}]$, namely establish a formula for α^p where $\alpha \in \mathbb{Z}[\sqrt{-7}]$ and $p > 7$ is a prime in $\mathbb{Z}$.

[25]

4. Let $\tau = \frac{1}{2}(-1+\sqrt{-7})$ and $R = \{a + b\tau \,|\, a, b \in \mathbb{Z}\}$.

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

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

where α^* is the complex conjugate of α.

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

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

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

(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 a positive prime number and that p is not irreducible in R.

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

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

and $N(\pi) = p$.

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

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

and then that there is an integer x such that

$$x^2 \equiv -7 \bmod p.$$

(c) Suppose that $p \in \mathbb{Z}$ is a positive prime number and that $\left(\frac{-7}{p}\right) = 1$. Prove that R contains at least one, and at most four, elements with norm p.

[You may assume, without proof, that R is a UFD.]

[25]

5. In parts (a) and (b) we suppose that x and y are integers that satisfy

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

and we work in the ring $\mathbb{Z}[i]$.

(a) Let d be a highest common factor of $x + 2i$ and $x - 2i$.
Prove that d is associate to π^t for some t, 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) Determine the possibilities for x and y.

(c) Let $p > 2$ be a prime number. Investigate the number of integer solutions to

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

You may re-use appropriate parts of your working in (a) and (b).

[25]

6. Write an essay on the proof of the $n = 3$ case of Fermat's Last Theorem. Your essay should contain a discussion of the relevant background results and emphasize the role played by the theory of unique factorization. Part of your essay should contain detailed mathematics. [25]