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 2012-13

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) Determine the factors of $7+6i$ in $\mathbb{Z}[i]$.

(b) Suppose that $\alpha \in \mathbb{Z}[i]$ and that $N(\alpha)$ is irreducible in $\mathbb{Z}$. Prove that α is irreducible in $\mathbb{Z}[i]$.

(c) (i) Suppose α and β are elements of a ring R. What is meant by a *highest common factor* of α and β?

Now suppose that α and β are non-zero Gaussian integers. Let η be a highest common factor of α and β in $\mathbb{Z}[i]$ and let h be a highest common factor of $N(\alpha)$ and $N(\beta)$ in $\mathbb{Z}$.

(ii) Prove that $N(\eta) \mid h$ in $\mathbb{Z}$.

(iii) Find a counterexample to the assertion that $N(\eta) = h$.

(iv) Show that there are infinitely many counterexamples to the assertion that $N(\eta) = h$. [*You may assume 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

$$32x \equiv 20 \bmod 108.$$

(b) (i) Let p be a prime and $f(x)$ a polynomial with integer coefficients. What can be said about the number of roots of $f(x)$ modulo p? Prove your answer.

(ii) State Fermat's Little Theorem.

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

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

has exactly d distinct solutions modulo p. Indicate clearly where your proof uses the hypothesis that p is a prime.

(c) Let p be a prime and d a natural number that is coprime to $p-1$. Show that there is a natural number e with $de \equiv 1 \bmod p-1$. Hence determine the number of solutions to

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

3. (a) (i) Define the Legendre symbol $\left(\frac{a}{p}\right)$.

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

$$\left(\frac{5}{13}\right) \quad \text{and} \quad \left(\frac{15}{37}\right).$$

(b) Let p be an odd prime.

(i) How many quadratic residues modulo p are there? How many quadratic non-residues modulo p are there? [*You are not required to prove your answer.*]

(ii) State and prove Euler's Criterion.

(c) Let p be a prime and suppose that

$$p = 2^{2^n} + 1$$

for some $n \geq 2$.

(i) Show that $p \equiv 2 \bmod 5$.
[*Hint:* $2^{2^n} = 4^{2^{n-1}} \equiv (-1)^{2^{n-1}} \bmod 5$.]

(ii) Use Gauss' Law of Quadratic Reciprocity to obtain

$$\left(\frac{5}{p}\right) = -1.$$

(iii) Use Euler's Criterion to deduce that

$$5^{2^{2^n-1}} \equiv -1 \bmod p.$$

(iv) Show that the order of 5 modulo p is equal to 2^m for some $m \leq 2^n$.
[*Two sentences at most.*]

(v) Deduce that 5 is a primitive root modulo p.

4. (a) Using a factorization in $\mathbb{Z}$, obtain all the integer solutions to

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

(b) Suppose that x and y are integers that satisfy

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

(i) By considering congruences modulo 4 prove that y is odd.

(ii) Prove that $x + \sqrt{-2}$ and $x - \sqrt{-2}$ are coprime in $\mathbb{Z}[\sqrt{-2}]$.

(iii) Deduce that $x + \sqrt{-2}$ is equal to a cube of a member of $\mathbb{Z}[\sqrt{-2}]$. Show that $(x, y) = (\pm 5, 3)$.

[*You may use any facts relating to unique factorization provided that they are stated clearly.*]

(c) Suppose that p is a prime with $p > 3$. Prove that the number of solutions to

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

is at most $p - 1$. [*You may reuse parts of your answers to (b).*]

5. Write an essay on the proof of Fermat's Last Theorem in the case $n = 3$. Your essay should contain an outline of the proof and a more detailed exposition of part of the proof. Your essay should also indicate the difficulties that would arise in any attempt to extend the proof to larger values of n.

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

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

Define a sequence $r_0, r_1, \ldots$ 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 integers $i \geq 0$.

(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 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 meant by the order of a modulo q?

(iii) Let a and q 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 $n \in \mathbb{N}$ 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.