UNIVERSITY OF BIRMINGHAM

School of Mathematics

Programmes in the School of Mathematics, Final Year

Programmes including Mathematics, Final Year

06 16226

06 16214

MSM 3P05: Number Theory LH

MSM 4P05: Number Theory LM

Summer 2007

Time allowed: 3 hours

Full marks may be obtained with complete answers to FOUR questions out of SIX. Credit will be given to the best FOUR answers only.

No calculator is permitted in this examination.

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

(b) (i) Define the term *irreducible*.

(ii) Define the term *prime*.

(iii) Using the fact that $\mathbb{Z}[i]$ is a Euclidean Ring, prove that every irreducible in $\mathbb{Z}[i]$ is prime.

(c) Suppose that $\pi \in \mathbb{Z}[i]$ is irreducible. Prove that there exists a prime number p such that $N(\pi) = p$ or $N(\pi) = p^2$.
[Hint: consider an ordinary prime number p that is a factor of $N(\pi)$ and then consider an irreducible factor of p.]

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

$$100x \equiv 8 \bmod 144.$$

(b) (i) State and prove the theorem of Lagrange on the number of roots of a polynomial modulo a prime.

(ii) State Fermat's Little Theorem.

(c) Let p be a prime and d a positive factor of $p-1$. Use (b) to prove that

$$x^{\frac{p-1}{d}}$$

takes exactly d distinct values modulo p as x ranges over $1, 2, \ldots, p-1$.

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:

$$\left(\frac{7}{11}\right), \quad \left(\frac{34}{71}\right), \quad \left(\frac{70}{101}\right).$$

(b) State Euler's Criterion and use it to show that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

whenever p is an odd prime and $a, b \in \mathbb{Z}$.

(c) Let $n \geq 2$ be a natural number, set

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

and suppose that p is a prime.

(i) Use Gauss' Law of Quadratic Reciprocity to show that

$$\left(\frac{3}{p}\right) = -1.$$

Apply Euler's Criterion to deduce that

$$3^{2^{2^n-1}} \equiv -1 \bmod p.$$

(ii) Show that the order of 3 modulo p is equal to 2^m for some $m \leq 2^n$.
[Two sentences at most.]

(iii) Deduce that 3 is a primitive root modulo p.

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

$$x^2 = y^4 + 9.$$

(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 an odd prime. Obtain an upper bound in terms of p for the number of solutions to

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

You may re-use parts of your answers to (b).

5. Write an essay on the proof that the Fermat equation

$$x^3 + y^3 = z^3$$

has no non-trivial integer solutions. Your essay should contain a discussion of the required background results and an outline of the proof. You should demonstrate an appreciation of the role played by the theory of unique factorization.

Your essay should also contain a more detailed exposition of part of the proof.

6. (a) Define what a Mersenne prime is. Show that if the Mersenne prime M_n is prime, then n is prime.

What can you say about the converse (no proof required)?

(b) (i) Show that in a ring R of complex numbers, for all prime numbers $p > 0$ the following is true:

$(a+b)^p \equiv a^p + b^p \bmod p$ for all $a, b \in R$.

(ii) State and prove an analogue of Fermat's Little Theorem for $\mathbb{Z}[i]$. You may use the result in (i).

(c) (i) Suppose that p is an odd prime and M_p is divisible by an odd prime q.

Show that q is congruent to 1 modulo p and hence congruent to ± 1 modulo 8.

(Hint for the second statement: Show that 2 is a quadratic residue modulo q.)

(ii) Suppose that $q > 3$ is prime and congruent to 3 modulo 4.

Show that if $2q+1$ is prime, then M_q is composite.

[Hint: Show that $2q+1$ divides M_q. Fermat's Little Theorem is useful.]