UNIVERSITY OF BIRMINGHAM

School of Mathematics

Programmes in the School of Mathematics Final Examination

Programmes including Mathematics Final Examination

06 14982

MSM 3P05: Number Theory

Summer Examinations 2009

Time allowed: 3 hours

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

No calculator is permitted in this examination.

1. (a) Determine the factors of 8 in $\mathbb{Z}[\sqrt{-3}]$.

(b) (i) Write down two essentially different factorizations of 8 into products of irreducibles in $\mathbb{Z}[\sqrt{-3}]$. Prove that the factors in your factorizations are indeed irreducible.

(ii) Explain briefly why $\mathbb{Z}[\sqrt{-3}]$ is not a Euclidean ring.

(c) Show that there exists $\alpha \in \mathbb{Z}[\sqrt{-3}]$ such that 8 and α do not have a highest common factor.

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

$$21x \equiv 12 \bmod 159.$$

(b) Let a and b be integers and n be a natural number. Consider the equation

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

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

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

Suppose that x_0 is a solution to $(*)$.

(ii) Suppose that y is also a solution to $(*)$. Prove that

$$y = x_0 + k\frac{n}{h}$$

for some integer k.

(iii) Deduce that every solution to $(*)$ is on the following list:

$$x_0,\ x_0+\frac{n}{h},\ x_0+2\frac{n}{h},\ldots,x_0+(h-1)\frac{n}{h}.$$

(c) Let n be a natural number and a,b,c,d,k,l be integers. Consider the system of equations

$$\left.\begin{array}{rcl} ax + by & \equiv & k \bmod n \\ cx + dy & \equiv & l \bmod n \end{array}\right\}. \qquad (**)$$

Let $D = ad - bc$.

Prove that if $\mathrm{hcf}(D,n) = 1$, then $(**)$ has a solution.

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

(ii) Use Gauss' Law of Quadratic Reciprocity to calculate the following Legendre Symbols:

$$\left(\frac{5}{19}\right), \left(\frac{15}{43}\right) \text{ and } \left(\frac{14}{47}\right).$$

(b) (i) State Fermat's Little Theorem. Deduce that if p is a prime and a is a quadratic residue modulo p, then

$$a^{\frac{1}{2}(p-1)} \equiv 1 \bmod p.$$

(ii) State Gauss' Lemma and use it to evaluate the Legendre Symbol

$$\left(\frac{3}{13}\right).$$

(c) State the Geometric Interpretation of Gauss' Lemma. Give an outline of how the Geometric Interpretation is deduced from Gauss' Lemma. There are three main steps in this. Fill in the details of one of these steps.

4. In this question you may assume any results related to unique factorization, provided that they are stated clearly.

(a) 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.

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

(ii) Write down a factorization of $x^2 + y^2$ in the Gaussian integers and show that the two factors are coprime.

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

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

or

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

(b) Let R be a ring of complex numbers. Assume that R is a Unique Factorization Domain that has only finitely many units. Let k be a non-zero member of R.

(i) Prove that the equation

$$x^2 - y^2 = k$$

has only finitely many solutions with $x, y \in R$.

(ii) Is it possible to draw the same conclusion without the hypothesis that R has only finitely many units? Justify your answer.

5. (a) Consider the equation

$$x^3+y^3=z^3. \qquad (*)$$

(i) Suppose that (x,y,z) is a non-trivial integer solution to $(*)$. Show that if d is a common prime factor of x and y, then d is a factor of z. Deduce that $(x/d, y/d, z/d)$ is also a non-trivial integer solution to $(*)$.

(ii) Deduce that if $(*)$ possesses a non-trivial integer solution, then there is a solution (x,y,z) in which x and y are coprime.

(iii) Suppose that (x,y,z) is a non-trivial integer solution to $(*)$. Show that at least one of x, y or z is a multiple of 3. [Hint: consider congruences modulo 9.]

(b) Let $\omega = e^{2\pi i/3} = \frac{1}{2}(-1+\sqrt{-3})$, $\mathbb{Z}[\omega] = \{ a+b\omega \mid a,b \in \mathbb{Z} \}$ and define $N : \mathbb{Z}[\omega] \longrightarrow \mathbb{Z}$ by $N(\alpha) = \alpha\alpha^*$. Set $\lambda = 1-\omega$.

(i) Let $\alpha = a+b\omega$ with $a,b \in \mathbb{Z}$. Derive a formula for $N(\alpha)$ in terms of a and b.

(ii) Prove that λ is irreducible in $\mathbb{Z}[\omega]$ and that λ^2 is associate to 3.

(iii) Consider the following:

$$\left.\begin{array}{l} x^3+y^3 = uz^3, \quad x,y,z \in \mathbb{Z}[\omega] - \{ 0 \}, \\ u \text{ is a unit of } \mathbb{Z}[\omega], \\ x \text{ and } y \text{ are coprime in } \mathbb{Z}[\omega], \text{ and} \\ \lambda \mid z \text{ but } \lambda \nmid x \text{ and } \lambda \nmid y. \end{array}\right\} \qquad (**)$$

Prove that if $(*)$ has a non-trivial integer solution, then $(**)$ has a solution.

(c) Let p be an odd prime and suppose that $x^p + y^p = z^p$ has a solution with x, y and z non-zero integers.

(i) Show that we may assume that any pair of x, y, z are coprime and that there exists $z' \in \mathbb{Z}$ such that $x^p + y^p + z'^p = 0$. Deduce that

$$-x^p = (y+z')(y^{p-1} - y^{p-2}z' + \cdots - yz'^{p-2} + z'^{p-1}).$$

(ii) Assume that p is not a factor of x, y or z'. Show that the above two factors are coprime.

[Hint: Assume that q is a common prime factor. Show that q is a factor of py^{p-1}.]

(iii) Deduce that $x+y, y+z'$ and $z'+x$ are p^{th} powers of integers.

6. (a) (i) Let p be a prime and suppose that $x \in \mathbb{N}$ is such that $x^2 \equiv 1 \mod p$ but $x \not\equiv 1 \mod p$. Prove that $x \equiv -1 \mod p$.

(ii) State the Miller–Rabin Test.

(b) (i) Define the following: Mersenne Number, Mersenne Prime.

(ii) True or false? (No proof required.)

- If M_n is prime, then n is prime.
- If n is prime, then M_n is prime.

(iii) Let $n \geq 3$ be prime. What is M_n congruent to modulo 12? Justify your answer.

(iv) Deduce that M_n has a prime factor q with $q \equiv \pm 5 \mod 12$.

(v) State the Lucas Test.

(c) A number is **perfect** if it is the sum of its positive proper factors. Suppose that $n \in \mathbb{N}$ is perfect and that $n = 2^m p$ with $m \geq 1$ and p an odd prime.
Prove that p is a Mersenne prime.
[Hint: use the facts that $2n = \sigma(n)$ and that σ is multiplicative.]