MA40238 NUMBER THEORY (2014/15 SEMESTER 1)
MOCK EXAMINATION

Problem 1.

(a) What does it mean to say a and b are *congruent* modulo m, where $a, b, m \in \mathbb{Z}$ and $m \neq 0$? [2]

(b) Define the Möbius μ-function. [2]

(c) State a sufficient and necessary condition for the congruence equation $ax \equiv b \pmod{m}$ to have solutions, where $a, b, m \in \mathbb{Z}$, $a \neq 0$ and $m \neq 0$. [2]

(d) Find all integer solutions to the equation $7x - 13y = 2$. [3]

(e) Show that 2 is a primitive root modulo 11. [3]

(f) State and prove the Chinese Remainder Theorem: Suppose that $m_1, m_2, \cdots, m_k$ are pairwise coprime non-zero integers and $m = m_1 m_2 \cdots m_k$. Then the system of congruences

$$x \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \quad \cdots, \quad x \equiv b_k \pmod{m_k}$$

has a unique solution modulo m. [4]

(g) Let p and q be positive primes, $p \neq q$. Prove that

$$p^q + q^p \equiv p + q \pmod{pq}.$$

[4]

Date: January 16, 2015.

Problem 2.

(a) What does it mean to say a is a *quadratic residue* modulo m, where $a, m \in \mathbb{Z}$, $m \neq 0$ and $\mathrm{hcf}(a, m) = 1$? [2]

(b) Define the *Jacobi symbol* $(\frac{a}{b})$, where $a, b \in \mathbb{Z}$, b is positive and odd. [2]

(c) Which of the follow four expressions has/have value 1? Justify your answers. If you use any results proved in class, state them clearly.

$$\left(\frac{-1}{15}\right), \qquad \left(\frac{9}{15}\right), \qquad \left(\frac{17}{15}\right)\left(\frac{15}{17}\right).$$

[3]

(d) Compute the Legendre symbol $(\frac{219}{383})$. [3]

(e) Using Euler's criterion proved in lectures, which should be stated clearly, prove the following formula: for any positive odd prime p,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4; \\ -1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

[3]

(f) State and prove Gauss' Lemma. [3]

(g) Let p be a positive prime, $p \equiv 3 \pmod 4$. Prove that there are infinitely many positive odd primes q, which are quadratic non-residues modulo p. [4]

Problem 3.

(a) Write down the definition of an *algebraic number field.* [2]

(b) Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field ($d \neq 1$ and square-free). Write down the set of all algebraic integers in K. Write down an integral basis for $\mathcal{O}_K$. [3]

In parts (c), (d), (e) and (f), K is an arbitrary number field of degree n over $\mathbb{Q}$, and $\mathcal{O}_K$ is the ring of algebraic integers in K.

(c) Define the *discriminant* of the n-tuple $\alpha_1, \alpha_2, \cdots, \alpha_n \in K$. Define the *discriminant* of a non-zero ideal I in $\mathcal{O}_K$ and the *discriminant* of K. [3]

(d) Let α be a non-zero element in $\mathcal{O}_K$, and I be the principal ideal generated by α. State a result proved in class, which relates the two norms $N(\alpha)$ and $N(I)$. [2]

(e) State the ascending chain condition for $\mathcal{O}_K$. [2]

(f) State the theorem of unique factorisation of ideals in $\mathcal{O}_K$. Prove the uniqueness part of this theorem. [4]

(g) Let $V = \{\gamma_1, \gamma_2, \cdots, \gamma_n\}$ be a finite set of non-zero complex numbers. Suppose a complex number α has the property that for each $i = 1, 2, \cdots, n$, the product $\alpha\gamma_i$ can be written as a rational linear combination of elements in the set V. Prove that α is an algebraic number. [4]

Problem 4.

In parts (a) and (b), K is an arbitrary number field, and $\mathcal{O}_K$ is the ring of algebraic integers in K.

(a) What are the definition of an *ideal class* in $\mathcal{O}_K$, the *ideal class group* of K and the *class number* of K? [4]

(b) State a result proved in lectures, which relates the class number h_K and a property of the ring of algebraic integers $\mathcal{O}_K$. [2]

(c) What is a *lattice* of rank 2 in $\mathbb{R}^2$? What is the *fundamental domain* of the lattice? [2]

(d) State and prove Minkowski's Theorem. [4]

(e) Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field, where $d \neq 1$ is a square-free integer. Write down the Minkowski bound for K. [2]

(f) Compute the class number of $K = \mathbb{Q}(\sqrt{13})$. [2]

(g) Consider the quadratic field $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer, $d < -2$ and $d \not\equiv 1 \pmod 4$. Let $\mathcal{O}_K$ be the ring of algebraic integers in K. Prove that there is an ideal I in $\mathcal{O}_K$, such that $N(I) = 2$ and I is not principal. Conclude that $h_K \geqslant 2$. [4]