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

Problem 1.

(a) We say a and b are congruent modulo m if m divides $a - b$. [2]

(b) For any positive integer n, $\mu(n) = 1$ if $n = 1$; $\mu(n) = 0$ if n is not square-free; $\mu(n) = (-1)^l$ if $n = p_1 p_2 \cdots p_l$ is the product of l distinct primes. [2]

(c) Let $\operatorname{hcf}(a, m) = d$, then the congruence equation $ax \equiv b \pmod{m}$ has solutions if and only if $d \mid b$. [2]

(d) Consider the congruence $7x \equiv 2 \pmod{13}$. By adding multiples of 13 on the right-hand side we get $7x \equiv 2 \equiv 28 \pmod{13}$. By cancellation law we get $x \equiv 4 \pmod{13}$. Hence $x = 13k + 4$ for any $k \in \mathbb{Z}$. By substitution, we have $7(13k + 4) - 13y = 2$, hence $y = 7k + 2$. The solutions to the original equation is given by $x = 13k + 4$, $y = 7k + 2$ where $k \in \mathbb{Z}$. [3]

(e) Since 11 is an odd prime, $\mathbb{Z}_{11}^*$ is a cyclic group of order 10. To show 2 is a primitive root modulo 11, we need to show 2 has order 10 modulo 11. In other words, its order is not $1, 2$ or 5. Indeed, $2^1 \equiv 2 \pmod{11}$, $2^2 \equiv 4 \pmod{11}$, $2^5 = 32 \equiv 10 \pmod{11}$. None of them is congruent to 1 modulo 29, hence 2 is a primitive root modulo 11. [3]

(f) We prove it by induction on k. For $k = 1$ there is nothing to prove. For $k = 2$, an integer solution to $x \equiv b_1 \pmod{m_1}$ is of the form $x = m_1 q + b_1$. So we need to have $m_1 q + b_1 \equiv b_2 \pmod{m_2}$, or $m_1 q \equiv b_2 - b_1 \pmod{m_2}$. Since $\operatorname{hcf}(m_1, m_2) = 1$, it has a unique solution for q, say $q \equiv q_0 \pmod{m_2}$. Or equivalently, $q = m_2 r + q_0$ for any $r \in \mathbb{Z}$. Hence $x = m_1 m_2 r + (m_1 q_0 + b_1)$ for any $r \in \mathbb{Z}$, which is the unique solution for x modulo $m = m_1 m_2$.

For general k, suppose we have proved the result for $k - 1$. That is, the first $k - 1$ congruence equations have a unique common solution $x \equiv s \pmod{m'}$ for some s, where $m' = m_1 m_2 \cdots m_{k-1}$. Then the problem reduces to a system of two congruences $x \equiv s \pmod{m'}$ and $x \equiv b_k \pmod{m_k}$. By the case for $k = 2$ above, there is a unique solution for x modulo $m = m' m_k$. This finishes the induction. [4]

(g) We have $(p^q + q^p) - (p + q) = (p^q - p) + (q^p - q)$. By Fermat's Little Theorem, since p and q are distinct primes, $p^{q-1} \equiv 1 \pmod{q}$, hence $p^{q-1} - 1$ is a multiple of q. Therefore $p^q - p = p(p^{q-1} - 1)$ is a multiple of pq. By switching p and q we know that $q^p - q = q(q^{p-1} - 1)$ is also a multiple of pq, so is the sum $(p^q - p) + (q^p - q)$. It follows that $p^q + q^p \equiv p + q \pmod{pq}$. [4]

Date: January 16, 2015.

Problem 2.

(a) We say a is a quadratic residue modulo m if $x^2 \equiv a \pmod m$ has a solution. [2]

(b) Let $b = p_1 p_2 \cdots p_m$ be its prime factorisation, where $p_1, p_2, \cdots, p_m$ are not necessarily distinct primes. The Jacobi symbol $(\frac{a}{b})$ is defined by $(\frac{a}{b}) = (\frac{a}{p_1})(\frac{a}{p_2})\cdots(\frac{a}{p_m})$. [2]

(c) Since $(\frac{-1}{b}) = 1$ if $b \equiv 1 \pmod 4$ and -1 if $b \equiv -1 \pmod 4$, we get $(\frac{-1}{15}) = -1$. By definition, $(\frac{9}{15}) = (\frac{9}{3})(\frac{9}{5}) = 0$ because 9 is a multiple of 3. By quadratic reciprocity for Jacobi symbols, when a and b are coprime positive odd integers, we have $(\frac{a}{b})(\frac{b}{a}) = 1$ if $a \equiv 1 \pmod 4$ or $b \equiv 1 \pmod 4$, and -1 if $a \equiv b \equiv 3 \pmod 4$. Since $17 \equiv 1 \pmod 4$, we have $(\frac{17}{15})(\frac{15}{17}) = 1$. Hence only the third expression takes value 1. [3]

(d) Since $219 \equiv 383 \equiv 3 \pmod 4$, by quadratic reciprocity for Jacobi symbols, we have $(\frac{219}{383}) = -(\frac{383}{219}) = -(\frac{164}{219}) = -(\frac{4}{219})(\frac{41}{219}) = -(\frac{41}{219})$. Since $41 \equiv 1 \pmod 4$, we have $-(\frac{41}{219}) = -(\frac{219}{41}) = -(\frac{14}{41}) = -(\frac{2}{41})(\frac{7}{41}) = -(\frac{7}{41})$, where the last equality is due to $41 \equiv 1 \pmod 8$. Again by $41 \equiv 1 \pmod 4$, we get $-(\frac{7}{41}) = -(\frac{41}{7}) = -(\frac{-1}{7}) = -(-1) = 1$, where the last equality is due to $7 \equiv 3 \pmod 4$. [3]

(e) *Euler's criterion.* For any integer a and odd prime p, we have $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod p$.

It follows that $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$. If $p \equiv 1 \pmod 4$, then $\frac{p-1}{2}$ is an even integer, hence $(\frac{-1}{p}) = 1$; if $p \equiv 3 \pmod 4$, then $\frac{p-1}{2}$ is an odd integer, hence $(\frac{-1}{p}) = -1$. [3]

(f) *Gauss' Lemma.* Let p be an odd prime, $r = \frac{p-1}{2}$, $p \nmid a$, and μ the number of integers among $a, 2a, \cdots, ra$ which have negative least residues modulo p. Then $\left(\dfrac{a}{p}\right) = (-1)^\mu$.

Proof. Let m_l or $-m_l$ be the least residue of la modulo p, where m_l is positive. As l ranges between 1 and r, μ is clearly the number of minus signs that occur in this way. We claim that $m_l \neq m_k$ for any $l \neq k$ and $1 \leqslant l, k \leqslant r$. For, if $m_l = m_k$, then $la \equiv \pm ka \pmod p$, and since $p \nmid a$ this implies that $l \pm k \equiv 0 \pmod p$. The latter congruence is impossible since $l \neq k$ and $|l \pm k| \leqslant |l| + |k| \leqslant p - 1$. It follows that the sets $\{1, 2, \cdots, r\}$ and $\{m_1, m_2, \cdots, m_r\}$ coincide. Multiply the congruences

$$1 \cdot a \equiv \pm m_1 \pmod p, \quad 2 \cdot a \equiv \pm m_2 \pmod p, \quad \cdots, \quad r \cdot a \equiv \pm m_r \pmod p.$$

Notice that the number of negative signs on the right hand sides is μ, we obtain

$$r! \cdot a^r \equiv (-1)^\mu \cdot r! \pmod p.$$

Since $p \nmid r!$, this yields

$$a^r \equiv (-1)^\mu \pmod p.$$

By Euler's criterion $a^r = a^{\frac{p-1}{2}} \equiv (\frac{a}{p}) \pmod p$ and the result follows. [3]

(g) We prove by contradiction. Assume there are only finitely many odd primes which are quadratic non-residues modulo p, given by the set $S = \{q_1, q_2, \cdots, q_s\}$. We consider $N = 2pq_1q_2\cdots q_s - 1$. We realise that $N \equiv -1 \pmod p$, hence $(\frac{N}{p}) = (\frac{-1}{p}) = -1$, since $p \equiv 3 \pmod 4$. Since $N > 1$ is odd, we have the factorisation $N = p_1 p_2 \cdots p_t$ where $p_1, p_2, \cdots, p_t$ are not necessarily distinct odd primes. For each $i = 1, 2, \cdots, t$, we have $p_i \notin S$ and $p_i \neq p$, hence p_i is a quadratic residue modulo p, which implies $(\frac{p_i}{p}) = 1$. Therefore $(\frac{N}{p}) = (\frac{p_1}{p})(\frac{p_2}{p})\cdots(\frac{p_t}{p}) = 1$. Contradiction. [4]

Problem 3.

(a) An algebraic number field is a field K, such that $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, and K has finite degree (or finite dimensional vector space) over $\mathbb{Q}$. [2]

(b) Algebraic integers in $K = \mathbb{Q}(\sqrt{d})$ are given by $\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$ if $d \equiv 2$ or $3 \pmod 4$; $\left\{a + b \cdot \frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\right\}$ if $d \equiv 1 \pmod 4$. An integral basis for $\mathcal{O}_K$ is given by $\{1, \sqrt{d}\}$ if $d \equiv 2$ or $3 \pmod 4$; $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ if $d \equiv 1 \pmod 4$. [3]

(c) We define the discriminant of the n-tuple to be

$$\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = \det \begin{pmatrix} T(\alpha_1\alpha_1) & T(\alpha_1\alpha_2) & \cdots & T(\alpha_1\alpha_n) \\ T(\alpha_2\alpha_1) & T(\alpha_2\alpha_2) & \cdots & T(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ T(\alpha_n\alpha_1) & T(\alpha_n\alpha_2) & \cdots & T(\alpha_n\alpha_n) \end{pmatrix}.$$

For any non-zero ideal I in $\mathcal{O}_K$, the discriminant of an integral basis for I is called the discriminant of the ideal I. The discriminant of $\mathcal{O}_K$ (or the discriminant of an integral basis for $\mathcal{O}_K$) is called the discriminant of the number field K. [3]

(d) Let $I = (\alpha)$ for some non-zero element $\alpha \in \mathcal{O}_K$. Then $N(I) = |N(\alpha)|$. [2]

(e) In the ring of integers $\mathcal{O}_K$, every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ stabilises. In other words, there is a positive integer N such that $I_m = I_{m+1}$ for all $m \geqslant N$. [2]

(f) *Theorem of Unique Factorsiation.* Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then every non-zero proper ideal in $\mathcal{O}_K$ can be uniquely written as a finite product of prime ideals up to reordering factors.

Proof of Uniqueness. Suppose $P_1P_2\cdots P_r = I = Q_1Q_2\cdots Q_s$ where P_i's and Q_j's are prime ideals. Then $P_1 \supseteq Q_1Q_2\cdots Q_s$. We claim that $P_1 \supseteq Q_j$ for some Q_j. If not, then for each $j = 1, 2, \cdots, s$, we can find $a_j \in Q_j \backslash P_1$. Since P_1 is a prime ideal, $a_1a_2\cdots a_s \notin P_1$. However $a_1a_2\cdots a_s \in Q_1Q_2\cdots Q_s \subseteq P_1$. Contradiction.

Therefore, by renumbering the Q_j's if necessary, we can assume that $P_1 \supseteq Q_1$. Since Q_1 is a prime ideal, it is also a maximal ideal, so we conclude that $P_1 = Q_1$.

Using cancellation law we obtain $P_2\cdots P_r = Q_2\cdots Q_s$. Continuing in the same way we eventually find that $r = s$ and $P_i = Q_i$ for all i after renumbering. [4]

(g) By assumption, for each $i = 1, 2, \cdots, n$, we can write $\alpha\gamma_i = \sum_{j=1}^{n} a_{ij}\gamma_j$, where each $a_{ij} \in \mathbb{Q}$. Using the language of linear algebra, we have $\alpha \cdot \mathbf{v} = \mathbf{M} \cdot \mathbf{v}$, where

$$\mathbf{M} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}, \quad \mathbf{v} = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_n \end{pmatrix}.$$

Since $\mathbf{v} \neq 0$, we see that α is an eigenvalue of the square matrix $\mathbf{M}$. In other words, α is a solution of the equation $\det(x \cdot \mathbf{I} - \mathbf{M}) = 0$. Since all entries of $\mathbf{M}$ are rational numbers, the left-hand side of the equation is a polynomial with rational coefficients. Therefore α is an algebraic number. [4]

Problem 4.

(a) Two non-zero ideals I, J in $\mathcal{O}_K$ are said to be equivalent, $I \sim J$, if there exist non-zero $\alpha, \beta \in \mathcal{O}_K$, such that $(\alpha)I = (\beta)J$. This is an equivalence relation. Each equivalence class is called an ideal class. The group of ideal classes in $\mathcal{O}_K$ under multiplication is called the ideal class group of K. The order of the ideal class group is called the class number of K. [4]

(b) We have $h_K = 1$ if and only if $\mathcal{O}_K$ is a PID. [2]

(c) Let e_1, e_2 be two linearly independent vectors in $\mathbb{R}^2$. The abelian group $L = \{m_1 e_1 + m_2 e_2 \mid m_1, m_2 \in \mathbb{Z}\}$ is called a lattice of rank 2 in $\mathbb{R}^2$. The fundamental domain of L is the set $T = \{a_1 e_1 + a_2 e_2 \mid a_1, a_2 \in \mathbb{R}, 0 \leqslant a_1 < 1, 0 \leqslant a_2 < 1\}$. [2]

(d) *Minkowski's Theorem.* Let L be a lattice of rank 2 in $\mathbb{R}^2$ with fundamental domain T. Let X be a centrally symmetric convex subset of $\mathbb{R}^2$. If $\mathrm{vol}(X) > 4\,\mathrm{vol}(T)$, then X contains a non-zero point of L.

Proof. We first shrink X to half of its size in length; precisely speaking, we consider $Y = \{p \in \mathbb{R}^2 \mid 2p \in X\}$. Then $\mathrm{vol}(Y) = \frac{1}{4}\mathrm{vol}(X) > \mathrm{vol}(T)$.

For every $h \in L$, we define $h + T = \{h + p \mid p \in T\}$ which is the transport of the fundamental domain along the vector h. It is clear that $\mathbb{R}^2$ becomes the disjoint union of these parallelograms. Let $Y_h = Y \cap (h+T)$ is the part of Y which lies in the parallelogram $h+T$ for each $h \in L$, then Y becomes the disjoint union of all Y_h's, hence $\sum_{h\in L} \mathrm{vol}(Y_h) = \mathrm{vol}(Y) > \mathrm{vol}(T)$. We transport each Y_h back to the fundamental domain, say $Y'_h = \{q \in T \mid h + q \in Y_h\}$. Then $\sum_{h\in L} \mathrm{vol}(Y'_h) = \sum_{h\in L} \mathrm{vol}(Y_h) > \mathrm{vol}(T)$. Since each $Y'_h \subseteq T$, this inequality implies they are not disjoint. Therefore there exist $h_1, h_2 \in L$, $h_1 \neq h_2$, such that we can find some $q \in Y'_{h_1} \cap Y'_{h_2}$. That implies $p_1 = h_1 + q \in Y_{h_1} \subseteq Y$ and $p_2 = h_2 + q \in Y_{h_2} \subseteq Y$, hence we found $p_1, p_2 \in Y$, such that $p_1 - p_2 = h_1 - h_2 \in L$.

Since $p_1, p_2 \in Y$, we have $2p_1, 2p_2 \in X$. Since X is centrally symmetric, $-2p_2 \in X$. Since X is convex, $\frac{1}{2}(2p_1) + \frac{1}{2}(-2p_2) \in X$, which is $h_1 - h_2$, a non-zero point in L. [4]

(e) The Minkowski bound M_K is $\frac{2}{\pi}|\Delta_K|^{\frac{1}{2}}$ if $d < 0$; and $\frac{1}{2}|\Delta_K|^{\frac{1}{2}}$ if $d > 0$. [2]

(f) The Minkowski bound is $M_K = \frac{1}{2}\sqrt{13} < 2$, hence each ideal class contains an ideal of norm at most 1, which has to be $\mathcal{O}_K$. Therefore the class number of $\mathbb{Q}(\sqrt{13})$ is 1. [2]

(g) By the formula given in class, since $d \not\equiv 1 \pmod 4$, we have the factorisation $(2) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of norm 2. Take $I = \mathfrak{p}$, then we have an ideal with $N(I) = 2$. It remains to show that I is not principal.

We prove by contradiction. Assume there exists a non-zero $\alpha \in \mathcal{O}_K$ such that $I = (\alpha)$, then $|N(\alpha)| = N(I) = 2$, hence $N(\alpha) = \pm 2$. Since $d \not\equiv 1 \pmod 4$, we can write $\alpha = a + b\sqrt{d}$ for some $a, b \in \mathbb{Z}$. Then $N(\alpha) = a^2 - b^2 d = a^2 + b^2(-d) = \pm 2$. Since $-d > 0$, we must have $a^2 + b^2(-d) = 2$. Since $-d > 2$, we must have $b = 0$, otherwise $a^2 + b^2(-d) > 0 + 2 = 2$. It follows that $a^2 = 2$, which has no integer solution. Contradiction.

Since I is not a principal ideal, I and $\mathcal{O}_K$ are not in the same ideal class. Hence there are at least two ideal classes. In other words, $h_K \geqslant 2$. [4]