NANYANG TECHNOLOGICAL UNIVERSITY

SEMESTER I EXAMINATION 2024-2025

MH3210 – NUMBER THEORY

November 2024 TIME ALLOWED: 2 HOURS

INSTRUCTIONS TO CANDIDATES

1. This examination paper contains **SEVEN (7)** questions and comprises **ELEVEN (11)** printed pages including **EIGHT (8)** pages of Appendix.
2. Answer **ALL** questions. The marks for each question are indicated at the beginning of each question.
3. Answer each question beginning on a **FRESH** page of the answer book.
4. This is a **CLOSED BOOK** examination.
5. Candidates may use calculators. However, they should write down systematically the steps in the workings.

QUESTION 1 (15 marks)

Solve the set of simultaneous congruences:

$$\begin{aligned} x &\equiv 1 \pmod 3, \\ x &\equiv 1 \pmod 6, \\ 3x &\equiv 1 \pmod 7, \\ x &\equiv 1 \pmod 8, \\ x &\equiv 0 \pmod{11}. \end{aligned}$$

QUESTION 2 (15 marks)

Solve $x^3 + 2x^2 + 9 \equiv 0 \pmod{125}$.

QUESTION 3 (12 marks)

Without using the fundamental theorem of arithmetic, prove the following.

(a) If $a|bc$, then $a|(a,b)\cdot(a,c)$.

(b) If $a|(a,b)\cdot c$ and $b|(a,b)\cdot c$, then $ab|(a,b)^2\cdot c$.

QUESTION 4 (12 marks)

Let $S(1) = 1$ and for $n > 1$, let $S(n)$ denote the number of square free divisors of n. Let $\omega(n)$ denote the number of distinct prime divisors of n. In other words, if $n = p_1^{\ell_1} p_2^{\ell_2} \cdots p_k^{\ell_k}$ where p_i's are distinct primes and all $\ell_i > 0$, then $\omega(n) = k$.

(a) Show that $S(n) = \sum_{d|n} |\mu(d)|$ where $\mu(n)$ is the Möbius function.

(b) Using Part (a) or otherwise, show that $S(n) = 2^{\omega(n)}$.

QUESTION 5 **(12 marks)**

Let $n \geq 30$ be an integer. Prove that there is a prime $p > 3$ such that

$$n < 6p < 2n.$$

QUESTION 6 **(24 marks)**

(a) Let p be a prime number such that $p \equiv 3 \pmod 4$, and suppose a is a quadratic residue modulo p.

(i) Prove that $x = a^{(p+1)/4}$ is a solution to the congruence $x^2 \equiv a \pmod p$.

(ii) Determine a solution to the congruence $x^2 \equiv 7 \pmod{787}$.

(b) Let q be a prime number satisfying $q \equiv 1 \pmod 4$, and suppose the number $r = 2q + 1$ is also a prime number. Show that 2 is a primitive root modulo r.

QUESTION 7 **(10 marks)**

(a) Find the continued fraction expansion of $\sqrt{30}$.

(b) Using your answer to Part (a), determine two pairs of positive integers (x, y) satisfying

$$x^2 - 30y^2 = 1.$$

END OF PAPER

Appendix

Theorem 1. Let a, b, c, x, m, y be integers.

(a) $a|b$ and $a|c$ imply $a|(bx + cy)$ for any integers x and y;

(b) $a|b$ and $b|a$ imply $a = \pm b$;

(c) $a|b$, $a > 0$, $b > 0$, imply $a \leq b$;

Theorem 2 (The Division Algorithm)**.** Given any integers a and b with $a > 0$, there exist unique integers q and r such that $b = qa + r, 0 \leq r < a$. If $a \nmid b$, then r satisfies the stronger inequalities $0 < r < a$.

Theorem 3. Let a, b, c, d, n be integers with $n > 0$. Then

(a) For all integers k, $k \equiv k \pmod{n}$.

(b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.

(c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

(d) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.

Definition 1. A *common divisor* of integers a and b is an integer c with $c|a$ and $c|b$.

Definition 2. A *greatest common divisor* of integers a and b is a number d with the following properties :

(a) The integer d is nonnegative.

(b) The integer d is a common divisor of a and b.

(c) If e is any common divisor of a and b, then $e|d$.

Definition 3. The greatest common divisor of a and b is denoted by (a, b).

Theorem 4. Let a and b be nonzero integers. Then the smallest positive integer in the set

$$P := \{sa + tb | s, t \in \mathbb{Z} \quad \text{and} \quad sa + tb > 0\}$$

is (a, b).

Theorem 5. Let a and b be integers. Then $(a, b) = 1$ (or a and b are relatively prime) if and only if $1 = ax + by$ for some integers x and y.

Theorem 6. Let a, b and c be integers. Ther

(a) $(a, b) = (b, a)$ (commutative law),

(b) $(a, (b, c)) = ((a, b), c)$ (associative law),

(c) $(ac, bc) = |c|(a, b)$, and

(d) $(a, 1) = (1, a) = 1$. If a is non-zero, then $(a, 0) = (0, a) = |a|$.

Theorem 7 (The Euclidean Algorithm)**.** Le a and b be two positive integers, where $a \nmid b$. Let $r_0 = b, r_1 = a$, and apply the division algorithm repeatedly to obtain a set of

remainders $r_2, r_3, ..., r_n, r_{n+1}$ defined successively by the relations

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, & 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, & 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_n + r_{n+1}, & r_{n+1} = 0. \end{aligned}$$

Then r_n, the last nonzero remainder in this process is (a, b), the greatest common divisor of a, and b.

Definition 4. A *common multiple* of two integers a and b is a positive integer m with the property that $a|m$ and $b|m$.

Definition 5. The *least common multiple* of two integers a and b is an integer m such that

(a) $m > 0$,
(b) $a|m$ and $b|m$, and
(c) If c is a common multiple of a and b then $m|c$.

Theorem 8. If $m > 0$, then $[ma, mb] = m[a, b]$. Furthermore,

$$[a, b] \cdot (a, b) = ab.$$

Lemma 9. Let $(m, n) = 1$. If $m|c$ and $n|c$ then $(mn)|c$.

Theorem 10. If $ca \equiv cb \pmod{n}$ and $(c, n) = 1$, then $a \equiv b \pmod{n}$.

Corollary 11. Let p be a prime. If $p|(ab)$, then $p|a$ or $p|b$.

Theorem 12 (Fundamental Theorem of Arithmetic)**.** Every positive integer $n > 1$ can be expressed as a product of primes; this representation is unique apart from the order in which the factors occur.

Let $(a, b) = d$ and $d|m$. Let x_0 and y_0 be a particular solution of $ax + by = m$. The general solution of the equation is

$$X = \frac{b}{d}k + x_0 \quad \text{and} \quad Y = -\frac{a}{d}k + y_0, \; k \in \mathbb{Z}.$$

Theorem 13. Given integers a, b such that $(a, b) = d$ and $d|N$, the number of solutions satisfying

$$(1) \qquad ax \equiv N \pmod{b}$$

is exactly d.

Theorem 14. Let p be an odd prime. Then

$$(p-1)! \equiv -1 \pmod{p}.$$

Theorem 15 (Fermat Little Theorem)**.** If p is a prime and $p \nmid a$ then

$$a^{p-1} \equiv 1 \pmod{p},$$

or

$$a^p - a \equiv 0 \pmod{p}.$$

Definition 6. The function $\varphi(n)$ is defined to be the number of elements $1 \leq x < n$ which are relatively prime to n. The function $\varphi(n)$ is usually called *Euler's φ function.*

Theorem 16 (Euler's Theorem)**.** Suppose $(a, n) = 1$. Then

$$a^{\varphi(n)} = 1 \pmod{n}.$$

Theorem 17. For positive integers m and n such that $(m, n) = 1$,

$$\varphi(mn) = \varphi(m)\varphi(n).$$

If $n = \prod_p p^{\alpha_p}$ then

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \prod_{p|n} \left(p^{\alpha_p} - p^{\alpha_p - 1}\right).$$

Definition 7. An *arithmetical function* f is a function from $\mathbb{N}$ to $\mathbb{C}$.

Definition 8. An arithmetical function f is said to be *completely multiplicative* if $f(1) = 1$ and for all positive integers m and n,

$$f(mn) = f(m)f(n).$$

Definition 9. An arithmetical function f is said to be *multiplicative* if $f(1) = 1$ and when $(m, n) = 1$,

$$f(mn) = f(m)f(n).$$

Definition 10. Let α be an integer. Let $\sigma_\alpha(1) = 1$ and

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha.$$

Definition 11. Let f and g be two arithmetical functions. We define the *Dirichlet product* of f and g, denoted by $f * g$, as

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

Theorem 18. Let f and g be multiplicative. Then $f * g$ is multiplicative.

Definition 12. The *Möbius function* $\mu(n)$ defined by $\mu(1) = 1$ and for $n = \prod_{k=1}^{m} p_k^{\alpha_k}$,

$$\mu(n) = \begin{cases} (-1)^m & \text{if } \alpha_i = 1, 1 \leq i \leq m \\ 0 & \text{otherwise.} \end{cases}.$$

Definition 13. For positive integer n, we define $I(n) = [1/n]$.

Theorem 19. Let $I(n)$ be given by $[1/n]$. The function I is the identity function for $*$, that is, $I*f = f*I = f$ for every arithmetical function f.

Theorem 20. The Dirichlet product is commutative and associative, that is, for any arithmetical functions f, g, k, we have

$$f * g = g * f$$

and

$$(f * g) * k = f * (g * k).$$

Theorem 21 (The Möbius inversion formula)**.** If $f = g * u$, then $g = f * \mu$. Conversely, $g = f * \mu$ implies that $f = g * u$.

Theorem 22 (Bertrand's Postulate)**.** Let $n \geq 2$ be any positive integer. There is at least a prime in the interval $(n, 2n)$.

Theorem 23 (Hensel's Lemma)**.** Suppose that $f(x)$ is a polynomial with integral coefficient. If $f(a) \equiv 0 \pmod{p^j}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $t \pmod{p}$ such that $f(a + tp^j) \equiv 0 \pmod{p^{j+1}}$.

Theorem 24. Let n be the degree of $f(x) \equiv 0 \pmod{p}$. If $n \geq p$, then either

- every integer is a solution of $f(x) \equiv 0 \pmod{p}$, or
- there is a polynomial $g(x) \in \mathbb{Z}[x]$ and leading coefficient 1, such that the congruence $g(x) \equiv 0 \pmod{p}$ is of degree less than p, and the solutions of $g(x) \equiv 0 \pmod{p}$ are precisely those of $f(x) \equiv 0 \pmod{p}$.

Theorem 25 (Lagrange)**.** Let p be a prime and $f(x)$ be a non-zero polynomial. If the degree of $f(x)$ is $n < p$, then the congruence

$$f(x) \equiv 0 \pmod{p} \tag{2}$$

has at most n solutions.

Corollary 26. If $d|(p-1)$ then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Theorem 27 (Wolstenholme's congruence)**.** Let p be an odd prime. Define σ_j as follows.

$$\begin{aligned}(x-1)(x-2)\cdots(x-(p-1)) &= x^{p-1} - \sigma_1 x^{p-2} + \sigma_2 x^{p-3} - \cdots \\ &\quad + \sigma_{p-3}x^2 - \sigma_{p-2}x + \sigma_{p-1}.\end{aligned}$$

For $p \geq 5$,

$$\sigma_{p-2} \equiv 0 \pmod{p^2}.$$

Definition 14. Let m be a positive integer and a be an integer with $(a, m) = 1$. Then the *order of a modulo m* is the smallest integer h such that $a^h \equiv 1 \pmod{m}$.

Theorem 28. If a has order h modulo m and $a^k \equiv 1 \pmod{m}$ for some positive integer k, then $h|k$.

Corollary 29. If $(a, m) = 1$, then if h is the order of a modulo m, then $h|\varphi(m)$.

Lemma 30. If a has order h modulo m, then a^k has order $h/(h, k)$ modulo m.

Definition 15. If g has order $\varphi(m)$ modulo m, then g is called a primitive root modulo m.

Theorem 31. If there exists a primitive root modulo m, then there are precisely $\varphi(\varphi(m))$ primitive roots modulo m.

Lemma 32. If n is an integer ≥ 1, then

$$n = \sum_{d|n} \varphi(d).$$

Theorem 33. Primitive roots modulo p exists for odd prime p.

Theorem 34. Let p be a prime number. The number of solutions to

$$x^d \equiv 1 (\text{mod } p) \tag{3}$$

is $(d, p-1)$.

Lemma 35. Let p be an odd prime. There exists a primitive root g modulo p such that

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Lemma 36. Let g be a primitive root modulo p such that

$$g^{p-1} \not\equiv 1 (\text{mod } p^2).$$

Then for every $\alpha \geq 3$ we have

$$g^{\varphi(p^{\alpha-1})} \not\equiv 1 \pmod{p^\alpha}.$$

Theorem 37. Let $\alpha > 1$ and p be an odd prime. Then primitive roots modulo p^α exist.

Theorem 38. Let p be an odd prime. Then primitive roots modulo m exists if

$$m = 2, 4, p^\alpha \quad \text{and} \quad 2p^\alpha.$$

Lemma 39. If $\beta \geq 3$ then primitive roots modulo 2^β do not exist.

Theorem 40. Suppose $m = 1, 2, 4, p^\alpha$ or $2p^\alpha$, where p is an odd prime. Let $(a, m) = 1$ and let $d = (\varphi(m), n)$. The congruence

$$x^n \equiv a (\text{mod } m) \tag{4}$$

is solvable if and only if

$$a^{\varphi(m)/d} \equiv 1 (\text{mod } m).$$

In the case when the congruence is solvable, there are exactly $(n, \varphi(m))$ solutions.

Theorem 41 (Euler's Criterion)**.** The congruence equation

$$x^2 \equiv a (\text{mod } p)$$

is solvable if and only if

$$a^{(p-1)/2} \equiv 1 (\text{mod } p).$$

Definition 16. For $(a, p) = 1$, we say that a is a quadratic residue modulo p if $x^2 \equiv a (\text{mod } p)$ is solvable. Otherwise, we say that a is a quadratic non-residue modulo p.

Theorem 42. Let p be a prime and let a be an integer such that $(a,p)=1$. Consider

$$S := \{a, 2a, \cdots, \frac{p-1}{2}a\}$$

and let

$$T := \{s(\text{mod } p) | s \in S\},$$

with elements in T between 0 and $p-1$. Suppose there are m elements in T which are greater than $p/2$, then

$$\left(\frac{a}{p}\right) = (-1)^m.$$

Theorem 43. Let p and q be distinct primes. Then we have

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$
$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$$
$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Definition 17. Let Q be a positive odd integer so that

$$Q = q_1 q_2 \cdots q_s$$

where q_i are not necessarily distinct. The Jacobi symbol is defined by

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right)$$

where the expressions on the right hand side involving q_j are the Legendre symbols.

Theorem 44. If Q is odd positive integer, then

$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$$
$$\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1)}{8}}$$
$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Lemma 45. Let p be an odd prime. We have

$$\sum_{m(\text{mod } p)}\left(\frac{m}{p}\right) = 0,$$

where $\sum_{m(\text{mod } p)}$ denote the sum over any complete set of residues modulo p.

Lemma 46. Let p be an odd prime. We have

$$\sum_{m(\text{mod } p)}\left(\frac{(m-a)(m-b)}{p}\right) = \begin{cases} p-1 & \text{if } a \equiv b \ (\text{mod } p), \\ -1 & \text{if } a \not\equiv b \ (\text{mod } p). \end{cases}$$

Theorem 47. Let $p \equiv 1 \ (\text{mod } 4)$ be a prime. If ℓ is a quadratic non-residue modulo p, then

$$\left(\frac{1}{2}\sum_{n=1}^{p}\left(\frac{n(n^2-1)}{p}\right)\right)^2 + \left(\frac{1}{2}\sum_{n=1}^{p}\left(\frac{n(n^2-\ell)}{p}\right)\right)^2 = p.$$

Definition 18. Let $d > 1$. A diophantine equation $x^2 - dy^2 = 1$ is known as Pell's equation.

Definition 19. Let $a_0, a_1, a_2, \cdots$ be an infinite sequence of integers, all positive except perhaps a_0. We define two sequences of integers $\{h_n\}$ and $\{k_n\}$ inductively as follows :

$$h_{-2} = 0, h_{-1} = 1, h_i = a_i h_{i-1} + h_{i-2} \quad \text{for } i \geq 0$$

$$k_{-2} = 1, k_{-1} = 0, k_i = a_i k_{i-1} + k_{i-2} \quad \text{for } i \geq 0.$$

Theorem 48. For any positive real number x,

$$< a_0, a_1, \cdots, a_{n-1}, x >= \frac{x h_{n-1} + h_{n-2}}{x k_{n-1} + k_{n-2}}.$$

Theorem 49. Let $r_n =< a_0, a_1, \cdots, a_n >$, then

$$r_n = \frac{h_n}{k_n}.$$

Theorem 50. For $i \geq 1$, the following identities hold:

$$h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1}$$

$$r_i - r_{i-1} = \frac{(-1)^{i-1}}{k_i k_{i-1}}$$

$$h_i k_{i-2} - h_{i-2} k_i = (-1)^i a_i$$

and

$$r_i - r_{i-2} = \frac{(-1)^i a_i}{k_i k_{i-2}}.$$

Theorem 51. The sequence $\{r_{2n}\}$ is monotonic increasing, bounded above by r_1, and the sequence $\{r_{2n-1}\}$ is monotonic decreasing and bounded below by r_0. The limit $\lim_{n\to\infty} r_n$ exists.

Theorem 52. If a/b is a rational number with positive denominator such that

$$\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{h_n}{k_n}\right|$$

for some $n \geq 1$, then $b > k_n$. In fact, if

$$|\xi b - a| < |\xi k_n - h_n|$$

for some $n \geq 0$, then $b \geq k_{n+1}$.

Theorem 53. Let ξ denote any irrational number. If there is a rational number a/b with $b > 1$ and $(a, b) = 1$ such that

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

then a/b equals one of the convergents of the simple continued fraction of ξ.

Definition 20. A continued fraction is pure periodic if there exists a positive integer m such that

$$a_{m+k} = a_k,$$

for all integers $k \geq 0$.

Theorem 54. Let ξ be a real number. The continued fraction expansion of ξ is purely periodic if and only if ξ is a real quadratic irrational number satisfying $\xi > 1$ and $-1 < \xi' < 0$, where

$$\xi' = a - b\sqrt{N} \quad \text{if} \quad \xi = a + b\sqrt{N}.$$

Theorem 55. Let d be a positive integer that is not a square. The number $\sqrt{d}+[\sqrt{d}]$ is purely periodic.

Theorem 56. Let d be a positive integer that is not a square. If

$$\sqrt{d}+[\sqrt{d}] =< a_0, a_1, \cdots, \xi_n >,$$

and

$$\sqrt{d} =< [\sqrt{d}], a_1, \cdots, \eta_n >,$$

then

$$\xi_n = \eta_n$$

for all integers $n \geq 1$.

Theorem 57. If d is a positive integer that is not a perfect square, then

$$h_n^2 - dk_n^2 = (-1)^{n-1} q_{n+1}$$

for all integers $n \geq -1$, where

$$\xi_{n+1} = \frac{m_{n+1} + \sqrt{d}}{q_{n+1}}.$$

Miscellaneous facts covered in the course

1. If $(a,b) = 1$ and $(a,c) = 1$ then $(a,bc) = 1$.
2. If $(a,b) = 1$, $a|n$ and $b|n$ then $ab|n$.
3. Let $(m,n) = 1$. The solutions to $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ is $x \equiv nua + mvb \pmod{mn}$ where $un \equiv 1 \pmod{m}$ and $vm \equiv 1 \pmod{n}$.
4. If f is completely multiplicative then f^{-1} is μf.
5. Let $f(a) \equiv 0 \pmod{p^j}$. If $p|f'(a)$ but $p \nmid \frac{f(a)}{p^j}$ then a does not lift to a solution of $f(x) \equiv 0 \pmod{p^{j+1}}$.
6. Let $f(a) \equiv 0 \pmod{p^j}$. If $p|f'(a)$ and $p|\frac{f(a)}{p^j}$ then a lifts to p solutions of $f(x) \equiv 0 \pmod{p^{j+1}}$.

MH3210 NUMBER THEORY

CONFIDENTIAL

Please read the following instructions carefully:

1. **Please do not turn over the question paper until you are told to do so. Disciplinary action may be taken against you if you do so.**

2. You are not allowed to leave the examination hall unless accompanied by an invigilator. You may raise your hand if you need to communicate with the invigilator.

3. Please write your Matriculation Number on the front of the answer book.

4. Please indicate clearly in the answer book (at the appropriate place) if you are continuing the answer to a question elsewhere in the book.