PURDUE UNIVERSITY

Department of Mathematics

INTRODUCTION TO NUMBER THEORY

MA 49500 and MA 59500 - SOLUTIONS

27th March 2025 75 minutes

This paper contains **SEVEN** *questions.*
All SEVEN answers will be used for assessment.
Calculators, textbooks, notes and cribsheets are **not** *permitted in this examination.*

Do not turn over until instructed.

1. [3+3+3+3+3+3=21 points] Decide which of the following statements are necessarily true, and which may be false. Mark those which are true with "T", and those which are false with "F".

   a. The reduced residue 5 is a primitive root modulo 2^{2025}.

   Solution: FALSE (We proved that there are no primitive roots modulo 2^h when $h \geq 3$).

   b. The arithmetic function $\omega(n)$ (the number of distinct prime divisors of n) is a multiplicative function.

   Solution: FALSE (One has $\omega(6) = 2 \neq 1 = \omega(2)\omega(3)$).

   c. Suppose that p and q are odd primes with $p \not\equiv q \pmod 4$. Then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$.

   Solution: TRUE (If $p \not\equiv q \pmod 4$, then either $p \equiv 1 \pmod 4$ or $q \equiv 1 \pmod 4$, in which case $(-1)^{(p-1)(q-1)/4} = 1$, so the desired conclusion follows from quadratic reciprocity).

   d. Suppose that a is an integer for which the Jacobi symbol $\left(\frac{a}{33}\right) = 1$. Then a is a quadratic residue modulo 33.

   Solution: FALSE (One has $\left(\frac{a}{33}\right) = 1$ when $\left(\frac{a}{3}\right) = -1$ and $\left(\frac{a}{11}\right) = -1$, and then a is not a quadratic residue modulo 33. Such is the case when $a = 2$).

   e. When g is a primitive root modulo 19, then either g is a primitive root modulo 19^{2025}, or $g + 19$ is a primitive root modulo 19^{2025}.

   Solution: TRUE (We proved that when p is odd and g is a primitive root modulo p, then either g or $g + p$ is a primitive root modulo p^2, and then this residue is a primitive root modulo p^k for any $k \geq 3$).

   f. Suppose that p is a prime number for which $p \equiv 2 \pmod 3$. Then the congruence $x^{(p-1)/3} \equiv 1 \pmod p$ has precisely $(p-1)/3$ solutions modulo p.

   Solution: FALSE (When $p \equiv 2 \pmod 3$, it is not even the case that $(p-1)/3$ is an integer, so this is clearly false).

   g. Suppose that p is prime with $p \equiv 3 \pmod 4$. Then $(p-1)!$ is a quadratic non-residue modulo p.

   Solution: TRUE (When p is prime, it follows from Wilson's theorem that $(p-1)! \equiv -1 \pmod p$, and moreover $\left(\frac{-1}{p}\right) = -1$ when $p \equiv 3 \pmod 4$).

2. [3+3+3+3=12 points]

   (a) Define the Möbius function $\mu(n)$.

   Solution: $\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{when } n \text{ is squarefree,} \\ 0, & \text{otherwise.} \end{cases}$

   Thus, if $n = p_1 p_2 \dots p_k$ with $p_1, \dots, p_k$ distinct primes, one has $\mu(n) = (-1)^k$, and otherwise $\mu(n) = 0$.

   (b) Define what is meant by a *quadratic residue* modulo m.

   Solution: When $(a, m) = 1$, we say that a is a **quadratic residue** modulo m provided that the congruence $x^2 \equiv a \pmod m$ is soluble.

Continued...

(c) Let $m \in \mathbb{N}$ satisfy $m \geq 2$. Define what is meant by a *primitive root* modulo m.

Solution: If g belongs to the exponent (or has order) $\phi(m)$ modulo m, then g is called a primitive root modulo m. Equivalently, the reduced residue g has the property that the smallest positive integer h with the property that $g^h \equiv 1 \pmod{m}$ is $\varphi(m)$.

(d) Let p be an odd prime number. Define the Legendre symbol $\left(\frac{a}{p}\right)$.

Solution: $\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{when } a \text{ is a quadratic residue modulo } p, \\ -1, & \text{when } a \text{ is a quadratic non-residue modulo } p, \\ 0, & \text{when } p|a. \end{cases}$

3. [6+6=12 points] (a) Let p and q be distinct odd primes. Show that

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

Solution: By the definition of the Jacobi symbol, and application of the Law of Quadratic Reciprocity, one has $\left(\frac{p+q}{pq}\right) = \left(\frac{p+q}{p}\right)\left(\frac{p+q}{q}\right) = \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$.

(b) Compute the quadratic residue symbol $\left(\frac{71}{713}\right)$.

Solution: Use quadratic reciprocity for Jacobi symbols:

$$\left(\frac{71}{713}\right) = (-1)^{(70)(712)/4}\left(\frac{713}{71}\right) = \left(\frac{3}{71}\right) = (-1)^{(2)(70)/4}\left(\frac{71}{3}\right) = -\left(\frac{-1}{3}\right) = -(-1) = 1.$$

4. [10 points] Suppose that $p > 3$ is a prime number. Find modulo p the sum, and the product, of all the distinct quadratic residues modulo p.

Solution: Let g be a primitive root modulo p. Then every reduced residue modulo p is congruent to g^α for some integer α, with $0 \leq \alpha < p-1$. Moreover, one sees that g^α is a quadratic residue modulo p if and only if α is even. The sum of all the quadratic residues distinct modulo p is therefore congruent modulo p to

$$1 + g^2 + \cdots + g^{p-3} = \frac{g^{p-1}-1}{g^2-1}.$$

But since $p > 3$ one has $(g^2-1, p) = 1$, and by Fermat's Little Theorem one has $g^{p-1} \equiv 1 \pmod{p}$. Thus the sum of all the quadratic non-residues distinct modulo p is congruent to 0 modulo p.

The product of all the quadratic residues distinct modulo p is congruent modulo p to $1 \cdot g^2 \cdot \cdots \cdot g^{p-3} = g^k$, where

$$k = \sum_{r=0}^{(p-3)/2} 2r = \left(\tfrac{1}{2}(p-1)\right)\left(\tfrac{1}{2}(p-3)\right).$$

But $g^{(p-1)/2} \equiv -1 \pmod{p}$, and so we deduce that

$$1 \cdot g^2 \cdot \cdots \cdot g^{p-3} \equiv (g^{(p-1)/2})^{(p-3)/2} \equiv (-1)^{(p-3)/2} \pmod{p}.$$

So the product of all the quadratic residues distinct modulo p is congruent to $(-1)^{(p-3)/2}$ modulo p.

Continued...

5. [3+6+6=15 points] (a) Define what is meant by a *multiplicative function.*

Solution: An arithmetical function f is said to be **multiplicative** if (a) f is not identically zero, and (b) whenever $(m,n)=1$, one has $f(mn)=f(m)f(n)$.

(b) By considering the Jacobi symbol $\left(\dfrac{2}{m}\right)$, prove that when n_1 and n_2 are odd natural numbers, then one has

$$(-1)^{(n_1^2-1)/8}(-1)^{(n_2^2-1)/8}=(-1)^{((n_1n_2)^2-1)/8}.$$

Solution: One has $(-1)^{(n_1^2-1)/8}(-1)^{(n_2^2-1)/8}=\left(\dfrac{2}{n_1}\right)\left(\dfrac{2}{n_2}\right)=\left(\dfrac{2}{n_1n_2}\right)=(-1)^{((n_1n_2)^2-1)/8}$.

(c) Define the function $f:\mathbb{N}\to\mathbb{Z}$ by putting

$$f(n)=\begin{cases}(-1)^{(n^2-1)/8}, & \text{when } n \text{ is odd,}\\ 0, & \text{when } n \text{ is even.}\end{cases}$$

Show that f is a multiplicative function.

Solution: Note first that $f(1)=(-1)^0=1$. Suppose next that $(n,m)=1$. If n is even, then $f(n)=0=f(nm)$, and thus $f(nm)=f(n)f(m)$, and similarly when m is even. When instead n and m are both odd, we have

$$f(nm)=(-1)^{\frac{1}{8}((nm)^2-1)}=(-1)^{\frac{1}{8}(n^2-1)}(-1)^{\frac{1}{8}(m^2-1)}=f(n)f(m).$$

Then we conclude that f is an arithmetic function satisfying $f(nm)=f(n)f(m)$ whenever $(n,m)=1$ which does not vanish everywhere, and so f is indeed multiplicative.

6. [4+6+6=16 points] (a) For what values of n do primitive roots modulo n exist? (Provide as complete a list as you are able, without justifying your answer).

Solution: For n equal to any of 1, 2, 4, p^r and $2p^r$, where p is any odd prime and $r\in\mathbb{N}$.

In the remainder of this question, we take p to be an odd prime number and g to be a primitive root modulo p^2.

(b) Show that each reduced residue modulo p^2 is congruent to g^r modulo p^2 for a unique integer r with $0\le r<p(p-1)$.

Solution: The reduced residues g^r are distinct modulo p^2 for distinct values of r with $0\le r<\varphi(p^2)$. Otherwise, if $g^r\equiv g^s\pmod{p^2}$ for some integers $0\le r<s\le\varphi(p^2)$, then $g^{s-r}\equiv 1\pmod{p^2}$ with $0<s-r<\varphi(p^2)$, contradicting the primitivity of g modulo p^2. The $\varphi(p^2)$ distinct reduced residues $g^r\pmod{p^2}$ with $0\le r<\varphi(p^2)$ must therefore be precisely the $\varphi(p^2)$ reduced residues a with $1\le a\le p^2$ with $(a,p)=1$. Hence, each reduced residue modulo p^2 is congruent to g^r modulo p^2 for a unique integer r with $0\le r<p(p-1)$.

(c) Suppose that a satisfies $(a,p)=1$. Show that the congruence $x^2\equiv a\pmod{p^2}$ is soluble if and only if $a^{p(p-1)/2}\equiv 1\pmod{p^2}$.

Solution: Let g be a primitive root modulo p^2. Then for some $r\in\mathbb{N}$ one has $a\equiv g^r\pmod{p^2}$. If $a^{p(p-1)/2}\equiv 1\pmod{p^2}$, then $g^{rp(p-1)/2}\equiv 1\pmod{p^2}$. But since g is primitive, the latter congruence can hold only when $p(p-1)|rp(p-1)/2$, whence $2|r$. Say $r=2s$. Then $a\equiv g^{2s}=(g^s)^2\pmod{p^2}$. Thus, the congruence $x^2\equiv a\pmod{p^2}$ is soluble.

On the other hand, if the congruence $x^2\equiv a\pmod{p^2}$ is soluble, then $a^{p(p-1)/2}\equiv x^{p(p-1)}\equiv 1\pmod{p^2}$, on making use of Euler's Theorem.

Continued...

7. [6+4+4=14 points] (a) Let $a(n)$ and $b(n)$ be multiplicative functions of n. Show that the arithmetic function

$$c(n) = \sum_{d|n} a(d)b(n/d)$$

is multiplicative.

Solution: Suppose that $a(n)$ and $b(n)$ are multiplicative. Then whenever $m, n \in \mathbb{N}$ satisfy $(m, n) = 1$, we have $a(mn) = a(m)a(n)$ and $b(mn) = b(m)b(n)$, whence

$$c(mn) = \sum_{d|mn} a(nm/d)b(d) = \sum_{e|n} \sum_{f|m} a\left(\frac{n}{e}\frac{m}{f}\right) b(ef).$$

Since the values of e and f in the latter summation are necessarily coprime, we obtain

$$c(mn) = \sum_{e|n} \sum_{f|m} a(n/e)a(m/f)b(e)b(f) = \Big(\sum_{e|n} a(n/e)b(e)\Big)\Big(\sum_{f|m} a(m/f)b(f)\Big).$$

Thus $c(mn) = c(m)c(n)$, and since $c(1) = a(1)b(1) = 1$, the function $c(n)$ is indeed a multiplicative function.

(b) Show that when n is a natural number, then $\sigma(n^2)$ is odd.

Solution: When p is an odd prime and $r \in \mathbb{N}$, one sees that $\sigma(p^{2r}) = 1 + p + \ldots + p^{2r} \equiv 2r+1 \equiv 1 \pmod 2$, and $\sigma(2^{2r}) = 1+2+\ldots+2^{2r} \equiv 1 \pmod 2$. Then by the multiplicativity of $\sigma(\cdot)$, we find that $\sigma(n^2) = \prod_{p^h \| n} \sigma(p^{2h}) \equiv 1 \pmod 2$, so that $\sigma(n^2)$ is odd.

(c) Show that if n is an odd perfect number, then n must have the shape $p^{4k+1}m^2$, where p is a prime number with $p \equiv 1 \pmod 4$, the exponent k is a non-negative integer, and $m \in \mathbb{N}$ satisfies $p \nmid m$.

Solution: If n is an odd perfect number, we have $\sigma(n) = 2n$ with n odd, and hence $\sigma(n) \equiv 2 \pmod 4$. Since, by multiplicativity, we have $\sigma(n) = \prod_{p^h \| n} \sigma(p^h)$, and when n is odd we have $\sigma(p^h) = 1+p+\ldots+p^h \equiv h+1 \pmod 2$, we see that h must be even for all but one of the prime powers p^h with $p^h \| n$. Then $n = \pi^r m^2$ for some odd prime π with $\pi \nmid m$, and r odd. But then we must have $\sigma(\pi^r) = 1+\pi+\ldots+\pi^r \equiv 2 \pmod 4$. When $\pi \equiv -1 \pmod 4$, the fact that r is odd implies that $\sigma(\pi^r) \equiv (1-1)+\ldots+(1-1) \equiv 0 \pmod 4$, so we must have $\pi \equiv 1 \pmod 4$. Hence $2 \equiv \sigma(\pi^r) \equiv r+1 \pmod 4$, whence $r \equiv 1 \pmod 4$. We thus conclude that n must have the shape $\pi^{4k+1}m^2$, where π is a prime number with $\pi \equiv 1 \pmod 4$, the exponent k is a non-negative integer, and $m \in \mathbb{N}$ satisfies $\pi \nmid m$.

End of examination.