PURDUE UNIVERSITY

Department of Mathematics

INTRODUCTION TO NUMBER THEORY

MA 49500 and MA 59500 - SOLUTIONS

6th November 2023 50 minutes

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

Do not turn over until instructed.

1. [4+4+4+4+4=20 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. Suppose that a is an integer for which the Jacobi symbol $\left(\frac{a}{35}\right) = 1$. Then a is a quadratic residue modulo 35.

   Solution: FALSE (One has $\left(\frac{a}{35}\right) = 1$ when $\left(\frac{a}{5}\right) = -1$ and $\left(\frac{a}{7}\right) = -1$, and then a is not a quadratic residue modulo 35. Such is the case when $a = 3$).

   b. The function $\omega(n)$ (the number of distinct 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 distinct 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. The reduced residue 5 is a primitive root modulo 2^{2023}.

   Solution: FALSE (There are no primitive roots modulo 2^k when $k \geq 3$).

   e. When g is a primitive root modulo 7^2, then g is a primitive root modulo 7^{2023}.

   Solution: TRUE (When p is an odd prime, then any primitive root modulo p^2 is also a primitive root modulo p^k for any $k \geq 2$).

2. [5+5+5+5=20 points]

   (a) Define what is meant by a *quadratic residue* modulo m, and also what is meant by a *quadratic non-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. If the latter congruence is insoluble, then we say that a is a **quadratic non-residue modulo** m.

   (b) 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 $\varphi(m)$.

   (c) 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 $\mu(n) = 0$.

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

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

Continued...

3. [8+8=16 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 $\left(\frac{69}{697}\right)$.

Solution: Use quadratic reciprocity for Jacobi symbols:

$$\begin{aligned}\left(\frac{69}{697}\right) &= (-1)^{(68)(696)/4}\left(\frac{697}{69}\right) = \left(\frac{7}{69}\right)\\ &= (-1)^{(6)(68)/4}\left(\frac{69}{7}\right) = \left(\frac{-1}{7}\right) = (-1)^{(7-1)/2} = -1.\end{aligned}$$

4. [12 points] In this question you may suppose that, whenever π is a prime number with $\pi \equiv 5 \pmod{12}$, then $\left(\frac{3}{\pi}\right) = -1$. Suppose that $p = 2^{2^n}+1$ is prime with $p > 3$. Show that 3 is a primitive root modulo p.

Solution: When $p = 2^{2^n}+1$ is prime, it follows from Fermat's Little Theorem that the order of 3 modulo p divides $p-1 = 2^{2^n}$. Then the order of 3 modulo p is a power of 2, and if 3 is not a primitive root, then this order divides $2^{2^n-1} = (p-1)/2$. But $p \equiv 1 \pmod 4$ and $p \equiv (-1)^{2^n}+1 \equiv 2 \pmod 3$, whence $p \equiv 5 \pmod{12}$. In such circumstances, we find by means of Euler's criterion that $-1 = \left(\frac{3}{p}\right) \equiv 3^{(p-1)/2} \equiv 1 \pmod p$, yielding a contradiction. Thus 3 must be a primitive root modulo p.

5. [7+7=14 points] (a) By considering the Jacobi symbol $\left(\frac{-1}{m}\right)$, prove that when n_1 and n_2 are odd natural numbers, then one has

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

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

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

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

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

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

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.

Continued...

6. [4+7+7=18 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 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 $0 \leq r < p(p-1)$.

Solution: The reduced residues g^r are distinct modulo p^2 for distinct values of r with $0 \leq r < \varphi(p^2)$. Otherwise, if $g^r \equiv g^s \pmod{p^2}$ for some integers $0 \leq r < s \leq \varphi(p^2)$, 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 $0 \leq r < \varphi(p^2)$ must therefore be precisely the $\varphi(p^2)$ reduced residues a with $1 \leq a \leq p^2$ 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 $0 \leq r < p(p-1)$.

(c) Show that

$$\prod_{\substack{a=1 \\ (a,p)=1}}^{p^2} a \equiv -1 \pmod{p^2}.$$

Solution: Each reduced residue a modulo p^2 is uniquely represented in the shape $a \equiv g^r \pmod{p^2}$, for an integer r with $0 \leq r < p(p-1)$. Thus, by Euler's theorem,

$$\prod_{\substack{a=1 \\ (a,p)=1}}^{p^2} a \equiv \prod_{0 \leq r < p(p-1)} g^r = g^{0+1+\ldots+(p^2-p-1)} = \left(g^{p(p-1)-1}\right)^{p(p-1)/2} \equiv (g^{-1})^{p(p-1)/2} \pmod{p^h}.$$

Write $b = g^{p(p-1)/2}$. Then it follows from Euler's Theorem that $b^2 \equiv 1 \pmod{p^2}$, yet $b \not\equiv 1 \pmod{p^2}$, since g is primitive. Thus $b \equiv -1 \pmod{p^2}$, and so

$$\prod_{\substack{a=1 \\ (a,p)=1}}^{p^2} a \equiv -1 \pmod{p^2}.$$

End of examination.