PURDUE UNIVERSITY

Department of Mathematics

INTRODUCTION TO NUMBER THEORY

MA 49500 and MA 59500 - SOLUTIONS

18th February 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+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. When p and q are distinct prime numbers, and $n \in \mathbb{Z}$, the equation $px + qy = n$ always has a solution in integers x and y.

Solution: TRUE (Since $(p, q) = 1$, it follows from the Euclidean Algorithm that there are integers u and v with $pu + qv = 1$, and then $p(un) + q(vn) = n$).

b. Let p be a prime number. Then for every integer a, one has $a^{p-1} \equiv 1 \pmod{p}$.

Solution: FALSE (When $p|a$, one has $a^{p-1} \equiv 0 \pmod{p}$).

c. For some natural number n, one has $(n(n^2 - 1), 6) = 2$.

Solution: FALSE (The product of 3 consecutive integers is always divisible by 6, so $(n(n^2 - 1), 6) = 6$).

d. The greatest common divisor of two non-zero integers a and b is the smallest positive value of $ax + by$, as x and y range over $\mathbb{Z}$.

Solution: TRUE (This is Theorem 2.7(i) from class).

e. There exists an integer x satisfying the simultaneous congruences

$$x^2 \equiv 5 \pmod{6} \quad \text{and} \quad x^2 \equiv 4 \pmod{15}.$$

Solution: FALSE (If such an integer were to exist, then from the first congruence we have $x^2 \equiv 2 \pmod{3}$, and from the second $x^2 \equiv 1 \pmod{3}$, leading to a contradiction).

f. Let a and b be natural numbers with $(a, b) = 1$. Then ab divides $[a, b]$.

Solution: TRUE (We proved that $ab = [a, b](a, b)$, so since $(a, b) = 1$ we have $[a, b] = ab$).

g. Suppose that p is prime and d is a natural number with $(p-1)|d$. Then the congruence $x^d \equiv 1 \pmod{p^3}$ always has precisely d solutions modulo p^3.

Solution: FALSE (The congruence $x^2 \equiv 1 \pmod{8}$ has 4 solutions 1, 3, 5, 7 modulo 8).

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

(a) Let a and b be non-zero integers. Define what is meant by the least common multiple $[a, b]$ of a and b.

Solution: The least common multiple of a and b is the smallest positive integer k having the property that $a|k$ and $b|k$.

(b) Define what is meant by a multiplicative function.

Solution: A function $f : \mathbb{N} \to \mathbb{C}$ is multiplicative if (i) f is not identically zero, and (ii) whenever $(m, n) = 1$, then $f(mn) = f(m)f(n)$.

(c) Let $f(x)$ be a polynomial with integer coefficients. Define what is meant by the degree of f modulo m.

Solution: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ be a polynomial with integral coefficients. Let j be the largest integer with $m \nmid a_j$. Then we say that the **degree** of f modulo m is j. If $m|a_j$ for every j, then the degree of f is undefined.

Continued...

(d) Let $m \in \mathbb{N}$. Define what is meant by a reduced residue system modulo m.

Solution: A reduced residue system modulo m is a set of integers $r_1, \ldots, r_n$ satisfying (i) $(r_i, m) = 1$ for $1 \le i \le n$, (ii) $r_i \not\equiv r_j \pmod{m}$ for $i \ne j$, and (iii) whenever $(x, m) = 1$, then $x \equiv r_i \pmod{m}$ for some i with $1 \le i \le n$.

3. [5+5=10 points] (a) Let n be a natural number with $n > 1$. Compute (n^2+1, n^3-1).

Solution: One has $(n^2+1, n^3-1) = (n^2+1, n^3-1-n(n^2+1)) = (n^2+1, n+1)$, and $(n^2+1, n+1) = (n^2+1-(n-1)(n+1), n+1) = (2, n+1)$. So

$$(n^2+1, n^3-1) = \begin{cases} 1, & \text{when } n \text{ is even,} \\ 2, & \text{when } n \text{ is odd.} \end{cases}$$

(b) Let n be a natural number with $n > 1$. For what values of n is there a solution of the equation

$$(n^2+1)x + (n^3-1)y = 1$$

in integers x and y? Explain your answer.

Solution: The equation has a solution if and only if n is an even integer. In order to see this, observe that as a consequence of the Euclidean algorithm, the equation

$$(n^2+1)x + (n^3-1)y = (n^2+1, n^3-1)$$

has a solution in integers x and y. Thus, the equation in question has a solution whenever n is even, as a consequence of the conclusion of part (a). On the other hand, if $(n^2+1, n^3-1) = 2$, then for all integers x and y, one has that 2 divides $(n^2+1)x + (n^3-1)y$, and thus the latter integer cannot be 1. Hence, again by part (a), there is no solution of the equation in question when n is odd.

4. [10 points] Recall that if p is prime and $x^2+1 \equiv 0 \pmod{p}$ is soluble, then $p = 2$ or $p \equiv 1 \pmod{4}$. By modifying Euclid's proof that there are infinitely many primes, deduce that there are infinitely many primes of the form $4k+1$ ($k \in \mathbb{N}$).

Solution: Suppose that there are only finitely many primes of the shape $4k+1$, say $p_1, \ldots, p_n$. Let $P = 2p_1p_2 \cdots p_n$, and put $Q = P^2 + 1$. Then Q is odd, and if $p|Q$, then $x^2+1 \equiv 0 \pmod{p}$ has the solution $x = P$. Then the prime divisors of Q are all congruent to 1 modulo 4. By construction, one has $(Q, p_i) = (P^2+1, p_i) = 1$ for each i, because $p_i|P$. Then none of the finite set of primes congruent to 1 modulo 4 divide Q. We have arrived at a contradiction, and this proves that there are infinitely many primes of the shape $4k+1$.

5. [4+6+6=16 points] Throughout this question, the letter p denotes an odd prime number.

(a) State Fermat's Little Theorem in a form applicable to all residues modulo p.

Solution: For all $a \in \mathbb{Z}$, one has $a^p \equiv a \pmod{p}$.

(b) Show that the congruence

$$x^p - 2x + 2 \equiv 0 \pmod{p}$$

has precisely one solution modulo p, and determine that solution.

Solution: By Fermat's Little theorem, for any integer x, one has

$$x^p - 2x + 2 \equiv x - 2x + 2 = -x + 2 \pmod{p}.$$

Thus, the congruence in question has the solution given by $x \equiv 2 \pmod{p}$, and no others.

Continued...

(c) Determine the number of solutions of the congruence

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

Justify your answer.

Solution: One can either apply Hensel's lemma, or proceed directly. We do the latter. If x is a solution of the congruence in question, then $x^p - 2x + 2 \equiv 0 \pmod{p}$, so from part (b) we must have $x \equiv 2 \pmod{p}$. Write $x = 2 + py$ and substitute. Then we seek to solve $0 \equiv (2 + py)^p - 2(2 + py) + 2 \equiv 2^p - 2 - 2py \pmod{p^2}$. We therefore conclude that one must have $y \equiv (2^{p-1} - 1)/p \pmod{p}$, and thus there is precisely one solution modulo p^2, namely $x \equiv 2 + py \equiv 2^{p-1} + 1 \pmod{p^2}$.

6. [4+6+6=16 points] (a) Give a formula for Euler's function $\varphi(n)$ explicit in terms of the prime factorisation of n.

   Solution: One has $\phi(n) = n \prod_{p|n}(1 - 1/p)$, where the product is taken over the distinct prime divisors p of n.

   (b) Suppose that p, q and r are distinct prime numbers, and put $N = [p - 1, q - 1, r - 1]$. Prove that whenever $(a, pqr) = 1$, one has $a^N \equiv 1 \pmod{pqr}$.

   Solution: Since $(p - 1)|N$, say $N = m(p - 1)$, and $(a, p) = 1$, it follows from Fermat's Little Theorem that $a^N = (a^{p-1})^m \equiv 1 \pmod{p}$. Likewise, one has $a^N \equiv 1 \pmod{q}$ and $a^N \equiv 1 \pmod{r}$. On noting that p, q and r are distinct primes, and therefore pairwise coprime, it therefore follows from the Chinese Remainder Theorem that $a^N \equiv 1 \pmod{pqr}$.

   (c) By observing that $1729 = 7 \cdot 13 \cdot 19$, prove that whenever $(a, 1729) = 1$, one has

   $$a^{1728} \equiv 1 \pmod{1729}.$$

   Solution: Observe that $[6, 12, 18] = 6[1, 2, 3] = 36$, and $1728 = 36 \cdot 48$. Thus 1728 is divisible by $[6, 12, 18]$, and we deduce from (b) that whenever $(a, 1729) = 1$, one has $a^{1728} = (a^{36})^{48} \equiv 1 \pmod{1729}$.

7. [4+6+5=15 points] Suppose that $f(x) \in \mathbb{Z}[x]$ is a polynomial of degree at least 2 having non-zero constant term.

   (a) By computing $(n, f(n))$, show that there are infinitely many integers n for which n and $f(n)$ are coprime.

   Solution: Write $f(n) = a_d n^d + \ldots + a_1 n + a_0$, with $a_i \in \mathbb{Z}$ and $a_d a_0 \neq 0$. Then we have $(n, f(n)) = (n, a_0)$. Put $n = ma_0 + 1$ for any $m \in \mathbb{Z}$. Then $(n, f(n)) = (ma_0 + 1, a_0) = (1, a_0) = 1$, whence there are infinitely many integers n for which n and $f(n)$ are coprime.

   (b) Explain why, for all integers m, the integer $f(n + mf(n))$ is divisible by $f(n)$.

   Solution: Observe that for all integers n, one has $f(n + mf(n)) \equiv f(n) \equiv 0 \pmod{f(n)}$, and hence $f(n + mf(n))$ is divisible by $f(n)$.

Continued...

(c) Assume the truth of Dirichlet's theorem asserting that whenever a and q are natural numbers with $(a, q) = 1$, then there are infinitely many primes congruent to a modulo q. Prove that there is no polynomial $f \in \mathbb{Z}[x]$ of degree at least 2 having the property that $f(p)$ is prime whenever p is prime.

Solution: Suppose that $f \in \mathbb{Z}[x]$ is a polynomial of degree at least 2 having the property that $f(p)$ is prime for every prime p. By choosing a large prime q, we can suppose that $f(q)$ is a prime with $|f(q)| > q$, and hence $(q, f(q)) = 1$. Thus, by Dirichlet's theorem, there exists a prime number with $p = q + mf(q)$ for some large integer m. In particular, we may suppose that p is large enough that $|f(p)| > |f(q)|$. But then part (b) shows that $f(p) = f(q + mf(q))$ is divisible by $f(q)$, and hence cannot be prime. This yields a contradiction, showing that no such polynomial f can exist.

End of examination.