PURDUE UNIVERSITY

Department of Mathematics

INTRODUCTION TO NUMBER THEORY
MA 49500 and MA 59500 - SOLUTIONS

2nd October 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. Let p be a prime number. Then for every integer a, one has $a^{p^2} \equiv a \pmod{p}$.

   Solution: TRUE (Since $a^p \equiv a \pmod{p}$, one has $a^{p^2} \equiv a^p \equiv a \pmod{p}$).

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

   Solution: FALSE (This is superficially similar to a true fact for greatest common divisors, but here the set of positive values is unbounded).

   c. Let c_1, c_2, m_1, m_2 be integers with $1 \le m_1 < m_2$. Then the two congruences

   $$x \equiv c_1 \pmod{m_1} \quad \text{and} \quad x \equiv c_2 \pmod{m_2}$$

   do not have a simultaneous integer solution x unless $(m_1, m_2) = 1$.

   Solution: FALSE (Consider, for example, $m_1 = 2$, $m_2 = 4$, $c_1 = c_2 = 0$, so that the two congruences in question are $x \equiv 0 \pmod{2}$ and $x \equiv 0 \pmod{4}$, with solution $x = 0$, and yet $(2, 4) \ne 1$).

   d. Let a and b be natural numbers. Then ab divides $(a, b)[a, b]$.

   Solution: TRUE (We proved that $(a, b)[a, b] = |ab|$).

   e. When p is prime and $d \in \mathbb{N}$, the congruence $x^d \equiv 1 \pmod{p}$ always has d solutions.

   Solution: FALSE (Consider for example $p = 5$, $d = 3$ so that $(p - 1, d) = (4, 3) = 1$, whence $x^d \equiv 1 \pmod{p}$ has a unique solution).

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

   (a) Let a and b be integers, not both 0. Define what is meant by the greatest common divisor (a, b) of a and b.

   Solution: The greatest common divisor of a and b is the largest (positive) integer d having the property that $d|a$ and $d|b$.

   (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) Define the Euler totient (Euler's φ-function).

   Solution: The number of elements in a reduced residue system is denoted by $\varphi(n)$. Thus $\varphi(n) = \text{card}\{1 \le a \le n : (a, n) = 1\}$.

   (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 $1 \le i \le n$.

Continued...

3. [6+6=12 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 $(n^2 - 1, n + 1) = (n^2 - 1 - (n - 1)(n + 1), n + 1) = (0, n + 1) = n + 1$.

(b) Prove that there are infinitely many primes of the shape $6k - 1$ ($k \in \mathbb{N}$).

Solution: Every prime other than 2 and 3 is of the shape $6k \pm 1$. Suppose that there are only finitely many prime numbers of the shape $6k - 1$ with $k \geq 1$, say $p_1, \ldots, p_n$. Consider the integer $Q = 6p_1 \ldots p_n - 1$. The integer Q is odd, not divisible by 3, and of the shape $6k - 1$, so cannot be divisible exclusively by primes of the shape $6k + 1$. Moreover, none of the primes $p_1, \ldots, p_n$ divide Q. Thus Q is divisible by a new prime of the shape $6k - 1$ not amongst $p_1, \ldots, p_n$, contradicting our initial hypothesis. This completes the proof that there are infinitely many primes of the shape $6k - 1$.

4. [12 points] We call a positive integer n *squarefull* if, whenever p is a prime divisor of n, then p^2 is also a divisor of n. Show that when n is squarefull, there exist positive integers a and b for which $n = a^2 b^3$.

Solution: Suppose that n is a squarefull number, and that for each prime number p dividing n, the largest power of p dividing n is p^{r_p}. Then one has $r_p \geq 2$. If r_p is even, we put $u_p = r_p/2$ and $v_p = 0$. Otherwise, the integer r_p is odd with $r_p \geq 3$, and we can put $v_p = 1$ and $u_p = (r_p - 3)/2$. In all cases, we now have $r_p = 2u_p + 3v_p$, with u_p a non-negative integer and $v_p = 0$ or 1. Putting $a = \prod_{p|n} p^{u_p}$ and $b = \prod_{p|n} p^{v_p}$, we now have

$$n = \prod_{p|n} p^{r_p} = \Big(\prod_{p|n} p^{u_p}\Big)^2 \Big(\prod_{p|n} p^{v_p}\Big)^3 = a^2 b^3,$$

and the desired conclusion is now immediate.

5. [4+7+7=18 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.

(c) Let j be an integer with $j \geq 2$. Determine the number of solutions of the congruence

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

Justify your answer.

Solution: The congruence in question has only the solution $x \equiv 2 \pmod{p}$ when $j = 1$. Write $f(t) = t^p - 2t + 2$. Then $f'(t) = pt^{p-1} - 2$ and so, since p is odd, one has $f'(2) \equiv -2 \not\equiv 0 \pmod{p}$. Then $p^0 \| f'(2)$, and by Hensel's Lemma, for every $j \geq 2$, the solution $x = 2$ of the congruence modulo p lifts uniquely to a solution modulo p^j. Then there is precisely one solution modulo p^j to the congruence in question.

Continued...

6. [4+7+7=18 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) Let n be a natural number having the property that $p = 6n+1$, $q = 12n+1$ and $r = 18n+1$ are all prime numbers. Prove that whenever $(a, pqr) = 1$, one has

$$a^{pqr-1} \equiv 1 \pmod{pqr}.$$

Solution: Observe that $[p-1, q-1, r-1] = [6n, 12n, 18n] = 36n$, and

$$pqr - 1 = (6n+1)(12n+1)(18n+1) - 1 = 36n(36n^2 + 11n + 1).$$

Thus $pqr-1$ is divisible by $[p-1, q-1, r-1]$, and we deduce from (b) that whenever $(a, pqr) = 1$, one has $a^{pqr-1} \equiv 1 \pmod{pqr}$.

End of examination.