

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

SOLUTIONS FOR EXAM 2, NOV. 20, 2006

NAME: Solvatum Numerore

Throughout the exam, m denotes a positive integer, and a, b, x, y denote elements of \mathbb{Z} .

1. DEFINITIONS: 3 POINTS EACH

I'm skippin' it, with your perm.

- a. $x \equiv y \pmod{m}$ means

- b. Fermat's little Theorem states that

- c. The set $(\mathbb{Z}/m\mathbb{Z})^\times$ is defined to be

- d. The Bézout Theorem states that

- e. We say that $\{a\}_m$ is a zero-divisor if

- f. State (any form of) the Chinese Remainder Theorem.

- g. If $\gcd(a, m) = 1$, $\text{order}(\{a\}_m) =$

- h. The Euler product formula for the Riemann Zeta function is

2. TRUE/FALSE: 2 POINTS EACH

- a. The equation $121x + 2008006y = 11$ is not solvable with $x, y \in \mathbb{Z}$. FALSE
- b. If $m > 1$, then there are exactly two elements $\{x\}_m \in \mathbb{Z}/m\mathbb{Z}$ that satisfy $\{x\}_m^2 = \{1\}_m$. FALSE, (but true if m is prime.)
- c. If $n > 1$, then n is prime if and only if for all integers a satisfying $1 < a \leq \sqrt{n}$, a does not divide n . TRUE

d. For each positive integer k , there exists an integer N_k such that for all $x \geq N_k$, $\pi(x) \leq x/k$. TRUE

3. SHORT ANSWER: 5 POINTS EACH

In this section, you do not need to justify your steps.

a. Determine the multiplicative inverse of $\{249\}_{49}$ or explain why no such inverse exists. hit it with bezout and you find $-12(249) + 61(49) = 1$ so $\{249\}_{49}^{-1} = \{-12\}_{49}$.

b. Compute $\text{order}(\{1986\}_{31})$.

First note $\{1986\}_{31} = \{2\}_{31}$. Now $2, 2^2, 2^3, 2^4$ are not 1 modulo 31 but 2^5 is, so $\text{order}(\{1986\}_{31}) = 5$.

c. Find the smallest positive integer x such that $x \equiv 7 \pmod{16}$ and $x \equiv 1 \pmod{47}$.

We Chinese Remainder it, so we bezout 16 and 47 first, that's easy: $3(16) - 1(47) = 1$, now we take $x \equiv (1)(3)(16) + 7(-1)(47) \equiv -281 \pmod{16 \cdot 47}$, so the smallest positive x is $x = -281 + 16 \cdot 47 = 471$. Hey, wait a minute, this is math 471...hardyharhar, that Farshid is so goofy.

d. Find **all** the solutions in $\mathbb{Z}/31\mathbb{Z}$ of the congruence $1 + x + x^2 + x^3 + x^4 \equiv 0 \pmod{31}$. (You do not need to prove anything, just find the solutions).

first of all, $x \neq 1$ as you can plainly see, so $x - 1$ ain't 0 so it's legal to multiply by it on both sides, which gives $x^5 - 1 \equiv 0 \pmod{31}$. So, I'm looking for elements of order 5, well 2 is one of 'em and so are 4, 8, 16. By Lagrange's theorem, there ain't any more.

4. PROOFS: Do Four (4) of these Six (6) Problems, 12 POINTS EACH

a. Suppose $\gcd(a, m) = 1$ and $e = \text{order}(\{a\}_m)$. Prove both of the following statements.

(i) For $i, j \in \mathbb{Z}$, $a^i \equiv a^j \pmod{m}$ if and only if $e|(i - j)$.

Say $e|i - j$, so $i - j = ek$ with $k \in \mathbb{Z}$. Then $a^{i-j} = a^{ek} = (a^e)^k \equiv 1^k \pmod{m}$, multiplying by a^j on both sides, we get $a^i \equiv a^j \pmod{m}$. Conversely, if $a^i \equiv a^j \pmod{m}$, since a and m are coprime, a is invertible mod m so I can multiply by a^{-j} on both sides to $a^{i-j} \equiv 1 \pmod{m}$. By the Very Important Fact, then, $e|i - j$.

(ii) The numbers a, a^2, \dots, a^e are pairwise inequivalent modulo m , i.e. for $1 \leq i < j \leq e$, $a^i \not\equiv a^j \pmod{m}$.

If $1 \leq i < j \leq e$, then $0 < i - j < e$ so e cannot divide $i - j$ so by (i), $a^i \not\equiv a^j \pmod{m}$.

b. Show that there are infinitely many primes p satisfying $p \equiv 2 \pmod{3}$.

Suppose not, then we can list all primes $p \equiv 2 \pmod{3}$, let's say they are $2 = p_1, p_2, \dots, p_s$. Let $N = 3p_1p_2 \cdots p_s - 1$. Then $N > 1$ clearly and $N \equiv 2 \pmod{3}$. Note also that N is odd. Now N is not divisible by p_j for $j = 1, \dots, s$ because it is congruent to -1 modulo p_j . Thus, N is not divisible by any primes of the form $3k + 2$. It is not divisible by 3 either. That leaves only primes of the form $3k + 1$. On the other hand, $N > 1$ so it must be divisible by *some* prime and it can only be divisible by primes of the form $3k + 1$. Any product of such primes is also of the form $3k + 1$, so $N \equiv 1 \pmod{3}$, that's a SHAZZAM, contradiction.

c. Suppose p is an odd prime, so $p = 2n + 1$ for some positive integer n . Prove that if a is any integer such that p does not divide a , then either $a^n + 1$ or $a^n - 1$ is divisible by p .

Since $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem. So $a^{2n} - 1 \equiv 0 \pmod{p}$. But then $p \mid a^{2n} - 1 = (a^n - 1)(a^n + 1)$. By the $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ theorem, $p \mid a^n - 1$ or $p \mid a^n + 1$.

d. Suppose a, b are integers not divisible by the prime p . Show that

(i) If $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$.

By the transitivity of congruences mod p and by Fermat's little theorem, $a \equiv a^p \equiv b^p \equiv b \pmod{p}$.

(ii) If $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

By (i), $a \equiv b \pmod{p}$, so we may write $b = a + pj$. Now we use the binomial theorem to get

$$b^p = (a + pj)^p = a^p + pa^{p-1}(pj)^1 + \sum_{k=2}^p \binom{p}{k} a^{p-k} (pj)^k.$$

The summation at the extreme right is clearly divisible by p^2 because of the $(pj)^k$ factor (since $k \geq 2$), so we get

$$b^p \equiv a^p + p^2 a^{p-1} j \equiv a^p \pmod{p^2}.$$

e. Suppose p, q are distinct odd primes, and a is an integer such that q divides $a^p - 1$ but q does not divide $a - 1$. Show that $q = 1 + kp$ for some integer k and then show that this integer k is even.

We have $a^p \equiv 1 \pmod{q}$ but $a \not\equiv 1 \pmod{q}$. The first congruence tells us by the Very Important Fact that $\text{order}(\{a\}_q) | p$ and the second congruence says that this order is not equal to 1. Since p is a prime, we conclude that $\text{order}(\{a\}_q) = p$. But by Fermat's little theorem, $a^{q-1} \equiv 1 \pmod{q}$. [Note we can use this form of it because q does not divide a : if it did, then by the "first congruence" above we would get $0 \equiv -1 \pmod{q}$.] Now by the Very Important Fact (AGAIN?, yes AGAIN!) $p = \text{order}(\{a\}_q) | (q - 1)$ i.e. $q - 1 = kp$ for some integer k , which is what we wanted. Now since $q - 1 = kp$ is even and p is odd, k must be even.

f. Suppose p is an odd prime dividing $n^2 + 1$ for some integer n . Show that $p \equiv 1 \pmod{4}$.

This is similar in flavor to the previous problem. Clearly n is not divisible by p so by Fermat, $n^{p-1} \equiv 1 \pmod{p}$. We have $n^2 \equiv -1 \pmod{p}$. Squaring, we get $n^4 \equiv 1 \pmod{p}$. Now $n \not\equiv 1 \pmod{p}$ else we'd get $n^2 \equiv 1 \equiv -1 \pmod{p}$ but p is odd. Also, $n^3 \not\equiv 1 \pmod{p}$ because if it were so, then dividing by $n^2 \equiv -1 \pmod{p}$ we'd get $n \equiv -1 \pmod{p}$ which squaring would give $n^2 \equiv 1 \equiv -1 \pmod{p}$, contradiction. But we showed that n^4 is $1 \pmod{p}$, so $\text{order}(\{n\}_p) = 4$. By the Very Important Fact, $4 = \text{order}(\{n\}_p) | p - 1$, so $p \equiv 1 \pmod{4}$. Sionara.