

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

SOLUTIONS FOR HOMEWORK 5: CONGRUENCES I

1. True or False:

(a) $2 \equiv -5 \pmod{7}$ $7|(2+5)$ so true.

(b) $55 \equiv 73 \pmod{11}$ $55 - 73 = 18$ is not a multiple of 11 so false.

(c) $1111 \equiv 11 \pmod{11}$ $1111 - 11 = 1100 = 11 \cdot 100$ so it's true.

2. For (a) and (b), compute the smallest non-negative integer in the following residue classes. For (c), reinterpret (b).

(a) $2^{283} \pmod{17}$

We have $2^4 \equiv -1 \pmod{17}$ so $2^8 \equiv 1 \pmod{17}$. So the question becomes how many times 8 goes into 283 because the powers of 2 modulo 17 just go in a cycle of length 8. We have $283 = 8 \cdot 35 + 3$, so $2^{283} \equiv 2^3 \equiv 8 \pmod{17}$, the answer is 8.

(b) $9^{2006} \pmod{100}$

Again, we look for an integer k such that $9^k \equiv 1 \pmod{100}$. With our generalization of Fermat's little theorem, in retrospect, we don't have to work hard to find this: namely $\varphi(100) = \varphi(4)\varphi(25) = 2 \cdot 5 \cdot 4 = 40$ so $9^{40} \equiv 1 \pmod{100}$. We divide $2006 = 40 \cdot 50 + 6$, so $9^{2006} \equiv 9^6 \equiv 3^{12} \equiv 41 \pmod{100}$.

(c) What are the last (i.e. right-most) two digits of 9^{2006} ?

The last two digits of a number match exactly its remainder when divided by 100, so we just use (b) to get the answer: 41.

3. Prove or disprove: $a \equiv b \pmod{m}$ implies that $a^2 \equiv b^2 \pmod{m^2}$.

Not gonna do it, wouldn't be prudent: $7 \equiv 3 \pmod{4}$ but $49 \not\equiv 9 \pmod{16}$.

4. Is $3^{2n+5} + 2^{4n+1}$ divisible by 7 for all $n \geq 1$? Prove it.

Sure: $3^{2n+5} = 9^n \cdot 3^5 \equiv 2^n \cdot 5 \pmod{7}$ and $2^{4n+1} = 16^n \cdot 2 \equiv 2^n \cdot 2 \pmod{7}$, so

$$3^{2n+5} + 2^{4n+1} \equiv 5 \cdot 2^n + 2 \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \pmod{7}.$$

5. Is the sum of three consecutive cubes always divisible by 9? (i.e. is $f(x) = x^3 + (x+1)^3 + (x+2)^3 \equiv 0 \pmod{9}$ for all integers $x \geq 1$)? To investigate this, make a table for $x = 1, 2, 3, 4, 5, 6, 7, 8, 9$.

If you make a table, you find it's true for $x = 1, 2, \dots, 9$.

6. The answer to the previous question is "Yes." Now let's show that the calculation we did is already enough to prove it.

(a) Show that if $x \equiv y \pmod{9}$, then $f(x) \equiv f(y) \pmod{9}$.

We'll prove this for ANY polynomial and ANY modulus. Suppose $f(x) = a_0 + a_1x + \dots + a_nx^n$ is a polynomial with integer coefficients and m is a positive integer. If $x \equiv y \pmod{m}$, then $x^2 \equiv y^2 \pmod{m}$ because of the rule that if $a \equiv b \pmod{m}$ and $a' \equiv b' \pmod{m}$ then $aa' \equiv bb' \pmod{m}$. Applying this principle again, we'll find by induction that $x \equiv y \pmod{m}$ implies $x^r \equiv y^r \pmod{m}$ for any integer $r \geq 1$. Thus, for any integer a_r , $a_rx^r \equiv a_ry^r \pmod{m}$, because if $a \equiv b \pmod{m}$, then for all integers c , $ca \equiv cb \pmod{m}$. Now we just add the congruences $a_rx^r \equiv a_ry^r \pmod{m}$ for $r = 0, \dots, n$ to get $f(x) \equiv f(y) \pmod{m}$.

(b) Show that 5 and 6(a) imply that the sum of three consecutive cubes is always a multiple of 9.

We have already checked 5 for $y = 1, 2, \dots, 9$. But if x is any integer, then $x \equiv y \pmod{9}$ holds for one of these values of y . By applying 6(a) we then get $f(x) \equiv 0 \pmod{9}$ because we've already checked $f(y) \equiv 0 \pmod{9}$.

7. Suppose the integer n has the base ten representation $a_m a_{m-1} \dots a_1 a_0$, i.e.

$$n = a_m 10^m + a_{m-1} 10^{m-1} + \dots + 10a_1 + a_0.$$

(a) Show that $n \equiv a_0 - a_1 + a_2 - \dots + (-1)^m a_m \pmod{11}$;

We have $10 \equiv -1 \pmod{11}$, so $n \equiv a_m(-1)^m + a_{m-1}(-1)^{m-1} + \dots - a_1 + a_0$. Thus, $n \equiv a_0 - a_1 + \dots + (-1)^m a_m \pmod{11}$.

(b) Show that $11|n$ if and only if

$$a_0 - a_1 + a_2 - \dots + (-1)^m a_m \equiv 0 \pmod{11}.$$

We have $11|n$ if and only if $n \equiv 0 \pmod{11}$ so by (a) if and only if $a_0 - a_1 + \dots \equiv 0 \pmod{11}$.

(c) Use (b) to check that 32323271626242003 is divisible by 11;

3-2+3-2+3-2+7-1+.... argh. you get the idea.

(d) Use (a) to check the fact the "all-ones-number" $11111 \dots 111$ is congruent either to 1 or 0 modulo 11 depending on whether there are oddly many ones or evenly many ones.

If there even evenly many 1s, you get half plus 1 and half -1 for a total of nada. If there are oddly many 1s, you get one extra plus 1, for a total of uno. So by (a) we are done.

8. Prove that if $a \equiv b \pmod{m}$, then $\gcd(a, m) = \gcd(b, m)$.

One easy way to see this is to recall that for integers x, y , if $g = \gcd(x, y)$, then g is the unique positive generator of the ideal (x, y) , so $(g) = (x, y)$. Now, if $a \equiv b \pmod{m}$, i.e. $b = a + km$ for some integer k , then $(\gcd(b, m)) = (b, m) = (a + km, m) = (a, m) = (\gcd(a, m))$, so if $\gcd(b, m) = \gcd(a, m)$.

Here is another proof. For any pair of integers x, y , let $D(x, y)$ be the set of common divisors of x and y . Then clearly $\gcd(x, y) = \max D(x, y)$. You'll agree that if we show $D(a, m) = D(b, m)$ then it will follow that $\gcd(a, m) = \max D(a, m) = \max D(b, m) = \gcd(b, m)$. But showing $D(a, m) = D(b, m)$ is easy (assuming $a \equiv b \pmod{m}$ of course). We write $b = a + km$ with $k \in \mathbb{Z}$. Suppose $d \in D(a, m)$. Then $d|a$ and $d|m$. It follows immediately that $d|a$ and $d|km$ so $d|(a+km)$ i.e. $d|a$ and $d|b$, so $d \in D(b, m)$. By a symmetric argument, if we start with $d \in D(b, m)$, then $d \in D(a, m)$. Hence $D(a, m) = D(b, m)$ and we can go home.