MAT 373 Homework 5

Justyce Countryman

February 19, 2024

Problem 1: Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$

Example: Suppose $a = 4$, $b = 5$, and $n = 3$. We can then say that $a^2 \equiv b^2 \pmod{n}$ because $3|16 - 25 = -9$. However, we then cannot state that $a \equiv b \pmod{n}$ since $3 \nmid 4 - 5 = -1$.

Problem 2: Find the remainders when 2^{50} and 41^{65} are divided by 7.

Firstly, in the case of $2^{50}/7$, we know know that $2^1 = 2$, $2^2 = 4$, and $2^3 = 8$. The remainder of $8/7$ is 1, so we can say that:

$$2^3 \equiv 1 \pmod{7} \tag{1}$$

We can then exponentiate both sides of equation (1) to the power of 16 to give us:

$$(2^3)^{16} \equiv 1^{16} \pmod{7}$$

$$2^{48} \equiv 1 \pmod{7} \tag{2}$$

Now, we can multiply both sides of equation (2) by 2^2:

$$2^{48} \cdot 2^2 \equiv 1 \cdot 2^2 \pmod{7}$$

$$2^{50} \equiv 4 \pmod{7} \tag{3}$$

Equation (3) then indicates that the remainder of $2^{50}/7$ is 4. Now, with the case of 41^{65}, we can easily say that $41^1 = 41$ and the remainder of $41/7$ is 6. As a result we are allowed to state that:

$$41 \equiv 6 \pmod{7} \tag{4}$$

Raising both sides of equation (4) to the power of 65 yields:

$$41^{65} \equiv 6^{65} \pmod{7} \tag{5}$$

Next, let's try and break down 6^{65}. We know that $6^1 = 6$ and $6^2 = 36$. The remainder of $36/7$ is 1. So we are able to mention that:

$$6^2 \equiv 1 \pmod{7} \tag{6}$$

Raising both sides of equation (6) to the power of 32 produces:

$$(6^2)^{32} \equiv 1^{32} \pmod{7}$$

$$6^{64} \equiv 1 \pmod 7 \tag{7}$$

Then multiplying both sides of equation (7) by 6^1 can then give us:

$$6^{64} \cdot 6^1 \equiv 1 \cdot 6^1 \pmod 7$$

$$6^{65} \equiv 6 \pmod 7 \tag{8}$$

By the transitive relation for congruence, we can utilize equations (5) and (8) to finally say that:

$$41^{65} \equiv 6 \pmod 7 \tag{9}$$

Therefore, equation (9) allows us to conclude the remainder of $41^{65}/7$ is 6.

Problem 3: Prove that if a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

Proof. Suppose a is an odd integer. We then know that $a = 2k + 1$ for some integer k. Calculating a^2 then gives us:

$$a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1 \tag{10}$$

We need to eventually say that $a^2 \equiv 1 \pmod 8$ by indicating that $a^2/8$ leaves a remainder of 1. Let's consider the two cases of k, k being either even or odd.

In the situation that k is even, $k = 2n$ for some integer n. Using this knowledge into equation (10) gives us:

$$a^2 = 4(2n)(2n + 1) + 1 = 8n(2n + 1) + 1 \tag{11}$$

Since we know that n is an integer and that adding or multiplying two integers results in another integer, $2n + 1$, and $n(2n + 1)$ are both integers. This means that when k is even, a^2 will be of the form $8m + 1$, for some integer m, and $a^2/8$ will have a remainder of 1.

On the other hand, suppose that k is odd. Then $k = 2n + 1$ for some integer n. Substituting $2n + 1$ for k in equation (10) equates to:

$$a^2 = 4(2n + 1)(2n + 2) + 1 = 4(4n^2 + 6n + 2) + 1 = 8(2n^2 + 3n + 1) + 1 \tag{12}$$

Once again, adding or multiplying two integers yields another integer, so n^2, $2n^2$, $3n$, $2n^2 + 3n$, and $2n^2 + 3n + 1$ are all integers. As a result, when k is odd, a^2 is still of the form $8m + 1$, for some integer m, and the remainder of $a^2/8$ is 1. Since we have checked all cases of k, we can determine that $4k(k + 1) + 1$ and a^2 will always have a remainder of 1 when divided by 8. We can then see that $8|a^2 - 1$ and by the definition of congruence, $a^2 \equiv 1 \pmod 8$. Therefore, if a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

□

Problem 4: Prove that if the integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$

Proof. Suppose integer a is not divisible by 2 or 3. We want to be able to say that $24|a^2 - 1$. To start, we know that $a^2 - 1$ is equivalent to:

$$(a + 1)(a - 1) \tag{13}$$

Since we already know that a is not divisible by 2 or 3, we can use lcm(2, 3) = 6, and the fact that when considering positive integers up to 6, only 1 and 5 do not divide 2 or 3, which allows a to be of one of these two forms:

$$a = 6k + 1 \tag{14}$$

or:

$$a = 6k + 5 \tag{15}$$

for some integer k. We only need to consider one of the two cases, so let's use equation (14) by plugging $6k + 1$ for a into equation (13):

$$(6k + 2)(6k) = 2(3k + 1)(6k) = 12k(3k + 1) \tag{16}$$

Now let's consider both cases of k. Suppose k is even, then $k = 2m$ for some integer m, which then updates equation (16) to:

$$12(2m)(3(2m) + 1) = 24(m)(6m + 1) \tag{17}$$

We know that adding or multiplying two integers yield another integer, so $6m + 1$ and $(m)(6m + 1)$ are both integers, meaning that equation (17) is of the form $24n$ for some integer n. Recall that we want to say that $24|(a + 1)(a - 1)$, so this information is helpful. Now suppose k is odd, then $k = 2m + 1$ for integer m, turning equation (16) into:

$$12(2m+1)(3(2m+1)+1) = 12(2m+1)(6m+4) = 12\cdot2(2m+1)(3m+2) = 24(2m+1)(3m+2) \tag{18}$$

We then notice that $2m + 1$, $3m + 2$, and $(2m + 1)(3m + 2)$ are all integers, so equation (18) is also of the form $24n$. Therefore, since we know all possible values of k are satisfied, we know that equation (14) will also satisfy that $24|(a + 1)(a - 1)$ and $24|a^2 - 1$. Thus, if integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

□

Problem 5: Verify that if $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then $a \equiv b \pmod{n}$, where the integer $n = \text{lcm}(n_1, n_2)$. Hence, whenever n_1 and n_2 are relatively prime, $a \equiv b \pmod{n_1 n_2}$.

Proof. Suppose $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$. We then know that $n_1|a - b$ and $n_2|a - b$. By the definition of least common multiples, we can then say that $n_1 n_2|a - b$ and by the definition of congruence, we have $a \equiv b \pmod{n_1 n_2}$. If we consider positive integer m to be any common multiple of n_1 and n_2, then we can say $\text{lcm}(n_1, n_2)|m$. We are then allowed to mention that $a \equiv b \pmod{n}$, where $n = \text{lcm}(n_1, n_2)$. □