MTH 4436 Homework Set 4.2; p. 67 1-7

SPRING 2015

Pat Rossi Name _____

1. Prove each of the following assertions:

   (a) If $a \equiv b \pmod{n}$ and $m|n$, then $a \equiv b \pmod{m}$

   Proof. Suppose that $a \equiv b \pmod{n}$ and $m|n$. Then $a - b = kn$ for some $k \in \mathbf{Z}$.
   Since $m|n$, There exists an integer j such that $n = jm$.
   Therefore, $a - b = kn = k(jm)$.
   i.e., $a - b = (kj)m \Rightarrow a \equiv b \pmod{m}$ ■

   (b) If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$

   Proof. Suppose that $a \equiv b \pmod{n}$ and $c|n$.
   Since $a \equiv b \pmod{n}$ there exists an integer k such that $a - b = kn$.
   Hence, $ca - cb = ckn \Rightarrow ca - cb = k(cn)$
   i.e., $ca \equiv cb \pmod{cn}$. ■

   (c) If $a \equiv b \pmod{n}$ and the integers a, b, n are all divisible by $d > 0$, then $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$.

   Proof. Let the hypotheses be given. Since a, b, n are all divisible by $d > 0$, there exist integers i, j, k, such that

   $$\begin{array}{lll} a = id & \Rightarrow & \frac{a}{d} = i \\ b = jd & \Rightarrow & \frac{b}{d} = j \\ n = kd & \Rightarrow & \frac{n}{d} = k \end{array}$$

   Also, since $a \equiv b \pmod{n}$, there exists an integer m such that $a - b = mn$.
   $\Rightarrow id - jd = m(kd) \Rightarrow i - j = mk \Rightarrow \frac{a}{d} - \frac{b}{d} = m\frac{n}{d}$.
   i.e., $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}$. ■

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

   Since $a^2 = b^2 \not\Rightarrow a = b$ (for example $(-1)^2 = (1)^2 \not\Rightarrow -1 = 1$), I'm assuming that the author intends for us to consider positive values of a and b only.

   So consider:

   $$\begin{array}{l} a = 2 \\ b = 4 \\ n = 12 \end{array}$$

   $(2)^2 \equiv (4)^2 \pmod{n}$, but of course, $(2) \not\equiv (4) \pmod{n}$.

3. If $a \equiv b \pmod{n}$, prove that $\gcd(a, n) \equiv \gcd(b, n)$.

pf/ Let the hypothesis be given. (i.e., suppose that $a \equiv b \pmod{n}$)

Then $a - b = kn$ for some $k \in \mathbb{Z}$.

Let $d = \gcd(a, n)$.

Then d is a divisor of both a and n.

Thus, $\exists\ p, q \in \mathbb{Z}$ such that $a = pd$ and $n = qd$.

Substituting these expressions for a and n in the equation $a - b = kn$, we have:

$pd - b = k(qd)$

$\Rightarrow b = pd - k(qd)$

$\Rightarrow b = pd - (kq)\, d$

$\Rightarrow b = (p - kq)\, d$

Hence, d is a divisor of b.

Since d is also a divisor of n, this means that d is a *common* divisor of b and n.

Hence, $d \leq \gcd(b, n)$

i.e., $\gcd(a, n) \leq \gcd(b, n)$

A similar argument can be used to show that $\gcd(b, n) \leq \gcd(a, n)$.

Hence, $\gcd(a, n) = \gcd(b, n)$

I got the idea for this proof from Gayle Stephens, Thuong Hoang, Kali Luker, and others. I liked their approach better than the one that I used in my own proof.

4. ~

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

Since $2^3 = 8 \equiv 1 \pmod 7$, our strategy should be to write 2^{50} in terms 2^3.

Observe $2^{50} = (2)^{48}(2)^2 = (2^3)^{16}(2)^2 \equiv (1)^{16}(2)^2 \pmod 7 \equiv (2)^2 \pmod 7 \equiv 4 \pmod 7$.

i.e., $2^{50} \equiv 4 \pmod 7$.

Regarding 41^{65}, observe $41 \equiv 6 \pmod 7 \equiv (-1) \pmod 7$.

Hence, $41^{65} \equiv (-1)^{65} \pmod 7 \equiv (-1) \pmod 7 \equiv 6 \pmod 7$.

i.e., $41^{65} \equiv 6 \pmod 7$.

b. What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5$$

Observe: If n is even, then $n^5 \equiv 0 \pmod 4$. This is because

$$n^5 = (2k)^5 = 2^5k^5 = 4\left(2^3k\right) \equiv 0 \pmod 4.$$

Next observe that consecutive odd numbers can be written as $(4k+1)$ and $(4k+3)$.

Furthermore, note that the sum of these, when raised to the fifth power is congruent to 0 mod 4. This is because

$$(4k+1)^5 + (4k+3)^5 \equiv (1)^5 + (-1)^5 \pmod 4 \equiv 1 + (-1) \pmod 4 \equiv 0 \pmod 4.$$

i.e., the sum of two consecutive odd numbers, raised to the fifth power, is congruent to 0 mod 4.

Hence, $1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5 =$

$[(1^5 + 3^5) + (5^5 + 7^5) + \ldots + (97^5 + 99^5)] + [2^5 + 4^5 + \ldots 98^5 + 100^5]$

$\equiv (0 + 0) \pmod 4 \equiv 0 \pmod 4$.

i.e., the remainder of $1^5 + 2^5 + 3^5 + \ldots + 99^5 + 100^5$, when divided by 4 is zero.

5. Prove that the integer $53^{103}+103^{53}$ is divisible by 39, and that $111^{333}+333^{111}$ is divisible by 7.

Proof. Observe:$53 \equiv 14 \pmod{39} \Rightarrow 53^2 \equiv 14^2 \pmod{39} \equiv 196 \pmod{39}$

$\equiv (5(39)+1) \pmod{39} \equiv 1 \pmod{39}$.

Also, $103 \equiv 25 \pmod{39} \equiv -14 \pmod{39} \equiv 196 \pmod{39}$

$\equiv (5(39)+1) \pmod{39} \equiv 1 \pmod{39}$.

Thus, $53^{103}+103^{53} = 53^{(2)(51)+1}+103^{(2)(26)+1} = (53^2)^{51}(53)+(103^2)^{26}(103)$

$\equiv \left[(1)^{51}(53)+(1)^{26}(103)\right] \pmod{39} \equiv (53+103) \pmod{39} \equiv (156) \pmod{39} \equiv 0 \pmod{39}$.

i.e., $53^{105}+103^{53} \equiv 0 \pmod{39}$.

Regarding $111^{333}+333^{111}$, observe: $111 = (15)(7)+6 \equiv 6 \pmod{7} \equiv (-1) \pmod{7}$.

Hence, $111^{333} \equiv (-1)^{333} \pmod{7} \equiv (-1) \pmod{7}$.

Similarly, $333 = 3 \cdot 111 \equiv 3 \cdot (-1) \pmod{7} \equiv -3 \pmod{7} \equiv 4 \pmod{7}$.

$\Rightarrow 333^3 \equiv 4^3 \pmod{7} \equiv 64 \pmod{7} \equiv 1 \pmod{7}$.

Thus, $333^{111} = (333^3)^{37} \equiv 1^{37} \pmod{7} \equiv 1 \pmod{7}$.

So finally we have $111^{333}+333^{111} \equiv (-1+1) \pmod{7} \equiv 0 \pmod{7}$.

i.e., $111^{333}+333^{111} \equiv 0 \pmod{7}$. ■

6. For $n \geq 1$, use congruence theory to establish each of the following divisibility statements:

a. $7 \mid (5^{2n}+3 \cdot 2^{5n-2})$

Observe: $5^2 = 25 = (3)(7)+4 \equiv 4 \pmod{7}$

Thus, $5^{2n} = (5^2)^n \equiv 4^n \pmod{7}$

Also, $2^5 = 32 \equiv 4 \pmod{7}$

Thus, $2^{5n-2} = (2^5)^n (2)^{-2} \equiv 4^n \left(\frac{1}{4}\right) \pmod{7}$

Hold it - there's a problem here!

Modulo arithmetic deals with integers only. We can't work with the fraction $\frac{1}{4}$.

To solve this problem, we write the exponents in terms of $(n-1)$ instead of n.

Thus, $5^{2n} = 5^{2(n-1)+2} = (5^2)^{n-1}(5)^2 \equiv 4^{n-1} \cdot (25) \pmod{7}$.

Also, $2^{5n-2} = 2^{5(n-1)+3} = (2^5)^{n-1}(2)^3 \equiv 4^{n-1} \cdot (8) \pmod{7}$

Finally this yields: $5^{2n}+3 \cdot 2^{5n-2} \equiv [4^{n-1} \cdot (25)+3(4^{n-1} \cdot (8))] \pmod{7} \equiv$
$[4^{n-1} \cdot (25)+4^{n-1} \cdot (24)] \pmod{7} \equiv [4^{n-1} \cdot (25+24)] \pmod{7} \equiv [4^{n-1} \cdot (49)] \pmod{7} \equiv$
$[4^{n-1} \cdot (0)] \pmod{7} \equiv 0 \pmod{7}$

i.e., $5^{2n}+3 \cdot 2^{5n-2} \equiv 0 \pmod{7}$, hence, $7 \mid (5^{2n}+3 \cdot 2^{5n-2})$.

b. $13 \mid (3^{n+2}+4^{2n+1})$

Observe: $3^{n+2}+4^{2n+1} = 3^n \cdot 3^2+(4^2)^n \cdot 4^1 = 3^n \cdot 9+(16)^n \cdot 4 \equiv (3^n \cdot 9+(3)^n \cdot 4) \pmod{13} \equiv$
$(3^n(9+4)) \pmod{13} \equiv 3^n \cdot 13 \pmod{13} \equiv 0 \pmod{13}$

i.e., $3^{n+2}+4^{2n+1} \equiv 0 \pmod{13}$, hence, $13 \mid (3^{n+2}+4^{2n+1})$.

c. $27 \mid (2^{5n+1} + 5^{n+2})$

Observe: $2^{5n+1} + 5^{n+2} = 2^{5n} \cdot 2^1 + 5^n \cdot 5^2 = (2^5)^n \cdot 2 + 5^n \cdot 25 = (32)^n \cdot 2 + 5^n \cdot 25 \equiv [(5)^n \cdot 2 + 5^n \cdot 25] \pmod{27} \equiv [5^n \cdot (2 + 25)] \pmod{27} \equiv [5^n \cdot (27)] \pmod{27} \equiv [5^n \cdot (0)] \pmod{27} \equiv 0 \pmod{27}$

i.e., $2^{5n+1} + 5^{n+2} \equiv 0 \pmod{27}$, hence, $27 \mid (2^{5n+1} + 5^{n+2})$.

d. $43 \mid (6^{n+2} + 7^{2n+1})$

Observe: $6^{n+2} + 7^{2n+1} = 6^n \cdot 6^2 + (7^2)^n \cdot 7^1 = 6^n \cdot 36 + (49)^n \cdot 7 \equiv [6^n \cdot 36 + (6)^n \cdot 7] \pmod{43} \equiv [6^n \cdot (36 + 7)] \pmod{43} \equiv [6^n \cdot (43)] \pmod{43} \equiv [6^n \cdot (0)] \pmod{43} \equiv 0 \pmod{43}$

i.e., $6^{n+2} + 7^{2n+1} \equiv 0 \pmod{43}$, hence, $43 \mid (6^{n+2} + 7^{2n+1})$.

7. For $n \geq 1$, show that

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

Proof. (By induction on n) Observe: the proposition holds for $n = 1$, as:

$(-13)^{1+1} = 169 \equiv -12 \pmod{181} \equiv (-13)^1 + (-13)^{1-1} \pmod{181}$.

Next, we assume that our proposition is true for $n = k$, and show that this implies that our proposition holds for $n = k + 1$.

i.e., We assume that $(-13)^{k+1} \equiv (-13)^k + (-13)^{k-1} \pmod{181}$,

and use this to show that $(-13)^{(k+1)+1} \equiv \left[(-13)^{k+1} + (-13)^{(k+1)-1}\right] \pmod{181}$.

i.e., Show that $(-13)^{k+2} \equiv \left[(-13)^{k+1} + (-13)^k\right] \pmod{181}$.

Observe: $(-13)^{k+2} \equiv (-13)(-13)^{k+1} \equiv (-13)\left[(-13)^k + (-13)^{k-1}\right] \pmod{181} \equiv \left[(-13)^{k+1} + (-13)^k\right] \pmod{181}$.

i.e., $(-13)^{k+2} \equiv \left[(-13)^{k+1} + (-13)^k\right] \pmod{181}$.

Hence, $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$ for $n \geq 1$. ■