MTH 4436 - Test #3 - Solutions

FALL 2021

Pat Rossi Name _____

Theorems, Definitions, etc.

1. Define *congruent modulo* n.

   Let a, b, and n be integers, with $n > 1$. The integers a and b are said to be *congruent modulo* n, denoted $a \equiv b \pmod{n}$, if $n \mid (a - b)$. (i.e. if $a - b = kn$ for some integer k.)
   Otherwise, a and b are said to be *incongruent modulo* n, denoted $a \not\equiv b \pmod{n}$

2. State a theorem that gives an alternative definition for *congruent modulo* n.

   Let a, b, and n be integers, with $n > 1$. $a \equiv b \pmod{n}$ if and only if a and b have the same non-negative remainder when divided by n.

3. State a theorem or corollary dealing with canceling and congruences. (e.g., a "cancellation law" or somthing similar.)

   - If $ca \equiv cb \pmod{n}$, then $a \equiv b \left(\mod \frac{n}{d}\right)$, where $d = \gcd(c, n)$
   - If $ca \equiv cb \pmod{n}$, and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$
   - Let p be prime. If $ca \equiv cb \pmod{p}$, and $p \nmid c$, then $a \equiv b \pmod{p}$

4. State a theorem or corollary dealing with congruences and polynomials.

   - Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function with integer coefficients. If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$.
   - Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function with integer coefficients. If $P(a) \equiv 0 \pmod{n}$ and $a \equiv b \pmod{n}$, then $P(b) \equiv 0 \pmod{n}$ also.

5. State a theorem or corollary dealing with testing large numbers for divisibility by a certain natural number.

   - Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_2 10^2 + a_1 10 + a_0$ be the base 10 decimal expansion of of a positive integer N, $0 \leq a_k < 10$; and let $S = a_m + a_{m-1} + \ldots + a_2 + a_1 + a_0$. Then $9 | N$ if and only if $9 | S$.
   - Let $N = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_2 10^2 + a_1 10 + a_0$ be the base 10 decimal expansion of of a positive integer N, $0 \leq a_k < 10$; and let $T = a_0 - a_1 + a_2 + (-1)^{m-1} a_{m-1} + (-1)^m a_m$. Then $11 | N$ if and only if $11 | T$.

6. State two properties/laws/rules having to do with working with congruences algebraically.

   Here are some possibilities:

   Let $n > 1$ be fixed. Then for arbitrary integers a, b, c, d and positive integer k. Then:

- $a \equiv a \pmod{n}$
- If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$
- $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$
- $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$
- $a \equiv b \pmod{n}$ then $a + c \equiv b + c \pmod{n}$ and $ac \equiv bc \pmod{n}$
- If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$

Exercises

7. Find all distinct solutions modulo 26. $5x \equiv 2 \pmod{26}$

   First, we want to find a solution (any solution) to the congruence.

   Note $x = 5$ yields $5(5) \equiv 25 \pmod{26} \equiv -1 \pmod{26}$

   i.e., $5(5) \equiv -1 \pmod{26}$

   Note that mutliplying both sides by -2 will yield:

   $(-2)(5)(5) \equiv (-2)(-1) \pmod{26}$

   $\Rightarrow (5)((-2)(5)) \equiv 2 \pmod{26}$

   i.e., $(5)(-10) \equiv 2 \pmod{26}$

   Since $-10 \equiv 16 \pmod{26}$, this yields $(5)(16) \equiv 2 \pmod{26}$

   $x = 16$ is a solution

   Next, note that our congruence fits the form: $\underbrace{5}_{a}x \equiv \underbrace{2}_{b} \left(\mathrm{mod}\, \underbrace{26}_{n} \right)$

   This congruence has d distinct solutions modulo 26, where $d = \gcd(a, n)$

   Hence, our congruence has $d = \gcd(5, 26) = 1$ solution.

Our only solution is $x = 16$

8. Find the remainder when 2^{65} is divided by 7.

   This is equivalent to saying "compute $2^{65} \pmod 7$. "

   Since we are given 2^{65}, we should find a power of 2 that is congruent to $1 \pmod 7$, in order to make this as easy as possible.

   Observe: $2^3 = 8 \equiv 1 \pmod 7$.

   Next, we should rewrite 2^{65} in terms of 2^3.

   By the Division Algorithm, $65 = (21)(3) + 2$

   Thus, $2^{65} = 2^{(21)(3)+2} = 2^{(21)(3)} \cdot 2^2 = (2^3)^{21} \cdot 2^2$

   $\Rightarrow 2^{65} = (2^3)^{21} \cdot 2^2 \equiv (1)^{21} \cdot 2^2 \pmod 7 \equiv 2^2 \pmod 7 \equiv 4 \pmod 7$

i.e., $2^{65} \equiv 4 \bmod 7$

9. Prove that the integer $53^{103} + 103^{53}$ is divisible by 39.

Since we are working with 53^{103} and 103^{53} it will probably prove to be helpful for us to find powers of 53 and 103 that are congurent to $1 \pmod{39}$.

Observe: $53 \equiv 14 \pmod{39}$

$\Rightarrow 53^2 = 14^2 = 196 \equiv 1 \pmod{39}$ $\quad (196 = (5)(39) + 1)$

i.e., $53^2 \equiv 1 \pmod{39}$

Also: $103 \equiv 25 \pmod{39} \equiv -14 \pmod{39}$ $\quad (103 = (2)(39)+25 \quad$ and $25-39 = -14)$

$\Rightarrow 103^2 = (-14)^2 = 196 \equiv 1 \pmod{39}$ $\quad (196 = (5)(39) + 1)$

i.e., $103^2 \equiv 1 \pmod{39}$

Next, we want to use the Division Algorithm to express 103^2 in terms of 53^2 and 103^2.

$103 = (51)(2) + 1$ and $53 = (26)(2) + 1$

Hence, $53^{103} + 103^{53} = 53^{(51)(2)+1} + 103^{(26)(2)+1} = 53^{(51)(2)} \cdot 53 + 103^{(26)(2)} \cdot 103 = (53^2)^{51} \cdot 53 + (103^2)^{26} \cdot 103$

i.e., $53^{103} + 103^{53} = (53^2)^{51} \cdot 53 + (103^2)^{26} \cdot 103$

Therefore, $53^{103} + 103^{53} = (53^2)^{51} \cdot 53 + (103^2)^{26} \cdot 103 \equiv (1)^{51} \cdot 53 + (1)^{26} \cdot 103 \pmod{39} \equiv 53 + 103 \pmod{39} \equiv 14 + (-14) \pmod{39} \equiv 0 \pmod{39}$

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

i.e., $53^{103} + 103^{53}$ has a remainder of 0 when divided by 39

Hence, $53^{103} + 103^{53}$ is divisible by 39 ■

10. Without performing divisions, determine whether the number 2475693 is divisible by 9 or 11

    Recall: 2475693 is divisible by 9 exactly when $(2+4+7+5+6+9+3)$ is divisible by 9.

    Observe: $2+4+7+5+6+9+3 = 36 = 4 \cdot 9$

    i.e., $9 \mid (2+4+7+5+6+9+3)$.

    Hence, $9 \mid 2475693$ also.

    Also: 2475693 is divisible by 11 exactly when $(2-4+7-5+6-9+3)$ is divisible by 11.

    Observe: $2-4+7-5+6-9+3 = 0 = 0 \cdot 11$

    i.e., $11 \mid (2-4+7-5+6-9+3)$

    Hence, $11 \mid 2475693$ also.