Modular Practice

Solve the following modular arithmetic equations for x and y.

(a) $9x + 5 \equiv 7 \pmod{11}$ (b) $9x + 5 \equiv 7 \pmod{11}$

(a) $9x + 5 \equiv 7 \pmod{11}$.

x = 2. (9-1 mod 11) (mod 11)

x = 10 (mod 11)

(b) Show that $3x + 15 \equiv 4 \pmod{21}$ does not have a solution.

3x = 10 (nod 21)

=7 3x= 1 (mod 3)

since &0,1,23 are not solutions to >x = 1 (mod 5), >x = 1 (mod 5) | m(x-y, 50 d(x-y 50 K = y (mod d)) has no solution, so 3x=10 (mod 21) (to 3x = 1 (mod 3), 3x = 1 (mod 3)

(mod 11) $2x = 4 \pmod{8}$ ave a solution. $x = 2 \pmod{8}$ $x = 2 \pmod{8}$

(have all , x= 4 (mod m) meas

(c) The system of simultaneous equations $3x + 2y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

2(2x+y=4 (rod 7)) 3x +24 = 0 (mod 7) X = 1 (mad 7)

2(1) t y=q (red 7) 4=2 (med 7)

X=1 Cmod 7) / Y=2 Cmod 7)

(d) $13^{2019} \equiv x \pmod{12}$.

(e)
$$7^{21} \equiv x \pmod{11}$$
.

$$7^{2} = 5 \pmod{11}$$
 $7^{4} = (7^{2})^{2} = 5^{2} = 3 \pmod{11}$
 $7^{8} = (7^{4})^{2} = 3^{2} = 9 \pmod{11}$
 $7^{16} = (7^{1})^{2} = 9^{2} = 9 \pmod{11}$

$$9^{21} = 7^{16} \cdot 7^{9} \cdot 7 = 9 \cdot 3 \cdot 7 = 7 \pmod{1}$$

$$X = 7 \pmod{1}$$

2 When/Why can we use CRT?

Let $a_1, \ldots, a_n, m_1, \ldots, m_n \in \mathbb{Z}$ where $m_i > 1$ and pairwise relatively prime. In lecture, you've constructed a solution to

$$x \equiv a_1 \pmod{m_1}$$
 \vdots
 $x \equiv a_n \pmod{m_n}$.

Let $m = m_1 \cdot m_2 \cdots m_n$.

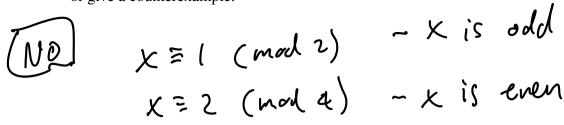
1. Show the solution is unique modulo m. (Recall that a solution is unique modulo m means given two solutions $x, x' \in \mathbb{Z}$, we must have $x \equiv x' \pmod{m}$.)

$$=7 m_i(X-X^l)$$

Q

$$=$$
 $\times = \times' \pmod m$

2. Suppose m_i 's are not pairwise relatively prime. Is it guaranteed that a solution exists? Prove or give a counterexample.



3. Suppose m_i 's are not pairwise relatively prime and a solution exists. Is it guaranteed that the solution is unique modulo m? Prove or give a counterexample.

 $X = 0 \pmod{4}$ $X = 0 \pmod{8}$

x=0,8 are solutions and 078 (mad 32)

3 Mechanical Chinese Remainder Theorem

In this problem, we will solve for x such that

$$x \equiv 1 \pmod{2}$$

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{5}$$

(a) Find a number $0 \le b_2 < 30$ such that $b_2 \equiv 1 \pmod{2}$, $b_2 \equiv 0 \pmod{3}$, and $b_2 \equiv 0 \pmod{5}$.

(b) Find a number $0 \le b_3 < 30$ such that $b_3 \equiv 0 \pmod{2}$, $b_3 \equiv 1 \pmod{3}$, and $b_3 \equiv 0 \pmod{5}$.

(c) Find a number $0 \le b_5 < 30$ such that $b_5 \equiv 0 \pmod 2$, $b_5 \equiv 0 \pmod 3$, and $b_5 \equiv 1 \pmod 5$.

(d) What is x in terms of b_2 , b_3 , and b_5 ? Evaluate this to get a numerical value for x.

$$x = 1.6 + 2.6 + 3.6$$

$$= 1.6 + 2.6 + 3.6$$

$$= 53$$

$$x = 23 \text{ (rad 30)}$$

$$x = 23 \text{ (rad 30)}$$