CS 70 Discussion 3A: tinyurl.com/frank-discussion 7/6/2020

1

2 min alone
5 min breakout
10 min go over

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

$-5 \quad -5$

$9x \equiv 2 \pmod{11}$ ×5

$9^{-1} \pmod{11} = 5$

$5(9)=45=44+1=4(11)+1$

$5(9x)\equiv 10 \pmod{11}$

$\boxed{x\equiv 10 \pmod{11}}$

(b) $3x+15\equiv 4 \pmod{21}$

$-15 \quad -15$

$3x\equiv -11 \pmod{21}$

$3x\equiv 10 \pmod{21}$

$3x=21b+10 \ (\exists b\in\mathbb{Z})$

$x=7b+\frac{10}{3}$

$\boxed{x \text{ has no integer solution}}$

(c) $\begin{cases} \cancel{3x+2y\equiv 0 \pmod 7} \\ 2x+y\equiv 4 \pmod 7 \end{cases}$ $\ominus$

×2 $\cancel{4x+2y\equiv 8 \pmod 7}$

$-x\equiv -8 \pmod 7$

$x\equiv 8 \pmod 7$

$\boxed{x\equiv 1 \pmod 7}$

$-x\equiv -1 \pmod 7$

$2x+y\equiv 4 \pmod 7$

$2+y\equiv 4 \pmod 7$

$\boxed{y\equiv 2 \pmod 7}$

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

$13 \bmod 12 = 1 \bmod 12$

$1^{2019}\equiv x \pmod{12}$

$\boxed{x\equiv 1 \pmod{12}}$

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

$\boxed{\text{FLT: } x^{p-1}\equiv 1 \pmod p \quad p \text{ is a prime}, x\not\equiv 0 \pmod p}$

$7^{10}\equiv 1 \pmod{11}$ $p=11$

$7^{21}=(7^{10})^2\cdot \boxed{7 \pmod{11}}$ $x=7$

5:27 **2**

2 min alone
6 min break
10 min go over

$\begin{cases} x\equiv a_1 \pmod{m_1} \\ \vdots \\ x\equiv a_n \pmod{m_n} \end{cases}$ $x \pmod M$ $M=\prod_{i=1}^{n} m_i$

$(a_1,\dots a_n, m_1,\dots m_n \in\mathbb{Z})$

(m_i are coprime; $m=\prod_{i=1}^{n} m_i$)

Let $x,x'\in\mathbb{Z}$ be two solutions.

Show that $x\equiv x' \pmod m$

$\forall i \ 1\le i\le n \quad x\equiv x' \pmod{m_i}$

$x-x'\equiv 0 \pmod{m_i}$

Since all m_i's are coprime with each other, it must be the case that

$x-x'\equiv 0 \pmod m$

5:50 $\boxed{x\equiv x' \pmod m}$

(b) $\begin{cases} x\equiv 1 \pmod 2 \\ x\equiv 2 \pmod 4 \end{cases}$

implies that x is odd

implies that x is even

$\boxed{\text{no solution}}$

Moral: If m_i aren't coprime, solution doesn't necessarily exist.

c) $\begin{cases} x\equiv 0 \pmod 4 \\ x\equiv 0 \pmod 8 \end{cases}$

$x\equiv 0, 8, 16, 24 \pmod{32}$

4×8

$\boxed{\text{Solutions aren't unique}}$

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 4 \pmod 7 \end{cases}$$

3 (a) mult inverse of $5 \times 7 \pmod 3$

$35 \pmod 3$

$2(35) = 70 = 69 + 1$, $69 = 3(23)$

$\boxed{2 \pmod 3}$

(b) smallest $a \in \mathbb{Z}^+$ where $5|a$, $7|a$, and $a \equiv 2 \pmod 3$

$a = 5 \times 7 \times ((35)^{-1} \pmod 3) \times 2$

$= 35 \times (\cancel{4} \bmod 3)$

$= \boxed{35}$

(c) mult inverse of $3 \times 7 \pmod 5$

$21 \bmod 5$

$\equiv 1 \bmod 5$

$\boxed{1}$

(d) smallest $b \in \mathbb{Z}^+$ where $3|b$, $7|b$, and $b \equiv 3 \pmod 5$

$b = 3 \times 7 \times (\cancel{(21)^{-1}} \pmod 5) \times 3$

$= 21 \times 3$

$= \boxed{63}$

(e) mult inverse of $3 \times 5 \pmod 7$

$15 \bmod 7$

$\equiv 1 \bmod 7$

$\boxed{1}$

(f) smallest $c \in \mathbb{Z}^+$ where $3|c$, $5|c$, and $c \equiv 4 \pmod 7$

$c = 3 \times 5 \times (\cancel{(15^{-1})} \bmod 7) \times 4$

$= \boxed{60}$

(g) solution:

$x \equiv a + b + c \pmod{3 \times 5 \times 7}$

$x \equiv 35 + 63 + 60 \pmod{105}$

$x \equiv 98 + 60 \pmod{105}$

$\boxed{x \equiv 53 \pmod{105}}$

Scanned with CamScanner