CS 70 Discrete Mathematics and Probability Theory
Summer 2021 DIS 2C

# 1 Modular Practice

Solve the following modular arithmetic equations for $x$ and $y$.

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

$9x \equiv 2 \pmod{11}$ // 5

$x \equiv 2 \cdot (9^{-1} \bmod 11) \pmod{11}$

$x \equiv 10 \pmod{11}$

$\boxed{2x \equiv 4 \pmod{8} \quad x \equiv 2 \pmod{8}}$

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

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

$\Rightarrow 3x \equiv 1 \pmod{3}$

since $\{0,1,2\}$ are not solutions to $3x \equiv 1 \pmod{3}$, $3x \equiv 1 \pmod{3}$ has no solution, so $3x \equiv 10 \pmod{21}$ has no solution

* if $d \mid m$ then $x \equiv y \pmod{m}$ $\Rightarrow x \equiv y \pmod{d}$

(have $d \mid m$, $x \equiv y \pmod{m}$ means $m \mid x-y$, so $d \mid x-y$ so $x \equiv y \pmod{d}$)

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

$2(2x + y \equiv 4 \pmod{7})$

$-\ \ 3x + 2y \equiv 0 \pmod{7}$

$x \equiv 1 \pmod{7}$

$2(1) + y \equiv 4 \pmod{7}$

$y \equiv 2 \pmod{7}$

$\boxed{x \equiv 1 \pmod{7} \quad y \equiv 2 \pmod{7}}$

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

$13^{2019} \equiv 1^{2019} \equiv 1 \pmod{12}$

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

$7^2 \equiv 5 \pmod{11}$

$7^4 \equiv (7^2)^2 \equiv 5^2 \equiv 3 \pmod{11}$

$7^8 \equiv (7^4)^2 \equiv 3^2 \equiv 9 \pmod{11}$

$7^{16} \equiv (7^8)^2 \equiv 9^2 \equiv 4 \pmod{11}$

$7^{21} \equiv 7^{16} \cdot 7^4 \cdot 7 \equiv 4 \cdot 3 \cdot 7 \equiv 7 \pmod{11}$

$\boxed{x \equiv 7 \pmod{11}}$

## 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

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

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 $x \equiv x' \pmod{m}$.)

$$x \equiv x' \pmod{m_i} \quad \forall m_i$$

$$\Rightarrow x - x' \equiv 0 \pmod{m_i} \quad \forall m_i$$

$$\Rightarrow m_i \mid x - x' \quad \forall m_i$$

$$\Rightarrow \prod_{i=1}^{n} m_i \mid x - x' \quad \text{b/c the } m_i\text{'s are relatively prime}$$

$$\Rightarrow m \mid x - x'$$

$$\Rightarrow x - x' \equiv 0 \pmod{m}$$

$$\Rightarrow x \equiv x' \pmod{m} \qquad \square$$

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

$\boxed{\text{NO}}$

$x \equiv 1 \pmod 2$ – x is odd

$x \equiv 2 \pmod 4$ – x is even

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.

$\boxed{\text{NO}}$

$x \equiv 0 \pmod 4$

$x \equiv 0 \pmod 8$

$x = 0, 8$ are solutions and $0 \not\equiv 8 \pmod{32}$

## 3 Mechanical Chinese Remainder Theorem

In this problem, we will solve for $x$ such that

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

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

$$b_2 = 3\cdot 5\left((3\cdot 5)^{-1} \bmod 2\right) = 15\left(15^{-1} \pmod 2\right) = 15$$

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

$$b_3 = 2\cdot 5\left((2\cdot 5)^{-1} \pmod 3\right) = 10\left(10^{-1} \pmod 3\right) = 10$$

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

$$b_5 = 2\cdot 3\left((2\cdot 3)^{-1} \pmod 5\right) = 6\left(6^{-1} \pmod 5\right) = 6$$

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

$$x = 1\cdot b_2 + 2\cdot b_3 + 3\cdot b_5$$
$$= 1\cdot 15 + 2\cdot 10 + 3\cdot 6$$
$$= 53$$

$$\boxed{x \equiv 23 \pmod{30}}$$

$b_2, b_3, b_5$ like "basis vectors"

$$\begin{bmatrix}1\\2\\3\end{bmatrix} = 1\cdot \underbrace{\begin{bmatrix}1\\0\\0\end{bmatrix}}_{b_2} + 2\cdot \underbrace{\begin{bmatrix}0\\1\\0\end{bmatrix}}_{b_3} + 3\underbrace{\begin{bmatrix}0\\0\\1\end{bmatrix}}_{b_5}$$