CS 235: Algebraic Algorithms, Spring 2021

Discussion 2

Date: Tuesday, February 09, 2021.

Problem 1. Modular Inverses

(a) Find the modular inverses of 4, 5, and 7 in $\mathbb{Z}_{11}$ and [redacted]. $\mathbb{Z}_{17}$

(b) Determine whether the following congruence has solution(s) or not (and how many). If the congruence has a unique solution, try to solve it using modular inverses.

(i) $66x \equiv 100 \pmod{121}$

(ii) $21x \equiv 14 \pmod{91}$

(iii) $3x \equiv 5 \pmod{17}$ $\rightarrow \gcd(17,3)=1,\ 3\cdot 6 \equiv 1 \pmod{17}$

$3\cdot 6x \equiv 5\cdot 6 \pmod{17}$

$x \equiv 13 \pmod{17}$

(iv) $10x \equiv 3 \pmod{11}$

a) $ax \equiv 1 \pmod{n}$

$\mathbb{Z}_{11}$: $4x \equiv 1 \pmod{11}$

$x = 3$

$5 \rightarrow 9,\quad 7 \rightarrow 8$

$\mathbb{Z}_{17}$: $4 \rightarrow 13,\quad 5 \rightarrow 7$

(iv) $10\cdot 10 \equiv 1 \pmod{11}$

b) (i) $66x \equiv 100 \pmod{121}$

$\gcd(121, 66) = 11,\quad 11 \nmid 100 \Rightarrow$ no sol

(ii) $21x \equiv 14 \pmod{91}$

$\gcd(91, 21) = 7,\quad 7 \mid 14$

$\gcd(a, n) = d$

Problem 2. More congruence drilling...

(a) Prove that the equation $x^2 - 7y^3 = 3$ has no solution for any $x, y \in \mathbb{Z}$. (**Hint:** consider mod 7 arithmetic)

(b) Prove the **Cancellation Law**, namely, if $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{m}$.

a) Suppose $x^2 - 7y^3 = 3$ has solution for $x, y \in \mathbb{Z}$

$\Rightarrow x^2 = 7y^3 + 3 \Rightarrow x^2 \equiv 3 \pmod 7$

(i.e. $x^2 \bmod 7 = 3$)

Consider: $x \equiv n \pmod 7$, for $x \in \mathbb{Z}$

$n = \{0, 1, 2, 3, 4, 5, 6\}$

$x^2 \equiv n \pmod 7$

$n = \{0, 1, 4, 2\} \Rightarrow x^2 \equiv 3 \pmod 7$ ($\lightning$)

Hence, $x^2 - 7y^3 = 3$ has no solution

b) Given: $ac \equiv bc \pmod n \overset{def}{\Rightarrow} n \mid (ac - bc)$

$\Rightarrow ac - bc = ny$ for $y \in \mathbb{Z}$

$\Rightarrow c(a-b) = ny \Rightarrow a - b = \frac{ny}{c}$

$\Rightarrow \frac{ny}{c}$ is an integer

$\Rightarrow \frac{y}{c}$ is an integer $\gcd(c, n) = 1$

$\Rightarrow a - b = nz$ where $z = \frac{y}{c} \in \mathbb{Z}$

$\Rightarrow n \mid (a - b) \quad \therefore a \equiv b \pmod n$ $\boxtimes$

Problem 3. Let p be an odd prime. Show that $\Sigma_{\alpha\in\mathbb{Z}_p^*}\ \alpha^{-1} = \Sigma_{\alpha\in\mathbb{Z}_p^*}\ \alpha = 0$.

$$\mathbb{Z}_p^* = \{1, 2, \dots, p-1\}$$

$$\sum_{\alpha\in\mathbb{Z}_p^*} \alpha = 1+2+\dots+p-1 = \frac{(p-1)(p-1+1)}{2}$$

$$= \frac{(p-1)\,p}{2}$$

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

$$= p\alpha \equiv 0 \pmod{p}$$

$$\Rightarrow \sum_{\alpha\in\mathbb{Z}_p^*} \alpha = 0 \pmod{p}$$

(page 28) $\alpha \in \mathbb{Z}_n^* \to \mathbb{Z}_p^*$

$$\Rightarrow \alpha^{-1} \in \mathbb{Z}_n^* \to \mathbb{Z}_p^*$$

$$\Rightarrow \sum \alpha^{-1} = \sum \alpha = 0$$

$\boxtimes$