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 $\mathbb{Z}_{17}$.

(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) $3x \equiv 5 \pmod{17}$

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

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 $a \equiv b \pmod{n}$.

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