CS 70 Spring 2019 — Discrete Mathematics and Probability Theory — Satish Rao and Babak Ayazifar — DIS 3B

1 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \dots \pmod{m}$. Prove that this sequence has repetitions. (**Hint:** Consider the Pidgenhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is k in terms of i and j?

2 Bijections

Let n be an odd number. Let $f(x)$ be a function from $\{0,1,\dots,n-1\}$ to $\{0,1,\dots,n-1\}$. In each of these cases say whether or not $f(x)$ is necessarily a bijection. Justify your answer (either prove $f(x)$ is a bijection or give a counterexample).

(a) $f(x) = 2x \pmod{n}$.

(b) $f(x) = 5x \pmod{n}$.

(c) n is prime and

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ x^{-1} \pmod{n} & \text{if } x \neq 0. \end{cases}$$

(d) n is prime and $f(x) = x^2 \pmod{n}$.

3 Introduction to Chinese Remainder Theorem

Solve for $x \in \mathbb{Z}$ where

$$\begin{aligned} x &\equiv 3 \pmod{11}, \\ x &\equiv 7 \pmod{13}. \end{aligned}$$

(a) Find the multiplicative inverse of 13 modulo 11.

(b) What is the smallest $b \in \mathbb{Z}^+$ such that $13 \mid b$ and $b \equiv 3 \pmod{11}$?

(c) Find the multiplicative inverse of 11 modulo 13.

(d) What is the smallest $a \in \mathbb{Z}^+$ such that $11 \mid a$ and $a \equiv 7 \pmod{13}$?

(e) Now, write down the set of possible solutions.