CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song DIS 4A

1 Bijections

Let n be an odd number. Let $f(x)$ be a function from $\{0,1,\ldots,n-1\}$ to $\{0,1,\ldots,n-1\}$. 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 $f(x) = x^2 \pmod{n}$.

2 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 $a, a^2, a^3, \ldots \pmod{m}$. Prove that this sequence has repetitions.

(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?

3 Combining Moduli

Suppose we wish to work modulo $n = 40$. Note that $40 = 5 \times 8$, with $\gcd(5,8) = 1$. We will show that in many ways working modulo 40 is the same as working modulo 5 and modulo 8, in the sense that instead of writing down $c \pmod{40}$, we can just write down $c \pmod 5$ and $c \pmod 8$.

(a) What is $8 \pmod 5$ and $8 \pmod 8$? Find a number $a \pmod{40}$ such that $a \equiv 1 \pmod 5$ and $a \equiv 0 \pmod 8$.

(b) Now find a number $b \pmod{40}$ such that $b \equiv 0 \pmod 5$ and $b \equiv 1 \pmod 8$.

(c) Now suppose you wish to find a number $c \pmod{40}$ such that $c \equiv 2 \pmod 5$ and $c \equiv 5 \pmod 8$. Find c by expressing it in terms of a and b.

(d) Repeat to find a number $d \pmod{40}$ such that $d \equiv 3 \pmod 5$ and $d \equiv 4 \pmod 8$.

(e) Compute $c \times d \pmod{40}$. Is it true that $c \times d \equiv 2 \times 3 \pmod 5$, and $c \times d \equiv 5 \times 4 \pmod 8$?