CS 70 Discrete Mathematics and Probability Theory
Spring 2019 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 $a, a^2, a^3, \ldots \pmod m$. 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?

Solution:

(a) There are only m possible values mod m, and so after the m-th term we should see repetitions.

The pidgenhole principle applies here - we have m boxes that represent the different unique values that a^k can take on $\pmod m$. Then, we can view $a, a^2, a^3, \cdots$ as the objects to put in the m boxes. As soon as we have more than m boxes (in other words, we reach a^{m+1} in our sequence), the Pidgenhole Principle implies that there will be a collision, or that at least two numbers in our sequence take on the same value $\pmod m$.

(b) We will temporarily use the notation a^* for the multiplicative inverse of a to avoid confusion. If we multiply both sides by $(a^*)^j$ in the third line below, we get

$$\begin{aligned}
a^i &\equiv a^j && \pmod m,\\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}} && \pmod m,\\
a^{i-j}\underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} &\equiv \underbrace{a\cdots a}_{j \text{ times}}\cdot\underbrace{a^*\cdots a^*}_{j \text{ times}} && \pmod m,\\
a^{i-j} &\equiv 1 && \pmod m.
\end{aligned}$$

(c) We can rewrite $a^{i-j} \equiv 1 \pmod m$ as $a^{i-j-1}a \equiv 1 \pmod m$. Therefore a^{i-j-1} is the multiplicative inverse of $a \pmod m$.

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

Solution:

(a) Bijection, because there exists the inverse function $g(y) = 2^{-1}y \pmod{n}$. Since n is odd, $\gcd(2,n) = 1$, so the multiplicative inverse of 2 exists.

(b) Not necessarily a bijection. For example, $n = 5, f(0) = f(1) = 0$.

(c) Bijection, because the multiplicative inverse is unique.

(d) Definitely not a bijection. For example, if $n = 3$, $f(1) = f(2) = 1$.

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 for x.

Solution:

(a) 6.

(b) We want to make sure that $b \equiv 0 \bmod 13$, we can see that 13×3 satisfies this requirement. To make sure b is still equivalent to 3 mod 11, we can multiply by the multiplicative inverse of 13 mod 11, which is 6 (from the last part). Although $13 \times 6 \times 3$ yields a correct answer, it is not the smallest number that meets both requirements. To do so, we can apply the modulus before multiplying by 13, giving us

$$13 \times ((6 \times 3) \bmod 11) = 91$$

(c) 6.

(d) Following a similar process to part (b), we get $11 \times ((6 \times 7) \bmod 13) = 33$

(e) $x \equiv 91 + 33 \pmod{\text{lcm}(11, 13)} \equiv 124 \pmod{143}$.