

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

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 $n = 3, f(1) = f(2) = 1$.

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 $a, a^2, a^3, \dots \pmod{m}$. 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 ?

Solution:

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

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

- (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 $a \pmod{m}$.

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 $c \times d \equiv 5 \times 4 \pmod{8}$?

Solution:

- (a) $8 \equiv 3 \pmod{5}$ and $8 \equiv 0 \pmod{8}$. We can find such a number by considering multiples of 8, i.e. 0, 8, 16, 24, 32, and find that if $a = 16$, $16 \equiv 1 \pmod{5}$. Therefore 16 satisfies both conditions.
- (b) We can find such a number by considering multiples of 5, i.e. 0, 5, 10, 15, 20, 25, 30, 35, and find that if $b = 25$, $25 \equiv 1 \pmod{8}$, so it satisfies both conditions.

- (c) We claim $c \equiv 2a + 5b \equiv 37 \pmod{40}$. To see that $c \equiv 2 \pmod{5}$, we note that $b \equiv 0 \pmod{5}$ and $a \equiv 1 \pmod{5}$. So $c \equiv 2a \equiv 2 \pmod{5}$. Similarly $c \equiv 5b \equiv 5 \pmod{8}$.
- (d) We can repeat the same procedure as above, and find that $d = 3a + 4b \equiv 28 \pmod{40}$.
- (e) $c \times d = 37 \times 28 \equiv 36 \pmod{40}$. Note that if $w \equiv x \pmod{n}$ and $y \equiv z \pmod{n}$ then $w \times y \equiv x \times z \pmod{n}$. Therefore we can multiply $c \equiv 2 \pmod{5}$ and $d \equiv 3 \pmod{5}$ to get $c \times d \equiv 2 \times 3 \pmod{5}$. Similarly we can multiply these equations modulo 8 and get $c \times d \equiv 5 \times 4 \pmod{8}$.