

## Section 2.3 Properties of Functions

Let  $f : A \rightarrow B$  be a function. There are three properties that  $f$  might possess.

**Injective (also called one-to-one):** Distinct elements in  $A$  map to distinct elements in  $B$ .

In other words,  $x \neq y$  implies  $f(x) \neq f(y)$  or, equivalently,  $f(x) = f(y)$  implies  $x = y$ .

Example. Let  $f : \mathbf{N}_8 \rightarrow \mathbf{N}$  be defined by  $f(x) = 2x \bmod 8$ .  $f$  is not injective. e.g.,  $f(0) = f(4)$ .

Quiz (1 minute). Let  $f : \mathbf{Z} \rightarrow \mathbf{N}$  be defined by  $f(x) = x^2$ . Is  $f$  injective?

Answer. No. e.g.,  $f(2) = f(-2)$ .

Quiz (1 minute). Are any of the three functions injective?  $\log_2$ , floor, ceiling.

Answer.  $\log_2$  is injective, but floor and ceiling are not.

**Surjective (also called onto):** The range is the codomain.

In other words, each  $b \in B$  has the form  $b = f(a)$  for some  $a \in A$ .

Example.  $f : \mathbf{Z} \rightarrow \mathbf{N}$  defined by  $f(x) = x^2$  is not surjective. E.g., 2 is not a square.

Example.  $f : \mathbf{Z} \rightarrow \mathbf{N}$  defined by  $f(x) = |x|$  is surjective but not injective.

**Bijective (also called one-to-one and onto):** Both injective and surjective.

Example. Let  $f : \mathbf{N} \rightarrow \{a\}^*$  by  $f(n) = a^n$ . Then  $f$  is a bijection.

Example. The function  $f : (0, 1) \rightarrow (2, 5)$  defined by  $f(x) = 3x + 2$  is a bijection.

Proof: If  $f(x) = f(y)$ , then  $3x + 2 = 3y + 2$ , which implies that  $x = y$ . So  $f$  is injective.

Let  $y \in (2, 5)$ . Does  $y = f(x) = 3x + 2$  for some  $x \in (0, 1)$ ? Solve the equation for  $x$  to get  $x = (y - 2)/3$ . Since  $y \in (2, 5)$ , we have  $y - 2 \in (0, 3)$ . So  $x = (y - 2)/3 \in (0, 1)$ . Thus  $f(x) = y$ . So  $f$  is surjective. Thus  $f$  is bijective.

Quiz (2 minutes). Let  $f : \mathbf{R} \rightarrow \mathbf{R}$  by  $f(x) = x^3$ . Is  $f$  bijective?

**Inverses:** If  $f : A \rightarrow B$  is a bijection, then there is an inverse function  $g : B \rightarrow A$  defined by  $g(b) = a$  iff  $f(a) = b$ . The inverse of  $f$  is denoted by  $f^{-1}$ .

Example. We have observed that the function  $f : (0, 1) \rightarrow (2, 5)$  defined by  $f(x) = 3x + 2$  is a bijection. So  $f^{-1} : (2, 5) \rightarrow (0, 1)$  is defined by  $f^{-1}(x) = (x - 2)/3$ .

Example.  $f : \mathbf{N}_5 \rightarrow \mathbf{N}_5$  defined by  $f(x) = (4x + 1) \bmod 5$  is a bijection (check each value). So it has an inverse. To see that it is a bijection (without listing the values) and to find a formula for the inverse, we can apply the following theorem.

### **Theorem (mod and inverses)**

Let  $n > 1$  and  $f : \mathbf{N}_n \rightarrow \mathbf{N}_n$  be defined by  $f(x) = (ax + b) \bmod n$ . Then

- $f$  is bijective iff  $\gcd(a, n) = 1$ .
- If so, then  $f^{-1}(x) = (kx + c) \bmod n$  where  $f(c) = 0$  and  $1 = ak + nm$ .

*Example.* Let  $f : \mathbf{N}_5 \rightarrow \mathbf{N}_5$  be defined by  $f(x) = (4x + 1) \bmod 5$ . Since  $\gcd(4, 5) = 1$ , the theorem says that  $f$  is a bijection. We test values to find  $c$  such that  $f(c) = 0$ . e.g.,  $f(1) = 0$ . We can use Euclid's algorithm to verify that  $1 = \gcd(4, 5)$  and then work backwards through the equations to find that  $1 = 4(-1) + 5(1)$ . So  $k = -1$ .

Thus  $f^{-1}(x) = (-x + 1) \bmod 5$ . (Check it out).

*Quiz:* Let  $f : \mathbf{N}_{13} \rightarrow \mathbf{N}_{13}$  be defined by  $f(x) = (7x + 5) \bmod 13$ . Find  $f^{-1}$  if it exists.

*Answer:*  $\gcd(7, 13) = 1$ . So  $f$  is a bijection.  $f(3) = 0$  and  $1 = 7(2) + 13(-1)$ .

So we can write  $f^{-1}(x) = (2x + 3) \bmod 13$ .

## Pigeon Hole Principle

If  $m$  things are put into  $n$  places and  $m > n$ , then one place has two or more things. Another way to say this is that if  $A$  and  $B$  are finite sets with  $|A| > |B|$ , then there are no injections from  $A$  to  $B$ .

Example. The function  $f : \mathbb{N}_7 \rightarrow \mathbb{N}_6$  defined by  $f(x) = x \bmod 6$  has  $f(0) = f(6)$ .

Example. In Mexico City there are two people with the same number of hairs on their heads. Everyone has less than 10 million hairs on their head and the population of Mexico City is more than 10 million. So the pigeon hole principle applies.

Example. If 11 numbers are chosen from  $S = \{1, 2, 3, \dots, 19, 20\}$ , then for two of the numbers chosen one divides the other.

Proof: Each natural number  $x \geq 1$  has a factorization  $x = 2^k m$  for some  $k \geq 0$  where  $m$  is odd. So the numbers in  $S$  can be written in this form:

$$1 = 2^0 \cdot 1, 2 = 2^1 \cdot 1, 3 = 2^0 \cdot 3, 4 = 2^2 \cdot 1, 5 = 2^0 \cdot 5, \dots, 12 = 2^2 \cdot 3, \dots, 19 = 2^0 \cdot 19, 20 = 2^2 \cdot 5.$$

Notice that the values of  $m$  are in the set  $\{1, 3, 5, 7, 9, 11, 13, 15, 17, 19\}$ , which has 10 elements. So by the pigeon hole principle two of the 11 chosen numbers, say  $x$  and  $y$ , must share the same  $m$ . i.e.,  $x = 2^k m$  and  $y = 2^j m$  for  $k \neq j$ . So either  $x \mid y$  or  $y \mid x$ . QED.

Quiz (2 minutes). Find 10 numbers in  $S$  that don't divide each other.

An answer: 6, 7, 8, 9, 11, 13, 15, 17, 19, 20.

## Ciphers and the mod function (some cryptology)

Let the letters from  $a$  to  $z$  be represented by  $0, 1, \dots, 25$ , respectively.

Now any bijection  $f : \mathbb{N}_{26} \rightarrow \mathbb{N}_{26}$  can act as a cipher and its inverse  $f^{-1}$  can act as a decipher.

*Example* (additive cipher):  $f(x) = (x + 2) \bmod 26$  and  $f^{-1}(x) = (x + 24) \bmod 26$ .

*Example* (multiplicative cipher):  $f(x) = 3x \bmod 26$  and  $f^{-1}(x) = 9x \bmod 26$ .

*Example* (affine cipher):  $f(x) = (5x + 1) \bmod 26$  and  $f^{-1}(x) = (-5x + 5) \bmod 26$ .

Some ciphers keep one or more letters fixed. For example, the cipher  $f(x) = 3x \bmod 26$  has  $f(0) = 0$ , so it sends the letter a to itself. The following theorem can be used to construct ciphers with no fixed letters.

### Mod and Fixed Points

Let  $n > 0$  and let  $f : \mathbf{N}_n \rightarrow \mathbf{N}_n$  be defined by  $f(x) = (ax + b) \bmod n$ . Then  $f$  has no fixed points iff  $\gcd(a - 1, n)$  does not divide  $b$ .

*Example.* Both the additive and affine ciphers in the preceding examples have no fixed points.

## Hash Functions

The goal is to use a key of some kind to look up information in a table, but without searching. A hash function maps a set  $S$  of keys into a finite set  $\mathbf{N}_n$  of table indexes. The table is called a hash table. Collisions occur if the function is not injective. If there are no collisions, then any key in  $S$  is mapped to the index where the information is stored without any searching.

*Example.* Let  $S$  be the students in a class and let  $h : S \rightarrow \mathbf{N}_{366}$  be defined by letting  $h(x)$  be the birthday of  $x$ . If two people have the same birthday, then a collision occurs.

## Resolving Collisions by Linear Probing

If a collision occurs at index  $k$ , then some key is placed in location  $k$  and the other colliding keys must be located elsewhere. Linear probing is a technique to search (probe) for an open place in the table by looking linearly at the following places, where  $g$  is a fixed gap:

$$(k + g) \bmod n, \quad (k + 2g) \bmod n, \quad \dots, \quad (k + (n - 1)g) \bmod n.$$

Example. Let  $S = \{\text{jan, feb, mar, apr, may, jun}\}$  and let  $h : S \rightarrow \mathbf{N}_6$  be defined by  $h(xyz) = p(x) \bmod 6$ , where  $p(x)$  is the position of  $x$  in the alphabet ( $p(a) = 1, \dots, p(z) = 26$ ).

We'll place the keys from  $S$  into a hash table by first placing jan, then feb, and so on.  $h(\text{jan}) = p(j) \bmod 6 = 10 \bmod 6 = 4$ . So place jan in position 4 of the table. Continue the process to get  $h(\text{feb}) = 0$ ,  $h(\text{mar}) = 1$ ,  $h(\text{apr}) = 1$  (collision with mar),  $h(\text{may}) = 1$  (collision with mar and apr), and  $h(\text{jun}) = 4$  (collision with jan).

The table shows the result of resolving collisions by linear probing with a gap of 1.

0	feb
1	mar
2	apr
3	may
4	jan
5	jun

Quiz (2 minutes). Resolve collisions with gap = 2.

Answer: feb, mar, jun, apr, jan, may.

Quiz (2 minutes). Resolve collisions with gap = 3.

Answer: *feb, mar, blank, blank, jan, blank.* (*apr, may, and jun* are not placed).

**Property:** If  $n$  is the table size and  $g$  is a gap, then

$\gcd(g, n) = 1$  implies that all indexes are probed with gap  $g$ .

So we were lucky to fill the table when the gap was 2. If the table size is a prime number  $p$ , then any gap other than  $p$  will insure that all keys are entered in the table.