MA014G
Algebra and Discrete Mathematics A

Lecture Notes 4

Autumn 2007

Pia Heidtmann
070811

CONGRUENCES

Definition

Let n be a positive integer.

Two integers a and b are said to be congruent modulo n, written

$$a \equiv b \pmod{n}$$

if $n \mid (a-b)$.

EXAMPLE

$10 \equiv 13 \pmod{3}$ because $10-13=-3$ and $3 \mid (-3)$

$20 \equiv 52 \pmod{2}$ because $20-52=-32$ and $2 \mid (-32)$

$37 \equiv 1 \pmod{2}$ because $37-1=36$ and $2 \mid 36$

There are several other ways of expressing that a and b are congruent modulo n:

Theorem [$a \equiv b \pmod n$]

Two integers a and b are congruent modulo n if and only if

(i) $n \mid (a-b)$ (this is the original definition)

(ii) a and b give the same remainder on division by n

(iii) there is an integer k such that $a = b + kn$

(iv) $a - b \equiv 0 \pmod n$.

(v) $a - b = kn$ for some integer k.

EXAMPLE

37 is congruent to 25 modulo 2

$$37 \equiv 25 \pmod 2.$$

because $2 \mid (37-25)$.

But also

(ii) 37 gives remainder 1 on division by 2

25 gives remainder 1 on division by 2

(v) $37 - 25 = 12 = 6 \cdot 2$

(iii) $37 = 25 + 6 \cdot 2$

(iv) $37 - 25 = 12$ and $12 \equiv 0 \pmod 2$ because $2 \mid (12 - 0)$.

The Division Algorithm

Given any number a and a positive number n, then there exist unique integers k and r such that

$$a = kn + r \quad \text{and} \quad 0 \leq r \leq n-1.$$

For congruences this means

Theorem Let a be any integer.
There is a unique integer r in the set $\{0, 1, 2, \dots, n-1\}$ such that

$$a \equiv r \pmod{n}$$

EXAMPLE

Let $n = 5$.

$17 \equiv 2 \pmod{5}$ because $17-2$ is divisible by 5.

$17 \not\equiv 0 \pmod{5}$

$17 \not\equiv 1 \pmod{5}$

$17 \not\equiv 3 \pmod{5}$

$17 \not\equiv 4 \pmod{5}$

Example

Let us determine the set of integers which are congruent to $0, 1, 2, 3$ or $4 \pmod 5$

The set of integers congruent to 0 modulo 5 is $C_0 =$
$\{\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots\} = \{x \mid x = 5z, z \in \mathbb{Z}\}$

The set of integers a such that $a \equiv 1 \pmod 5$ is $C_1 =$

$\{\ldots, -14, -9, -4, 1, 6, 11, 16, \ldots\} = \{x \mid x = 5z + 1, z \in \mathbb{Z}\}$.

The set of integers a such that $a \equiv 2 \pmod 5$ is $C_2 =$
$\{\ldots, -13, -8, -3, 2, 7, 12, 17, \ldots\} = \{x \mid x = 5z + 2, z \in \mathbb{Z}\}$.

The set of integers a such that $a \equiv 3 \pmod 5$ is $C_3 =$
$\{\ldots, -12, -7, -2, 3, 8, 13, 18, \ldots\} = \{x \mid x = 5z + 3, z \in \mathbb{Z}\}$

The set of integers a such that $a \equiv 4 \pmod 5$ is $C_4 =$
$\{\ldots, -11, -6, -1, 4, 9, 14, 19, \ldots\} = \{x \mid x = 5z + 4, z \in \mathbb{Z}\}$

> **Definition**
>
> The set of all integers a such that $a \equiv b \pmod n$ is known as the congruence class modulo n with representative b and we write $[b]_n$ for this set or just $[b]$ if it is clear from the context what n is.

Note in the above example $C_3 = [3]_5 = [8]_5 = [13]_5 = [-2]_5 = \cdots$

Result

Congruence modulo n, where n is a positive integer, partitions the integers into n disjoint sets:

Let $\mathcal{C}_0 = \{x \in \mathbb{Z} \mid x \equiv 0 \pmod{n}\} = [0]_n$

$\mathcal{C}_1 = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod{n}\} = [1]_n$

$\mathcal{C}_2 = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod{n}\} = [2]_n$

$\vdots$

$\mathcal{C}_{n-1} = \{x \in \mathbb{Z} \mid x \equiv n-1 \pmod{n}\} = [n-1]_n$

Then $\mathcal{C}_0 \cup \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_n = \mathbb{Z}$ and $\mathcal{C}_i \cap \mathcal{C}_j = \emptyset$ when $i \neq j$.

EXAMPLE

Let $n=3$.

$\mathcal{C}_0 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = [0]_3$

$\mathcal{C}_1 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\} = [1]_3$

$\mathcal{C}_2 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\} = [2]_3$

Note that if $x \in \mathcal{C}_i$ and $y \in \mathcal{C}_i$ then $x \equiv y \pmod{3}$.

But if $x \in \mathcal{C}_i$ and $y \in \mathcal{C}_j$ where $i \neq j$ then $x \not\equiv y \pmod{3}$.

We saw that there are precisely 3 congruence classes (mod 3) and precisely 5 congruence classes (mod 5).

By the result on page 71 there are generally n congruence classes (mod n), namely

$$[0]_n,\ [1]_n,\ [2]_n,\ \dots,\ [n-1]_n.$$

But note that we might have chosen any element of each class as representative of the class rather than the representative between 0 and $n-1$.

$$[0]_n = [n]_n = [-n]_n = [2n]_n = [-2n]_n = \cdots$$
$$[1]_n = [n+1]_n = [1-n]_n = [2n+1]_n = [1-2n]_n = \cdots$$
$$[2]_n = [n+2]_n = [2-n]_n = [2n+2]_n = [2-2n]_n = \cdots$$
$$\vdots$$
$$[n-1]_n = [2n-1]_n = [-1]_n = [3n-1]_n = [-n-1]_n = \cdots$$

However, it is usual to use the numbers $0, 1, \dots, n-1$ as class representatives whenever possible.

Definition

Let $\mathbb{Z}_n$ be the set of congruence classes modulo n:

$$\mathbb{Z}_n = \{ [0]_n, [1]_n, [2]_n, \dots, [n-1]_n \}.$$

We call $\mathbb{Z}_n$ the set of integers modulo n. heltalen (mod n)

When it is clear from the context which "modulo n" we mean, we shall usually just write

$$\mathbb{Z}_n = \{ [0], [1], [2], \dots, [n-1] \}.$$

We can define an addition $\oplus$ and a multiplication $\odot$ for congruence classes as follows:

addition of ordinary integers.

$$[x] \oplus [y] := [x+y]$$

$$[x] \odot [y] := [xy]$$

ordinary multiplication

EXAMPLE

$\mathbb{Z}_3 = \{ [0], [1], [2] \}$ where e.g. $[1] = \{ \dots, -5, -2, 1, 4, 7, \dots \}$.

We can compute the addition table and multiplication table for $\mathbb{Z}_3$:

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Result [Rules of arithmetic in $\mathbb{Z}_n$]

The set of integers modulo n together with its addition $\oplus$ and multiplication $\odot$ satisfies the following rules of arithmetic:

1. For all $[x], [y] \in \mathbb{Z}_n$ we have
$$[x] \oplus [y] \in \mathbb{Z}_n \quad \text{and} \quad [x] \odot [y] \in \mathbb{Z}_n.$$

2. For all $[x], [y], [z] \in \mathbb{Z}_n$ we have
$$[x] \oplus ([y] \oplus [z]) = ([x] \oplus [y]) \oplus [z] \quad \text{and}$$
$$[x] \odot ([y] \odot [z]) = ([x] \odot [y]) \odot [z].$$

3. The element $[0] \in \mathbb{Z}_n$ is such that
$$[x] \oplus [0] = [0] \oplus [x] = [x]$$
for all $[x] \in \mathbb{Z}_n$.

   The element $[1] \in \mathbb{Z}_n$ is such that $[1] \neq [0]$ and
$$[x] \odot [1] = [1] \odot [x] = [x]$$
for all $[x] \in \mathbb{Z}_n$.

4. For all $[x] \in \mathbb{Z}_n$ there is an element $[-x] \in \mathbb{Z}_n$ such that
$$[x] \oplus [-x] = [-x] \oplus [x] = [0].$$

5. For all $[x], [y] \in \mathbb{Z}_n$ we have
$$[x] \oplus [y] = [y] \oplus [x] \text{ and}$$
$$[x] \odot [y] = [y] \odot [x].$$

6. For all $[x], [y], [z] \in \mathbb{Z}_n$ we have that
$$[x] \odot ([y] \oplus [z]) = ([x] \odot [y]) \oplus ([x] \odot [z])$$

In short : all the usual rules of arithmetic for integers also work in $\mathbb{Z}_n$ - except one :

For the ordinary integers we have the following rule, which is known as the Zero-divisor law (lagen om nolldelare). It says :

For all integers x and y, if $x \cdot y = 0$ then $x = 0$ or $y = 0$ (or both).

EXAMPLE

You have used the zero-divisor law often when solving equations :

$$(x+2)(x+4) = 0 \Rightarrow (x+2) = 0 \text{ or } (x+4) = 0 \Rightarrow x = -2 \text{ or } x = -4$$

here you used the zero-divisor law.

EXAMPLE

The zero-divisor law does <u>not</u> hold in $\mathbb{Z}_6$:

$$\mathbb{Z}_6 = \{ [0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6 \}.$$

$$[4]_6 \odot [3]_6 = [12]_6 = [0]_6$$

So in $\mathbb{Z}_6$ $[4] \odot [3] = [0]$

while both $[4] \neq [0]$ and $[3] \neq [0]$

EXAMPLE

The zero-divisor law does not hold in $\mathbb{Z}_4$, for e.g.

$$[2]_4 \odot [2]_4 = [4]_4 = [0]_4.$$

There are n for which the zero-divisor law does hold in $\mathbb{Z}_n$ though:

EXAMPLE

The zero-divisor law holds in $\mathbb{Z}_3$ because when considering the multiplication table for $\mathbb{Z}_3$ we find that in $\mathbb{Z}_3$

$$[a]_3 \odot [b]_3 = [0] \text{ only when } [a]_3 = [0] \text{ or } [b]_3 = [0]$$

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Theorem

Let $n \geq 2$ be an integer.

The zero-divisor law holds in $\mathbb{Z}_n$ if and only if n is a prime.

Förkortningsregeln

Theorem (Cancellation rule for $\mathbb{Z}_p$ where p prime)

If p is a positive prime and $[a] \in \mathbb{Z}_p$ where $[a] \neq [0]$

then

if $[a] \odot [x] = [a] \odot [y]$ for some $[x], [y] \in \mathbb{Z}_p$

then $[x] = [y]$.

EXAMPLE

In $\mathbb{Z}_3$ if $[2]_3 \odot [x]_3 = [2]_3 \odot [y]_3$ then $[x]_3 = [y]_3$.

WARNING

The cancellation rule does NOT hold in $\mathbb{Z}_n$ if n is a composite positive integer, e.g. in $\mathbb{Z}_6$ we have

$$[2]_6 \odot [3]_6 = [6]_6 = [0]_6$$

and $[2]_6 \odot [0]_6 = [0]_6$

So

$$[2]_6 \odot [3]_6 = [2]_6 \cdot [0]_6$$

but $[3]_6 \neq [0]_6$.

Solving equations

EXAMPLE

How do we solve an equation like e.g.

$$3X = 12$$

in the ordinary real numbers $\mathbb{R}$?

A solution:

$$3X = 12$$

Now, in the real numbers $\mathbb{R}$ there is the number $\frac{1}{3}$. We multiply the equation through by this number:

$$\frac{1}{3} \cdot 3X = \frac{1}{3} \cdot 12$$
$$\Downarrow$$
$$\left(\frac{1}{3} \cdot 3\right) X = 4$$
$$\Downarrow$$
$$\underline{\underline{X = 4}}$$

The number $\frac{1}{3}$ is known as the multiplicative inverse of 3

In the same way we define:

$[m] \in \mathbb{Z}_n$ is called a multiplicative inverse of $[x] \in \mathbb{Z}_n$ if

$$[x]_n \odot [m]_n = [m]_n \odot [x]_n = [1]_n .$$

EXAMPLE

$[2]_5$ is the multiplicative inverse of $[3]_5$ in $\mathbb{Z}_5$ because

$$[2]_5 \odot [3]_5 = [6]_5 = [1]_5$$

Not every element in $\mathbb{Z}_n$ has a multiplicative inverse:

EXAMPLE

$[2]_6$ has no multiplicative inverse in $\mathbb{Z}_6$.
To see this, note that $[1]_6$ does not appear in the row for $[2]_6$ in the multiplication table for $\mathbb{Z}_6$:

$\odot$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]_6$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[2]_6$	$[0]$	$[2]$	$[4]$	$[0]$	$[2]$	$[4]$
$[3]_6$	$[0]$	$[3]$	$[0]$	$[3]$	$[0]$	$[3]$
$[4]_6$	$[0]$	$[4]$	$[2]$	$[0]$	$[4]$	$[2]$
$[5]_6$	$[0]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Note that $[5]_6$ has a multiplicative inverse in $\mathbb{Z}_6$:

$$[5]_6 \odot [5]_6 = [1]_6,$$

so $[5]_6$ is its own inverse!

Theorem

Let $n \geq 2$ be a positive integer, and let $[x]_n \in \mathbb{Z}_n$ be such that $[x]_n \neq [0]_n$. Then $[x]_n$ has a multiplicative inverse in $\mathbb{Z}_n$ if and only if $\gcd(x,n) = 1$. Further, if the multiplicative inverse exists, it is unique.

EXAMPLE

The elements in $\mathbb{Z}_6$ which have multiplicative inverses are $[1]_6$ and $[5]_6$.
$[2]_6$, $[3]_6$ and $[4]_6$ have no multiplicative inverse in $\mathbb{Z}_6$ for $\gcd(2,6)=2$, $\gcd(3,6)=3$ and $\gcd(4,6)=2$.

PROOF

Suppose that $\gcd(x,n)=1$

Then use Euclid's algorithm to find $s,t \in \mathbb{Z}$ such that

$$1 = sx + tn$$
$$\Updownarrow$$
$$sx = 1 - tn$$
$$\Updownarrow$$
$$sx \equiv 1 \pmod{n}$$
$$\Updownarrow$$
$$[s]_n \odot [x]_n = [1]_n$$
$$\Updownarrow$$

$[s]_n$ is a multiplicative inverse of $[x]_n$ in $\mathbb{Z}_n$.

Conversely, suppose $[x]_n$ has a multiplicative inverse $[a]_n \in \mathbb{Z}_n$

Then

$$[a]_n \odot [x]_n = [1]_n$$
$$\Updownarrow$$

$ax = 1 + kn$ for some $k \in \mathbb{Z}$

$$\Downarrow$$
$$ax + (-k)n = 1$$
$$\Downarrow$$

$\gcd(x,n) \mid 1$ (as the only integers that can be written as a linear combination of x and n are the ones divisible by $\gcd(x,n)$)

$$\Downarrow$$
$$\gcd(x,n) = 1$$

To see that the multiplicative inverse is unique:

Suppose $[a]_n \odot [x]_n = [1]_n = [b]_n \odot [x]_n$

$$\Downarrow$$

$$\begin{aligned}
\underline{[a]_n} = [a]_n \odot [1]_n &= [a]_n \odot ([b]_n \odot [x]_n) \\
&= [a]_n \odot ([x]_n \odot [b]_n) \\
&= ([a]_n \odot [x]_n) \odot [b]_n \\
&= [1]_n \odot [b]_n \\
&= \underline{[b]_n}
\end{aligned}$$

METHOD

We find the multiplicative inverse in $\mathbb{Z}_n$ of $[a]_n$ by using Euclid's Algorithm:

① $\gcd(a,n)=1$ otherwise $[a]$ has no inverse in $\mathbb{Z}_n$.

② Find $s,t \in \mathbb{Z}$ such that $sa+tn=1$. by Euclid's algorithm.

③ Then the solutions to $[a]\odot[x]=[1]$ are all elements in $[s]$.

EXAMPLE

Find the multiplicative inverse of $[5]$ in $\mathbb{Z}_{12}$.

① $\gcd(5,12)=1$

② Euclid's algorithm gives

$$12 = 5(2)+2 \quad \Rightarrow \quad 2 = 12+5(-2)$$

$$5 = 2(2)+\boxed{1} \quad \Rightarrow \quad 1 = 5+2(-2) = 5+[12+5(-2)](-2) = 5(5)+12(-2).$$

$$2 = 1(2)+0$$

$$1 = 5\cdot 5 + (-2)\cdot 12$$

③ So the multiplicative inverse of $[5]$ in $\mathbb{Z}_{12}$ is actually $[5]$ itself.

Aim: We want to find all possible $x \in \mathbb{Z}$ satisfying the congruence

$$ax \equiv b \pmod{n}.$$

Which is the same as finding all $[x] \in \mathbb{Z}_n$ satisfying the equation

$$[a]_n \odot [x]_n = [b]_n.$$

EXAMPLE

Any $[x] \in \mathbb{Z}_n$ which satisfies that

$$[a] \odot [x] = [1]$$

corresponds to $x \in \{1, 2, \dots, n-1\}$ solving the congruence

$$ax \equiv 1 \pmod{n}.$$

$[2] \in \mathbb{Z}_5$ satisfies that

$$[3]_5 \odot [2]_5 = [1]_5$$

So therefore $x=2$ satisfies the congruence

$$3x \equiv 1 \pmod{5}$$

Result [Solving $ax \equiv b \pmod{n}$ and $[a]_n \odot [x]_n = [b]_n$ in $\mathbb{Z}_n$]

Let $n \geq 2$ be an integer, and let also a and b be integers.
Let $\gcd(a,n) = g$

- If $g \nmid b$ the equation $[a]_n \odot [x]_n = [b]_n$ has no solution in $\mathbb{Z}_n$ and the congruence $ax \equiv b \pmod{n}$ has no solutions either.

- If $g \mid b$ the equation $[a]_n \odot [x]_n = [b]_n$ has precisely g solutions in $\mathbb{Z}_n$, namely $$[x]_n = [x_0 + t\tfrac{n}{g}]_n \quad \text{where } t = 0, 1, \ldots, g-1.$$

  and $x_0 \in \{0, 1, \ldots, \frac{n}{g} - 1\}$ is a solution of the reduced congruence
  $$\frac{a}{g} x \equiv \frac{b}{g} \pmod{\tfrac{n}{g}}$$

The elements in the congruence classes $[x_0 + t\frac{n}{g}]$, $t = 0, 1, \ldots, g-1$ are the solutions to the congruence $ax \equiv b \pmod{n}$.

EXAMPLE

Solve the congruence $5x \equiv 2 \pmod 7$

Note this corresponds to the equation

$$[5] \odot [x] = [2] \quad \text{in } \mathbb{Z}_7$$

① Find $\gcd(5,7) = 1$

So there is precisely 1 solution in $\mathbb{Z}_7$ of $[5] \odot [x] = [2]$.

② Find the reduced congruence:

$$5x \equiv 2 \pmod 7$$

is already reduced as $\gcd(5,7) = 1$.

③ Solve the reduced congruence by finding a multiplicative inverse of $[5]$ in $\mathbb{Z}_7$ and multiplying the reduced equation by it.

$7 = 5(1) + 2 \quad \Rightarrow 2 = 7 - 5$

$5 = 2(2) + 1 \quad \Rightarrow 1 = 5 + 2(-2) = 5 + [7-5](-2) = 5(3) + 7(-2)$

$2 = 1(2) + 0$

So $[3]$ is the multiplicative inverse of $[5]$ in $\mathbb{Z}_7$

$$\begin{aligned}
& [5]_7 \odot [x]_7 = [2]_7 \\
\Downarrow \quad & [3]_7 \odot [5]_7 \odot [x]_7 = [3]_7 \odot [2]_7 \\
\Downarrow \quad & [15]_7 \odot [x]_7 = [6]_7 \\
\Downarrow \quad & [1]_7 \odot [x]_7 = [6]_7 \\
\Downarrow \quad & [x]_7 = [6]_7
\end{aligned}$$

④ The solution to $[5] \odot [x] = [2]$ in $\mathbb{Z}_7$ is thus $\underline{[x] = [6]}$

The solutions to $5x \equiv 2 \pmod 7$ is

$x \in [6]_7$, that is $\underline{x \in \{\ldots, -15, -8, -1, 6, 13, 20, 27, \ldots\}}$

EXAMPLE

The congruence

$$4x \equiv 7 \pmod{18}$$

and the equation

$$[4]_{18} \odot [x]_{18} = [7]_{18} \text{ in } \mathbb{Z}_{18}$$

have no solutions as

$$\gcd(4, 18) = 2$$

and $2 \nmid 7$.

EXAMPLE

$\gcd(4,18)=2$ and $2 \mid 10$, so let us find all solutions x to the congruence

$$4x \equiv 10 \pmod{18}$$

and all solutions $[x]_{18}$ to the equation $[4]_{18} \odot [x]_{18} = [10]_{18}$ in $\mathbb{Z}_{18}$.

1. First solve the reduced congruence

$$2x \equiv 5 \pmod 9.$$

This is done by Euclid's Algorithm:

$\gcd(2,9)=1 = 9+2(-4)$ $\left[\begin{array}{ll} \text{because} & 9=2(4)+1 \Rightarrow 1=9+2(-4) \\ & 2=1(2)+0 \end{array}\right]$

So $1=(-4)2+1\cdot 9$

And so $[-4]_9=[5]_9$ is the multiplicative inverse of $[2]$ in $\mathbb{Z}_9$

$$[2]_9 \odot [x] = [5]_9$$
$$\Downarrow$$
$$[5]_9 \odot [2]_9 \odot [x] = [5]_9 \odot [5]_9$$
$$\Downarrow$$
$$[x]_9 = [25]_9 = [7]_9$$

So $x_0 \equiv 7 \pmod 9$ are all solutions to $2x_0 \equiv 5 \pmod 9$

2. The result from p. 82 now gives that

$[x]_{18} = [7 + t\,\frac{18}{2}]_{18}$ for $t=0,1$ are all solutions in $\mathbb{Z}_{18}$ of $[4]_{18}\odot[x]_{18}=[10]_{18}$, that is the two congruence classes which solve the equation are

$\underline{[x]=[7]_{18} \text{ and } [16]_{18}}$

And so the congruence $4x\equiv 10 \pmod{18}$ has solutions

$x \in [7]_{18}$ or $x \in [16]_{18}$, that is

$\underline{x \in \{\ldots,-29,-11,7,25,43,61,\ldots\} \text{ or } x \in \{\ldots,-20,-2,16,34,52,\ldots\}}$

A relation on a set X is just a subset $R \subseteq X \times X$.

We write $x R y$ to mean $(x,y) \in R$

EXAMPLE [relations]

Let X be the set of all people. The following are relations on X:

- $x R y$ if x is the same sex as y.
- $x R y$ if x has the same colour eyes as y.
- $x R y$ if x is younger than y
- $x R y$ if x is born in the same month as y
- $x R y$ if x is the mother of y
- $x R y$ if x knows y
- $x R y$ if x is the brother of y.

EXAMPLE [relations]

Let $X = \mathbb{Z}$. Then the following are relations on $\mathbb{Z}$

- xRy if x divides y
- xRy if $x > y$
- xRy if $x \leq y$
- xRy if $x = y$
- xRy if $x \equiv y \pmod 3$

EXAMPLE

Let $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Then R defined by

$$(x, y) \in R \text{ if } x \text{ divides } y$$

is a relation on X.

Note, we could also have written

$$xRy \text{ if } x \text{ divides } y$$

The two notations "xRy" and "$(x, y) \in R$" are the same thing.

We now list some properties that some relations have and some do not have.

Symmetry

Let R be a relation on a set X. Then R is symmetric if

$$xRy \Rightarrow yRx \quad \text{for all } x, y \in X.$$

Transitivity

Let R be a relation on a set X. Then R is transitive if

$$xRy \text{ and } yRz \Rightarrow xRz \quad \text{for all } x, y, z \in X.$$

Reflexivity

Let R be a relation on a set X. Then R is reflexive if

$$xRx \quad \text{for all } x \in X.$$

A relation which is reflexive, symmetric and transitive is called an equivalence relation.

An equivalence relation on a set X <u>partitions</u> the set X. Each part of the partition is a set of elements of X which are all related to each other by relation R. These parts are called equivalence classes.

EXAMPLE

> The relation R on the set of integers defined by
> $$xRy \text{ if and only if } 3 \mid (x-y)$$
> is an equivalence relation.

① We must check that the relation is reflexive, symmetric and transitive in order to prove this

ⓐ reflexive: For any $x \in \mathbb{Z}$ $x-x=0$ and $3 \mid 0$ so xRx for all $x \in \mathbb{Z}$.

ⓑ symmetric: For any $x, y \in \mathbb{Z}$ $x-y=-(y-x)$, so
if $3 \mid (x-y)$ then $3 \mid (y-x)$
and thus $xRy \Rightarrow yRx$ for all $x, y \in \mathbb{Z}$

ⓒ transitive: For any $x, y, z \in \mathbb{Z}$ if $3 \mid (x-y)$ and $3 \mid (y-z)$
then $3 \mid (x-z)$ as $x-z=(x-y)+(y-z)$.
thus xRy and $yRz \Rightarrow xRz$ for all $x, y, z \in \mathbb{Z}$.

② The equivalence classes of R are

$$C_0 = \{\ldots, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$$

$$C_1 = \{\ldots, -8, -5, -2, 1, 4, 7, 10, 13, \ldots\}$$

$$C_2 = \{\ldots, -7, -4, -1, 2, 5, 8, 11, 14, \ldots\}$$

Do you know another "name" for R?

Let us continue discussing properties a relation R on a set X may have. Until now we have met

reflexive relations, that is, xRx for all $x \in X$.

symmetric relations, that is, if xRy then yRx for all $x,y \in X$.

transitive relations, that is, if xRy and yRz then xRz for all $x,y,z \in X$.

There is one more important property a relation R on X may have:

Anti-symmetry

Let R be a relation on a set X. Then R is anti-symmetric if

$$xRy \text{ and } yRx \Rightarrow x=y \quad \text{for all } x,y \in X.$$

A relation which is reflexive, antisymmetric and transitive is called a partial order.

EXAMPLE

Let us show that the relation R on the power set $\mathcal{P}(X)$ of $X = \{a, b, c\}$ given by

$$A \, R \, B \quad \text{if and only if} \quad A \subseteq B. \quad \text{for all } A, B \in \mathcal{P}(X).$$

is a partial order.

If $X = \{a, b, c\}$ then

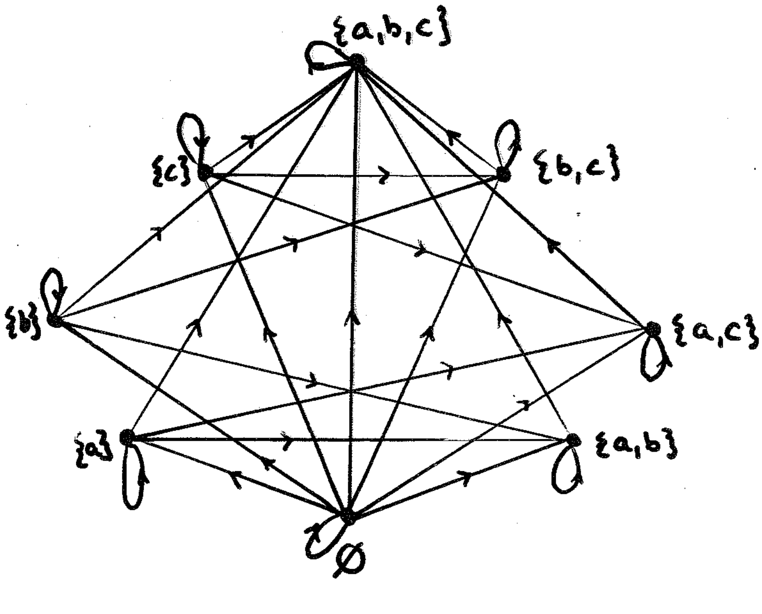
$$\mathcal{P}(X) = \{ \emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\} \}$$

We can draw a picture of R by creating a point for each element of $\mathcal{P}(X)$. We then draw an arrow

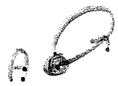
$$A \longrightarrow B$$

between $A, B \in \mathcal{P}(X)$ if $A R B$.

The picture looks like this:

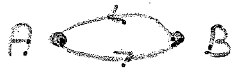


To check whether "$\subseteq$" is a partial order, we check

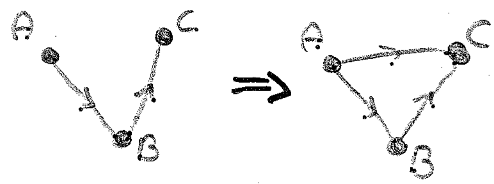
reflexive : $A \subseteq A$ for all $A \in \mathcal{P}(X)$ 

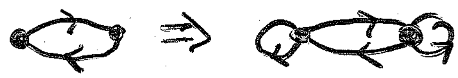
in the picture.

antisymmetric: $A \subseteq B$ and $B \subseteq A \Rightarrow A = B$ for all $A, B \in \mathcal{P}(X)$.

in the picture we do **NOT** have 

unless $A = B$.

transitive : $A \subseteq B$ and $B \subseteq C \Rightarrow A \subseteq C$ 



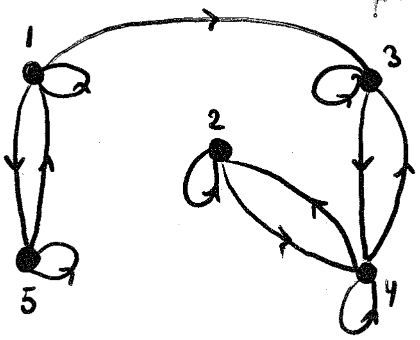
EXAMPLE

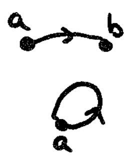
Let R be the relation on $X = \{1,2,3,4,5\}$ defined by

aRb if and only if $(a,b) \in \{(1,3), (2,4), (4,2), (1,5), (5,1), (3,3), (3,4), (1,1), (2,2), (4,3), (4,4), (5,5)\}$

Is R an equivalence relation?

Again we draw a picture of R:





aRb

aRa.

And we see that the relation is

- reflexive $\quad aRa$ for all $a \in X$
- not symmetric $\quad$ for $1R3$ but $3 \not R 1$
- not transitive $\quad$ for $2R4$ and $4R3$ but $2 \not R 3$

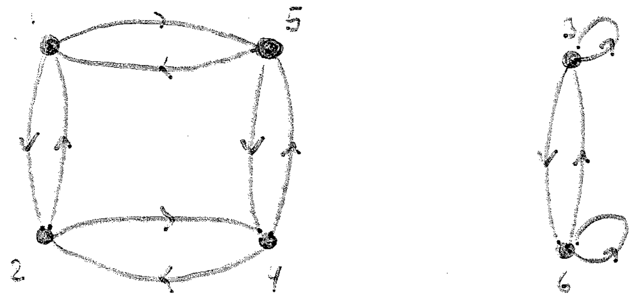
The relation is thus NOT an equivalence relation

Is the relation antisymmetric?

EXAMPLE

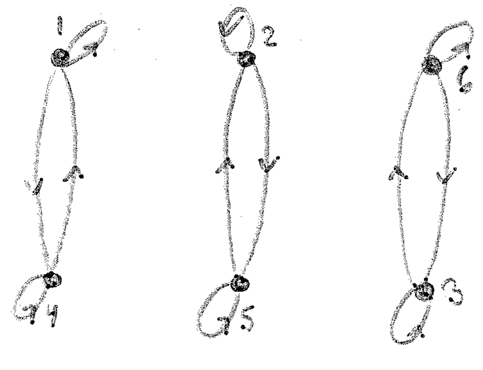
Let R be defined on $S = \{1,2,3,4,5,6\}$ by

(i) aRb if $3 \mid (a+b)$. Is R an equivalence relation? No



- not reflexive $1 \not R 1$
- symmetric ✓
- not transitive $1R5$, $5R4$ but $1 \not R 4$

(ii) aRb if $3 \mid (a-b)$. Is R an equivalence relation? Yes



- reflexive ✓
- symmetric ✓
- transitive ✓

(iii) aRb if $a=b$. Is R an equivalence relation? Yes

- reflexive ✓
- symmetric ✓
- transitive ✓
- antisymmetric ✓

RELATIONS

A relation R from a set X to a set Y is simply a subset of the Cartesian product $X \times Y$.

If $(x,y) \in R$ we write xRy and we say that x is related to y.

The set $\{x \in X \mid (x,y) \in R \text{ for some } y \in Y\}$ is called the domain of the relation R.

The set $\{y \in Y \mid (x,y) \in R \text{ for some } x \in X\}$ is called the range of the relation R.

EXAMPLE

Let $X = \{\overset{P}{\text{Pia}}, \overset{S}{\text{Sam}}, \overset{A}{\text{Alex}}\}$ $\quad Y = \{\overset{m}{\text{Mel}}, \overset{f}{\text{Fran}}\}$.

Then $X \times Y = \{(P,m), (P,f), (S,m), (S,f), (A,m), (A,f)\}$

One relation R from X to Y could be:

$$R = \{(P,m), (P,f), (S,m)\}$$

The domain of this relation is $\{P,S\}$

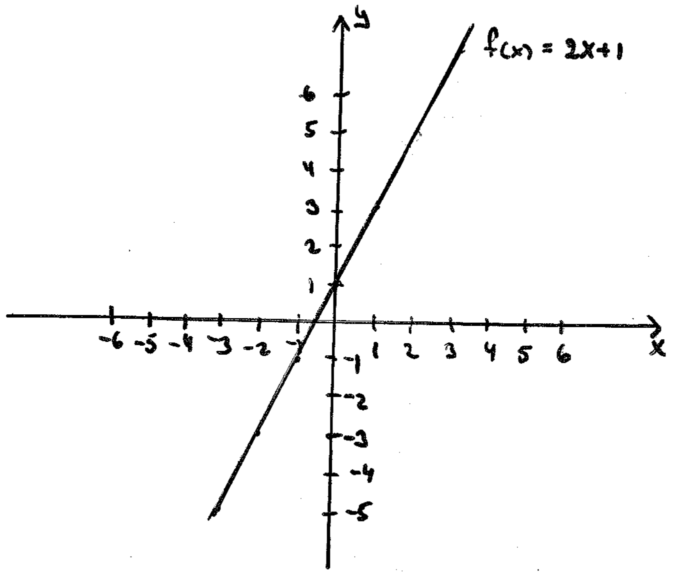
The range of the relation is $\{m,f\}$.

FUNCTIONS

A function is a relation from a set A to a set B so that for each "input" a there is exactly one "output" b.

EXAMPLES

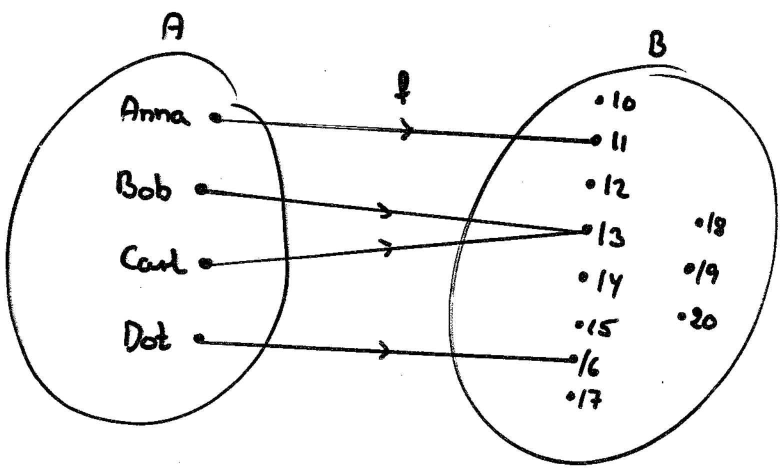
① $f: \mathbb{R} \to \mathbb{R}$ $\quad f(x) = 2x+1$



② $A = \{Anna, Bob, Carl, Dot\}$ $\quad B = \{10, 11, 12, \dots, 20\}$

$f: A \to B$ $\quad f(x) =$ the age of x

$f = \{(Anna, 11), (Bob, 13), (Carl, 13), (Dot, 16)\}$

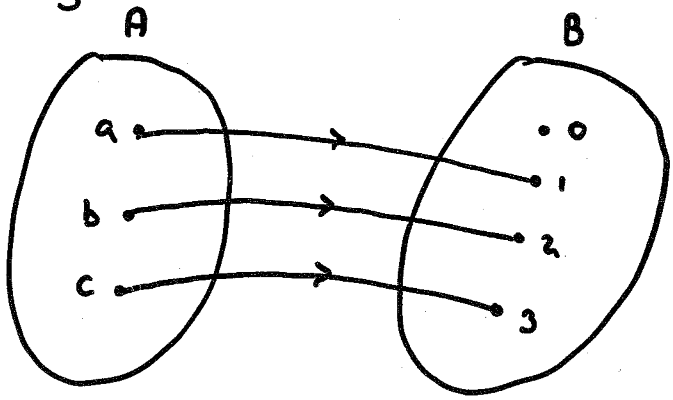


EXAMPLE

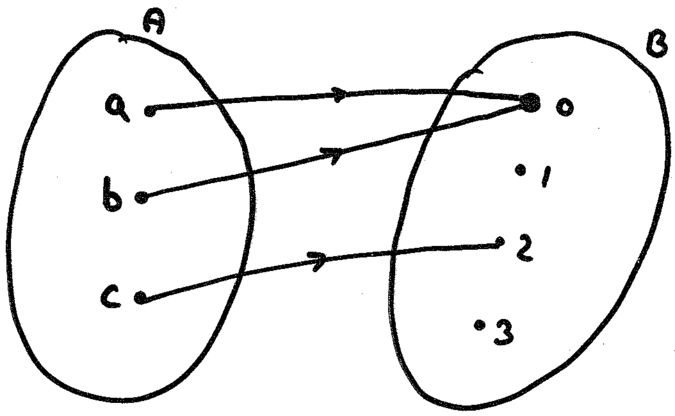
Let $A = \{a, b, c\}$ and $B = \{0, 1, 2, 3\}$

Which of the following are functions from A to B?

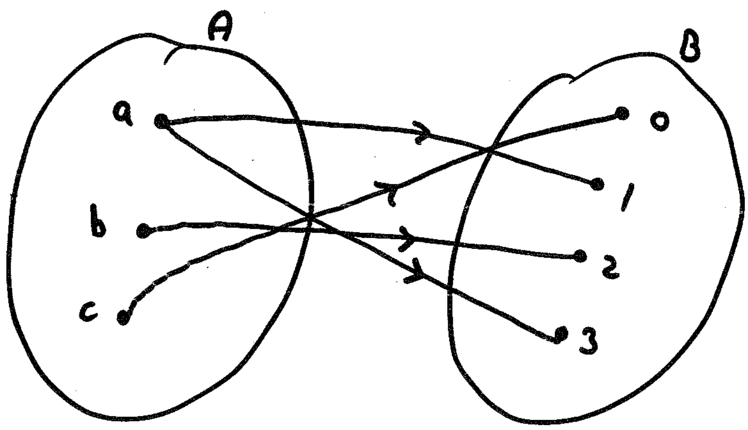
① f is given by



② g is given by



③ h is given by



Definition of function

Given two non-empty sets A and B, a function f from A to B, denoted by

$$f : A \to B$$

is a rule which assigns to each element $x \in A$ a unique element $y \in B$ called the image (bild) of x under f.

We write $f(x)$ to denote the unique image of x under f, that is

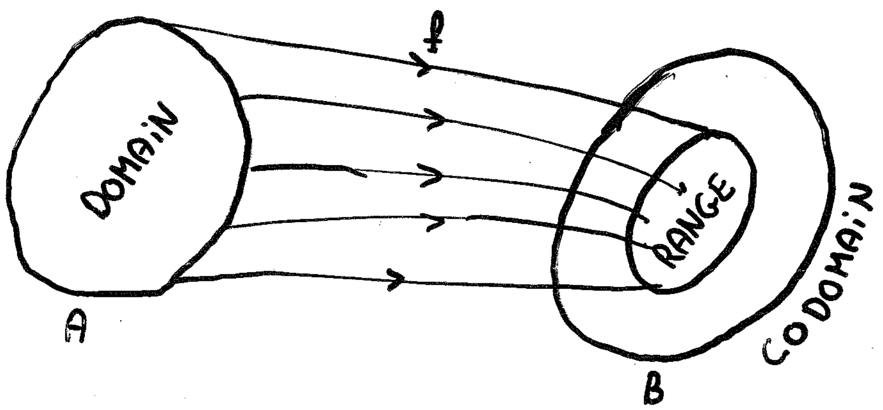
$$y = f(x).$$

If $f : A \to B$ is a function, the set A is called the domain of f, (domän el. definitionsmgd) and the set B is called the (kodomän el. bildmängd) codomain of f.

The (värdemängd) range of f is usually denoted by $f(A)$ and is the set

$$\{ f(x) \in B \mid x \in A \},$$

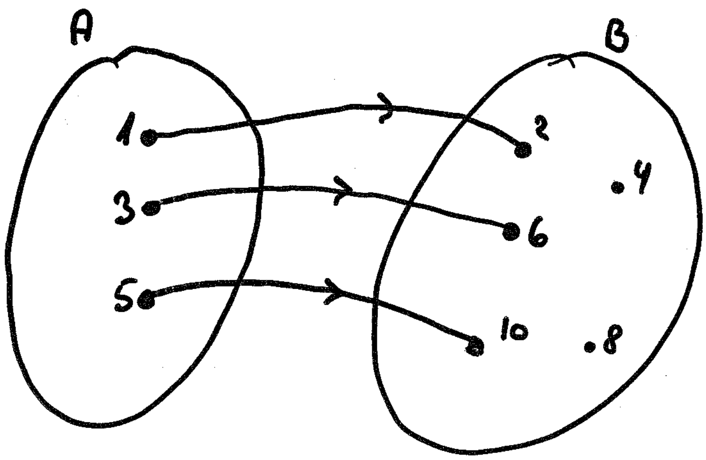
so the range are all elements in the codomain that are actually images of some x under f.



EXAMPLE

Let $A = \{1, 3, 5\}$ and $B = \{2, 4, 6, 8, 10\}$

Let $f : A \to B$ be given by the rule $f(x) = 2x$.



Domain f =

Codomain f =

Range f =

PROPERTIES OF FUNCTIONS

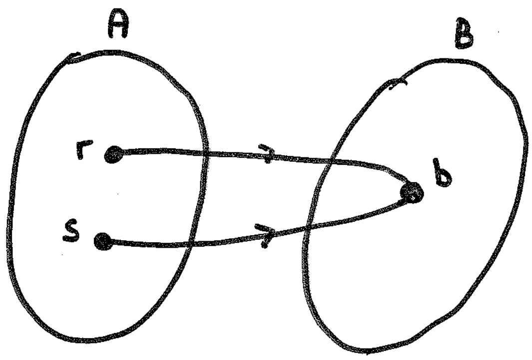
We next give some properties that some functions have while other functions don't.

Let A and B be two sets and let $f: A \to B$ be a function.

'Definition' [One-to-one]

If the images under f are all different, then the function is said to be one-to-one (or 1-1 or injective).
(In Swedish it is said to be enentydig or injektiv)

Pictorially it means that no two different elements of A map to the same element of B. That is,
THIS PICTURE IS NOT A PICTURE OF AN INJECTIVE FUNCTION:



Formal definition of one-to-one

A function $f: A \to B$ is one-to-one if
for all $r, s \in A$, IF $f(r) = f(s)$ THEN $r = s$

Contrapositive statement of this definition

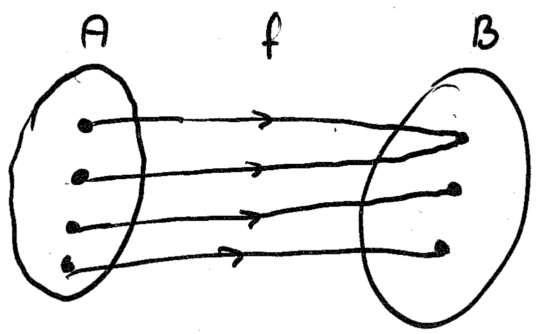
$f: A \to B$ is one-to-one if
for all $r, s \in A$, IF $r \neq s$ THEN $f(r) \neq f(s)$

Onto

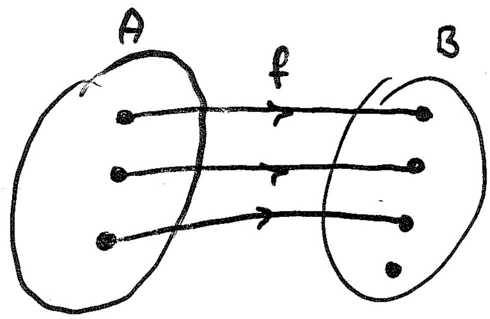
A function $f: A \to B$ is called onto (på) (or surjective (surjektiv)), if its codomain is the same as its range, that is if $B = f(A)$.

Formally

A function $f: A \to B$ is onto if for all $b \in B$ there is at least one $a \in A$ such that $f(a) = b$.



This function is onto, but not one-to-one.

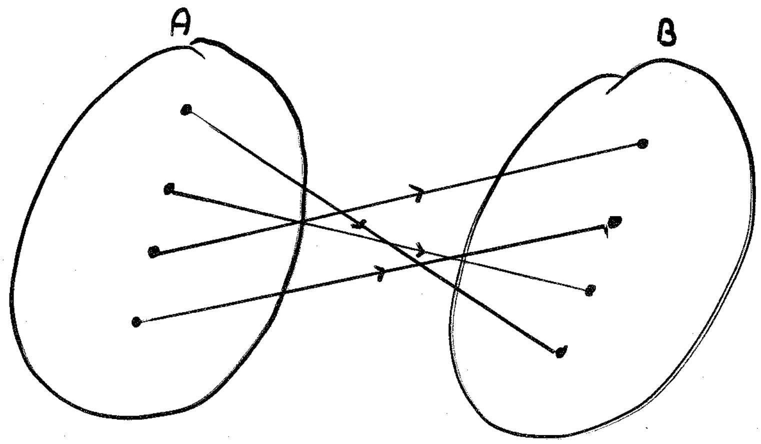


This function is one-to-one, but not onto

Bijection (or one-to-one correspondence)

A function which is both one-to-one and onto is called a bijection (or a one-to-one correspondence)
(bijektion)

Pictorially it looks:



That is, a bijection "pairs up" the elements of A and B.

EXAMPLES

Consider the following functions and decide whether they are injections (1-1), surjections (onto) or bijections.

- $f : \mathbb{N} \to \mathbb{N} \qquad f(x) = x^2$
- $g : \mathbb{Z} \to \mathbb{Z} \qquad g(x) = 2x+1$
- $h : \mathbb{R} \to \mathbb{R} \qquad h(x) = 2x+1$
- $k : \mathbb{Z} \to \mathbb{Z} \qquad k(x) = x+1$
- $\alpha : \mathbb{N} \to \mathbb{Z} \qquad \alpha(x) = \begin{cases} x & \text{if } x \text{ is odd} \\ -x & \text{if } x \text{ is even.} \end{cases}$
- $\beta : \{1,2,3,4\} \to \{a,b,c,d\}$

$$\beta(1) = c \quad \beta(2) = b \quad \beta(3) = a \quad \beta(4) = d$$

- $\gamma : \{1,2,3,4\} \to \{a,b,c\}$

$$\gamma(1) = b \quad \gamma(2) = c \quad \gamma(3) = a \quad \gamma(4) = c$$

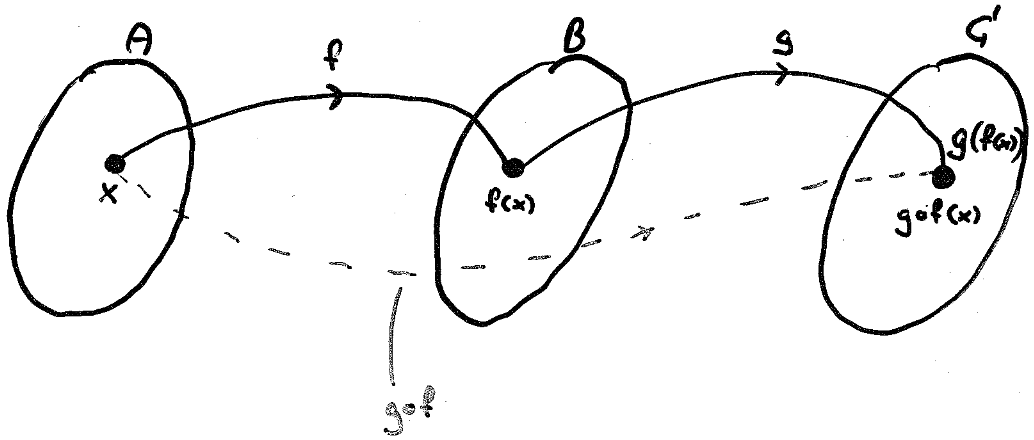
- $\delta : \{1,2,3\} \to \{a,b,c,d\}$

$$\delta(1) = b \quad \delta(2) = c \quad \delta(3) = a$$

Composition of functions

If we have two functions $f: A \to B$ and $g: B \to C$, we can define the composition $g \circ f: A \to C$ to be the function given by the rule that

$$g \circ f(x) := g(f(x)) \quad \text{for all } x \in A.$$



EXAMPLE

Let $f: \mathbb{Z} \to \mathbb{Z}$ be given by the rule $f(x) = x^2+1$.

Let $g: \mathbb{Z} \to \mathbb{Z}$ be given by the rule $g(x) = 3x+2$.

$$f \circ g(x) = f(g(x)) = f(3x+2) = (3x+2)^2+1 = 9x^2+12x+5$$

$$g \circ f(x) = g(f(x)) = g(x^2+1) = 3(x^2+1)+2 = 3x^2+5$$

Note that function composition is NOT commutative, that is, generally

$$f \circ g(x) \neq g \circ f(x).$$

THEOREM

Let $f: A \to B$ and $g: B \to C$ be two functions.

① If f and g are both one-to-one then $g \circ f$ is one-to-one.

② If f and g are both onto then $g \circ f$ is onto

③ If f and g are both bijections then $g \circ f$ is a bijection.

Inverse of functions

Intuitively a function is invertible, if when we are given **any** 'output' of the function in the codomain, we can determine a **unique** 'input' in the domain from where the 'output' came.

EXAMPLES

Let us consider the following functions to see if they are invertible.

- $f: \mathbb{N} \to \mathbb{N}$ $\quad f(x) = x+3$

- $g: \mathbb{Z} \to \mathbb{Z}$ $\quad g(x) = x+3$

- $h: \mathbb{Z} \to \mathbb{Z}$ $\quad h(x) = x^2$

- $\alpha: \{1,2,3,4\} \to \{a,b,c,d\}$
  $\alpha(1) = b$
  $\alpha(2) = a$
  $\alpha(3) = c$
  $\alpha(4) = d$

- $\beta: \{1,2,3,4\} \to \{a,b,c\}$
  $\beta(1) = b$
  $\beta(2) = a$
  $\beta(3) = c$
  $\beta(4) = b$

- $\gamma: \{1,2,3\} \to \{a,b,c,d\}$
  $\gamma(1) = b$
  $\gamma(2) = a$
  $\gamma(3) = c$

Formal definition of inverse function

Let $f: A \to B$ be a function.

If there exists a function $g: B \to A$ such that

for all $a \in A$ and $b \in B$ we have that

if $f(a) = b$ **then** $g(b) = a$,

Then we say that f is invertible with inverse g, and we write $g = f^{-1}$.

THEOREM

Let $f: A \to B$ be a function.

Then f is invertible if and only if f is a bijection.