Introduction

Throughout, we shall use the following notation for various collections of numbers:-

$\mathbb{N}$: The collection of all *natural numbers* $\mathbb{N}$ ={1,2,3,...}

$\mathbb{N}_0$: The collection of all *natural numbers* plus zero

$\mathbb{N}_0$ ={0,1,2,...}

$\mathbb{Z}$: The collection of all *integers* $\mathbb{Z}$ ={...,-3,-2,-1,0,1,2,...}

$\mathbb{Q}$: The collection of all *rationals*, which are numbers of the form $\frac{m}{n}$ where m is an integer and n is a *non-zero* integer. Any rational number can be simplified to a form such that m, n have no common factors > 1, and n is a natural number.

Examples

$$\frac{9}{12} = \frac{3}{4}$$

$$\frac{2}{-4} = \frac{-1}{2} = -\frac{1}{2}$$

So we can always write a rational such that $\text{HCF}(m, n) = 1$ and $n \geq 1$.

$\mathbb{R}$: The collection of all *real numbers*; we shall later show that there are far more of these than there are in $\mathbb{Q}$, even

though any real number can be approximated to arbitrary accuracy by a rational.

Example $\sqrt{3}$ is a real number that is not rational.

Proof Suppose that $\sqrt{3}$ is rational.

We know that $\sqrt{3} > 0$, so $\sqrt{3} = \frac{m}{n}$ where m, n are natural numbers and HCF$(m, n) = 1$

$$\therefore \quad m = \sqrt{3}n$$

$$\therefore \quad m^2 = 3n^2$$

$$\therefore \quad 3 \text{ is a factor of } m^2$$

$$\therefore \quad 3 \text{ is a factor of } m$$

$$\therefore \quad \text{there exists a natural number } k \text{ such that } m = 3k$$

$$\therefore \quad 9k^2 = 3n^2$$

$$\therefore \quad n^2 = 3k^2$$

$$\therefore \quad 3 \text{ is a factor of } n^2 \text{ and hence of } n.$$

This violates HCF $(m, n) = 1$ because we have shown that 3 is a factor of both m and n.

$$\therefore \quad \text{The supposition that} \sqrt{3} \text{ is rational is } \textit{false}.$$

$$\therefore \quad \sqrt{3} \text{ is irrational.}$$

In the above proof, we used a mixture of logic and calculation. The calculations were based on the rules of arithmetic. Such rules are called *axioms*.

The axioms of arithmetic

A set of axioms that enable us to calculate using integers are as follows.

Let $\mathbb{Z}$ denote the collection of all integers, and let

"$x \in \mathbb{Z}$" denote "x is an integer",

"$x, y \in \mathbb{Z}$" denote "x and y are integers", etc.

The axioms are:-

AM: There exist operations called *addition* and *multiplication* such that if $x, y \in \mathbb{Z}$ then $x + y \in \mathbb{Z}$ and $xy \in \mathbb{Z}$.

A1: Addition is *commutative*: if $x, y \in \mathbb{Z}$ then

$$x + y = y + x$$

A2: Addition is *associative*: if $x, y, z \in \mathbb{Z}$ then

$$x + (y + z) = (x + y) + z$$

A3: An *additive identity* exists: there exists an integer $0 \in \mathbb{Z}$ such that $0 + x = x + 0 = x$ for every $x \in \mathbb{Z}$.

A4: Each integer has an *additive inverse*: if $x \in \mathbb{Z}$ then there exists an integer $-x \in \mathbb{Z}$ such that

$$x + (-x) = -x + x = 0$$

M1: Multiplication is *commutative*: if $x, y \in \mathbb{Z}$ then

$$xy = yx$$

M2: Multiplication is *associative*: if $x, y, z \in \mathbb{Z}$ then

$$x(yz) = (xy)z$$

M3: A *multiplicative identity* exists: there exists an integer $1 \in \mathbb{Z}$ such that

$$1x = x1 = x \quad \text{for every } x \in \mathbb{Z}$$

D: Multiplication is distributive over addition: if $x, y, z \in \mathbb{Z}$ then

$$x(y + z) = xy + xz$$

NZ: if x, y are both *non-zero* intergers then so is xy.

Exercise Try to deduce each of the following properties of $\mathbb{Z}$ from the axioms of arithmetic.

C0: if $x \in \mathbb{Z}$ then $-(-x) = x$.

C1: $0y = 0$ for every $y \in \mathbb{Z}$.

C2: if $x, y \in \mathbb{Z}$ then $(-x)y = -(xy)$.

C3: if $x, y \in \mathbb{Z}$ then $(-x)(-y) = xy$.

C4: the additive identity is unique: if $x \in \mathbb{Z}$ satisfies

$$x + y = y \quad \text{for every } y \in \mathbb{Z} \quad \text{then } x = 0.$$

C5: additive inverses are unique: if $x, y \in \mathbb{Z}$ and $x + y = 0$ then $y = -x$.

C6: the multiplicative identity is unique: if $x \in \mathbb{Z}$ satisfies $xy = y$ for every $y \in \mathbb{Z}$ then $x = 1$.

Note Given these axioms, we can construct all of $\mathbb{Z}$ from the two elements $0, 1$ that we know belong to $\mathbb{Z}$.

For instance $2 = 1 + 1, \quad 3 = 1 + 2$, etc.

-1 is the additive inverse of 1

$-2 = (-1) + (-1), \quad -3 = (-1) + (-2), \quad$ etc.

Solutions

C0: If $x \in \mathbb{Z}$, then $-x \in \mathbb{Z}$, and so $-(-x) \in \mathbb{Z}$ (A4 twice)

$$\begin{aligned}
\therefore -(-x) &= 0 + (-(-x)) && \text{(A3)} \\
&= (x + (-x) + (-(-x)) && \text{(A4)} \\
&= x + ((-x) + (-(-x))) && \text{(A2)} \\
&= x + 0 && \text{(A4)} \\
&= x && \text{(A3)}
\end{aligned}$$

C1: Let $x, y \in \mathbb{Z}$. Then

$xy = (0 + x)y = 0y + xy$ (A3,D)

$$\begin{aligned}
\therefore 0 &= xy + (-(xy)) = (0y + xy) + (-(xy)) && \text{(A4)} \\
&= 0y + (xy + (-(xy))) && \text{(A2)} \\
&= 0y + 0 && \text{(A4)} \\
&= 0y && \text{(A3)} \\
\therefore 0y &= 0 \qquad \text{for every } y \in \mathbb{Z}
\end{aligned}$$

C2: Let $x, y \in \mathbb{Z}$. Then

$$\begin{aligned}
0 &= 0y \qquad \text{(C1)} \\
&= (x + (-x))y \quad \text{(A4)} \\
&= xy + (-x)y \quad \text{(D)} \qquad (*) \\
\therefore \quad (-x)y &= (-x)y + 0 = (-x)y + (xy + (-(xy)) \quad \text{(A3 \& A4)} \\
&= ((-x)y + xy) + (-(xy)) \quad \text{(A1)} \\
&= (xy + (-x)y) + (-(xy)) \quad \text{(A1)} \\
&= 0 + (-(xy)) = -(xy) \quad (* \text{ and A3})
\end{aligned}$$

C3: Let $x, y \in \mathbb{Z}$. Then

$$\begin{aligned}
(-x)(-y) &= -(x(-y)) \qquad \text{(C2)} \\
&= -((-y)x) \qquad \text{(M1)} \\
&= -(-(yx)) \qquad \text{(C2)} \\
&= yx \qquad \text{(C0)} \\
&= xy \qquad \text{(M1)}
\end{aligned}$$

C4: Suppose that $x + y = y$ for each $y \in \mathbb{Z}$. Let $y \in \mathbb{Z}$.

Then $\exists -y \in \mathbb{Z}$ such that $y + (-y) = -y + y = 0$ (A4)

$$\begin{aligned} \therefore \quad x &= x + 0 = x + (y + (-y)) \qquad \text{(A3)} \\ &= (x + y) + (-y) = y + (-y) \qquad \text{(A2)} \\ &= 0 \qquad \text{(A3)} \end{aligned}$$

C5: Suppose that $x + y = 0$.

$$\begin{aligned} \therefore \quad y + x &= 0 \qquad \text{(A1)} \\ \therefore \quad (y + x) + (-x) &= 0 + (-x) = -x \quad \text{(A4, A3)} \\ \therefore \quad y + (x + (-x)) &= -x \qquad \text{(A2)} \\ \therefore \quad y + 0 &= -x \qquad \text{(A4)} \\ \therefore \quad y &= -x \qquad \text{(A3)} \end{aligned}$$

C6: Let y be a *non-zero* integer. We know that $xy = y$.

$$\begin{aligned} \text{Then } 0 &= xy + (-(xy)) = y + (-x)y \quad \text{(C2)} \\ &= 1y + (-x)y \qquad \text{(M3)} \\ &= (1 + (-x))y \qquad \text{D} \end{aligned}$$

NZ implies that $1 + (-x) = 0$, because $y \neq 0$.

$$\therefore \quad (1 + (-x)) + x = 0 + x = x \qquad \text{(A3)}$$

$$\therefore \quad 1 + (-x + x) = x \qquad \text{(A2)}$$

$$\therefore \quad 1 + 0 = x \qquad \text{(A4)}$$

$$\therefore \quad 1 = x, \ i.e. \ x = 1 \qquad \text{(A3)}$$

The axioms for $\mathbb{Z}$ are also true for $\mathbb{Q}$ and $\mathbb{R}$, but they need additional axioms also - we will not go into these.
Given the axioms (rules), we use logic to deduce some conclusions. The results are usually stated as Theorems (Proposition/Lemmas/Corollaries also), which must be followed by a Proof that has no loopholes. Each step in the argument must follow on logically from a previous one. For this reason, we now study some simple ideas from logic.

Note: In a formal proof, *every* step must be shown - this is very boring. For this reason, elementary steps that are well-known can be omitted to shorten the proof. However, you should be able to fill in the gaps if necessary!

Formal Logic

Definition A *proposition* is a statement that is either true, or false, but not both.

Propositions may be denoted by capital letters, e.g.

Example $P : \sqrt{3}$ is irrational

Q: HCF $(m, n) = 1$

Definition The *negation* of a proposition P is written $\sim P$ and is said as "not P". It is formed from P by taking the opposite of P. In other words, it is the statement that is true when P is false, and false when P is true.

Example (cont.) For the statements P, Q in the previous example, we have the following negations:-

$$\sim P \ : \ \sqrt{3} \text{ is rational}$$

$$\sim Q \ : \ \text{HCF } (m, n) \neq 1$$

(or HCF $(m, n) > 1$, as we know that HCF (m, n) is always a natural number.)

Note By definition, if P is any proposition then

$$\sim (\sim P) = P$$

In our proof that $\sqrt{3}$ is irrational, we started by supposing the opposite, which led us to a contradiction because we showed that both HCF $(m, n) = 1$ and HCF $(m, n) \neq 1$. In symbolic notation, with P, Q as in the above two examples, we took the following logical steps:-

Aim: to prove P (is true)

Method: suppose $\sim P$; then $\sqrt{3} = \frac{m}{n}$ and Q (is true). After some calculations, we found that $\sim Q$.

Conclusion: if $\sim P$ then both Q and $\sim Q$. This is a logical inconsistency, so P (is true).

Note: We will not usually write (is true) - this is assumed.

The above method of proof is called *proof by contradiction.* Here it is in general:-

To prove P:

Assume $\sim P$. If this means that there is a proposition Q such that Q and $\sim Q$ hold, the assumption is wrong, so P is true.

Example Prove that the proposition P: $x^2 - y^2 = 1$ has no solutions with $x, y \in \mathbb{N}$.

Proof Suppose $\sim P$, i.e. $x^2 - y^2 = (x + y)(x - y) = 1$ has

at least one solution such that $x, y \in \mathbb{N}$

As x, y are natural numbers, $x + y \in \mathbb{N}$ and $x - y \in \mathbb{Z}$.

Moreover as $(x + y)(x - y) = 1$ which is positive, it follows that $x - y \in \mathbb{N}$.

$$\therefore \quad x + y = 1 \quad \text{and } x - y = 1$$

$$\therefore \quad x = 1 \quad \text{and } y = 0.$$

But this contradicts the statement $y \in \mathbb{N}$.

Hence the supposition $\sim P$ is incorrect. Hence P is true.

Exercise i) Prove that $2^{\frac{1}{3}}$ is irrational.

Definition A natural number $p > 1$ is *prime* if it cannot be divided by any natural number other than p and 1.

Exercise ii) Prove that there are infinitely many prime numbers.

[Hint: If there are only finitely many, find a natural number that cannot be divided by any of them.]

Solutions i) Suppose $2^{\frac{1}{3}}$ is rational, i.e. $2^{\frac{1}{3}} = \frac{m}{n}$ where HCF $(m, n) = 1$ and $m, n \in \mathbb{N}$. Then

$$m^3 = 2n^3 \quad \therefore \quad m \text{ is divisible by 2, i.e. } m = 2k$$

$$\therefore 4k^3 = n^3 \quad \therefore \quad n \text{ is divisible by 2, so HCF}(m, n) \neq 1$$

This is a contradiction, so $2^{\frac{1}{3}}$ is irrational.

ii) Suppose that there are finitely many primes,

$p_1 < p_2 < ... < p_n$, (so $p_1 = 2$, $p_2 = 3$, etc). All other numbers > 1 must be divisible by one of these.

Let $N = p_1 p_2 ... p_n + 1$

Then N is larger than p_n and is not divisible by any of $p_1 ... p_n$.

This is a contradiction, so there are infinitely many primes.

Note This proof does *not* mean that every number of the form $p_1 p_2 ... p_n + 1$ is a prime, even though the first few are. For instance, $2 + 1 = 3,\ 2 \times 3 + 1 = 7,\ 2 \times 3 \times 5 + 1 = 31,$ are primes, but

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$$

is not.

Further examples

1. Proof that there are no rational solutions of $x^3 + x + 1 = 0$:-

Suppose that such a solution exists, i.e. $x = \frac{m}{n}$ where HCF $(m, n) = 1$

$$\therefore \quad \frac{m^3}{n^3} + \frac{m}{n} + 1 = 0$$

$$\therefore \quad m^3 + mn^2 + n^3 = 0$$

If m, n are both odd, LHS is the sum of 3 odd numbers and is odd.

If m is even, n is odd, LHS is the sum of 1 odd and 2 evens and is odd.

If m is odd, n is even, LHS is the sum of 1 odd and 2 evens and is odd.

So the only way for the LHS to be even (like 0) is if m and n are even. Then 2 divides both m, n so HCF $(m, n) \neq 1$. This is a contradiction. So the result holds.

2. Proof that if a is irrational and b is rational then $a + b$ is irrational.

Let a be irrational and $b = \frac{m_1}{n_1}$, where HCF $(m_1, n_1) = 1$, $m_1 \in \mathbb{Z}, \quad n_1 \in \mathbb{N}$.

Suppose that $a + b$ is rational. Then there exists $m_2 \in \mathbb{Z}, \quad n_2 \in \mathbb{N}$ such that

$$a + b = \frac{m_2}{n_2} \quad \text{and HCF } (m_2, n_2) = 1.$$

$$\therefore \quad a = \frac{m_2}{n_2} - \frac{m_1}{n_1} = \frac{m_2 n_1 - m_1 n_2}{n_1 n_2}$$

So a is rational, because $n_1 n_2 \in \mathbb{N}$ and $m_2 n_1 - m_1 n_2 \in \mathbb{Z}$.

Any common factors can be removed, as follows

Let $d =$ HCF $(m_2n_1 - m_1n_2, \quad n_1n_2)$

Then let $m_3 = \frac{(m_2n_1 - m_1n_2)}{d}, \quad n_3 = \frac{n_1n_2}{d}$.

$\therefore a = \frac{m_3}{n_3}$ where $m_3 \in \mathbb{Z}, \quad n_3 \in \mathbb{N}$ and HCF $(m_3, n_3) = 1$

So a is rational. This contradicts the fact that a is irrational, so the supposition that $a + b$ is rational is wrong.

3. Proof that the sum of cubes of two consecutive integers cannot be the cube of the next integer.

Suppose that $(n-1)^3 + n^3 = (n+1)^3$ for some $n \in \mathbb{Z}$

Then $n^3 - 6n^2 - 2 = 0 \quad \therefore \; n^2(n-6) = 2$

For $n = 0$, the LHS is zero, so this is not a solution.

For $n \neq 0, \quad n^2 > 0$, so the only possible solutions must have $n > 6$.

But the only (natural) factors of 2 are 1 and 2, of which only 1 is square. Hence $n^2 = 1$ and $n - 6 = 2$.

This is a contradiction, so the original supposition was wrong.

Formal Logic - Binary Operators

Negation acts on a single proposition - it is a *unary* operator.

By contrast, *binary operators* involve two propositions.

Here is a list of the main binary operators in formal logic.

$\Rightarrow$ "implies"

$P \Rightarrow Q$ means "if P is true then Q is true", ie. "P implies Q".

Note that no conclusion can be drawn about Q if P is not true.

However, if Q is false then P cannot be true.

Hence $P \Rightarrow Q$ is logically equivalent to $\sim Q \Rightarrow \sim P$,

which is called the *contrapositive* of $P \Rightarrow Q$.

Warning: $P \Rightarrow Q$ and $Q \Rightarrow P$ are two quite different statements - don't muddle them up! ($Q \Rightarrow P$ is the *converse* of $P \Rightarrow Q$.)

$\Leftrightarrow$ **" if and only if"** (written"iff" sometimes)

$P \Leftrightarrow Q$ means "$P \Rightarrow Q$ and $Q \Rightarrow P$" so it could also be written $Q \Leftrightarrow P$. In other words P is true exactly when Q is true. The logically-equivalent contrapositive of this statement is $\sim P \Leftrightarrow \sim Q$.

Logicians also use $P \equiv Q$ ("P is logically equivalent to Q") to mean $P \Leftrightarrow Q$; we shall use this interchangeably with $P \Leftrightarrow Q$.

$\wedge$ **"and"**

$P \wedge Q$ means "P *and* Q are both true".

$\vee$ **"inclusive or"**

$P \vee Q$ means "at least one of P and Q are true" so P is true *or* Q is true *or* both are true.

$\triangle$ **"exclusive or"**

$P \triangle Q$ means " exactly one of P and Q is true" so P is true *or* Q is true, but not both.

Except for $\Rightarrow$, all of the logical operators above are *symmetric*, i.e. the order of the P, Q does not matter.

Truth Tables

The proposition $P \wedge Q$ is true if both P and Q are true, and is false otherwise. In the same way, each binary operator forms a proposition whose truth is determined by the truth of P and Q.

This leads to a rigorous method of calculating the truth of propositions, using a *truth table*. We restrict attention to the simplest case, in which propositions involve P and Q only.

Let 1 denote "true" and let 0 denote "false".

Then the truth tables for $P \wedge Q$, $P \vee Q$, and $P \triangle Q$ are

P	$\wedge$	Q	P	$\vee$	Q	P	$\triangle$	Q
1	**1**	1	1	**1**	1	1	**0**	1
1	**0**	0	1	**1**	0	1	**1**	0
0	**0**	1	0	**1**	1	0	**1**	1
0	**0**	0	0	**0**	0	0	**0**	0

Bold type = Step 1

The method of construction is to write 1,1,0,0 and 1,0,1,0 in any column containing P and Q respectively, so that each

row gives one of the possible permutations of the truth values of P, Q. Under each operator, write the truth value of the statement that it creates.

This method extends to more complicated statements, eg.

$(\sim P) \wedge Q$				$\sim (P \wedge Q)$				$P \wedge (\sim Q)$			
0	1	*0*	1	*0*	1	**1**	1	1	*0*	0	1
0	1	*0*	0	*1*	1	**0**	0	1	*1*	**1**	0
1	0	*1*	1	*1*	0	**0**	1	0	*0*	**0**	1
1	0	*0*	0	*1*	0	**0**	0	0	*0*	**1**	0

and

$(\sim P) \vee (\sim Q)$				
0	1	*0*	**0**	1
0	1	*1*	**1**	0
1	0	*1*	**0**	1
1	0	*1*	**1**	0

Bold type = Step 1 Italic type = Step 2

Note that the order matters.

The 2^{nd} and 4^{th} tables prove that $\sim (P \wedge Q)$ and $(\sim P) \vee (\sim Q)$ are logically equivalent, i.e.

$\sim (P \wedge Q) = (\sim P) \vee (\sim Q)$

Exercise de Morgan's laws are

$$\text{i)} \sim (P \wedge Q) \equiv (\sim P) \vee (\sim Q)$$

$$\text{ii)} \sim (P \vee Q) \equiv (\sim P) \wedge (\sim Q)$$

We have proved i); use a truth table to prove ii).

Solution

$\sim$	$(P$	$\vee$	$Q)$		$(\sim$	$P)$	$\wedge$	$(\sim$	$Q)$
0	1	**1**	1		**0**	1	*0*	**0**	1
0	1	**1**	0		**0**	1	*0*	**1**	0
0	0	**1**	1		**1**	0	*0*	**0**	1
1	0	**0**	0		**1**	0	*1*	**1**	0

So far, we have not written down the truth tables for $\Rightarrow$ and $\Leftrightarrow$.

$P \Rightarrow Q$ means "if P is true then Q is true", so its truth table looks like this:-

P	$\Rightarrow$	Q
1	**1**	1
1	**0**	0
0	**a**	1
0	**b**	0

Here $\mathbf{a}, \mathbf{b}$ are each either 0 or 1. The trouble is that we

do not know what happens if P is false.

However, the contrapositive $\sim Q \Rightarrow \sim P$ tells that if Q is false, so is P; hence $b = 1$. Let us now compare the tables for $P \Rightarrow Q$ and $Q \Rightarrow P$

P	$\Rightarrow$	Q		Q	$\Rightarrow$	P
1	**1**	1		1	**1**	1
1	**0**	0		0	**a**	1
0	**a**	1		1	**0**	0
0	**1**	0		0	**1**	0

If $\mathbf{a} = 0$, the tables for $P \Rightarrow Q$ and $Q \Rightarrow P$ are the same, so they would be logically equivalent. We know that this is untrue, e.g.

P : Joe is a cat

Q : Joe is a mammal

$P \Rightarrow Q$, but Q does not imply P (there are mammals that are not cats).

Therefore $\mathbf{a} = 1$. So the truth table for $P \Rightarrow Q$ is

P	$\Rightarrow$	Q
1	**1**	1
1	**0**	0
0	**1**	1
0	**1**	0

So $P \Rightarrow Q$ is true if P is false, which seems strange!

The truth table for $P \Leftrightarrow Q$ is obtained from the definition $P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P)$

$(P$	$\Rightarrow$	$Q)$	$\wedge$	$(Q$	$\Rightarrow$	$P)$	shortens to	P	$\Leftrightarrow$	Q
1	**1**	1	*1*	1	**1**	1		1	**1**	1
1	**0**	0	*0*	0	**1**	1		1	**0**	0
0	**1**	1	*0*	1	**0**	0		0	**0**	1
0	**1**	0	*1*	0	**1**	0		0	**1**	0

Exercise Define the operator $\square$ by

P	$\square$	Q
1	**0**	1
1	**1**	0
0	**1**	1
0	**1**	0

i) Show that $P \square P \equiv \sim P$

ii) Express $P \wedge Q$ and $P \vee Q$ in terms of $\square$

iii) Express $\triangle, \Rightarrow$ and $\Leftrightarrow$ in terms of $\sim, \wedge, \vee$.

This exercise shows that each of our binary operators can be written in terms of $\square$. In fact, all 16 possible truth tables can be obtained from $\square$.

Solution

i) Only two rows are needed

P	$\square$	P		$\sim$	P
1	**0**	1		**0**	1
0	**1**	0		**1**	0

$\therefore P \square P \equiv \sim P$

ii)

$$P \wedge Q \equiv \sim (P \,\square\, Q) \equiv (P \,\square\, Q) \,\square\, (P \,\square\, Q)$$

$$P \vee Q \equiv (\sim P) \,\square\, (\sim Q) \equiv (P \,\square\, P) \,\square\, (Q \,\square\, Q)$$

iii)

$$P \triangle Q \equiv (\sim (P \wedge Q)) \wedge (P \vee Q)$$

$$P \Rightarrow Q \equiv (P \wedge Q) \vee (\sim P)$$

$$P \Leftrightarrow Q \equiv (P \wedge Q) \vee (\sim (P \vee Q))$$

Laws of Inference

During a mathematical proof, we use logic to infer each statement from a previous one. In other words, we are using *implication* repeatedly. Here are some common methods of inference:-

a) $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ If P is true and P implies Q, then Q is true

b) $(\sim Q \wedge (P \Rightarrow Q)) \Rightarrow \sim P$ If Q is false and P implies Q, then P is false

c) $(P \Rightarrow (Q \wedge \sim Q)) \Rightarrow \sim P$ If P implies both Q and not Q, then P is false - this is the idea behind Proof by Contradiction.

d) $(\sim Q \Rightarrow \sim P) \Rightarrow (P \Rightarrow Q)$ If not Q implies not P, then P implies Q.

This last statement gives rise to a method of proof called *Proof by Contraposition:-*

To prove that P implies Q, show that whenever Q is false, so is P.

Examples

1.**Theorem** Let $a, b \in \mathbb{R}$. If ab is irrational then at least one of a, b is irrational.

As propositions, we have

$$P \ : \ ab \text{ is irrational}$$

$$Q \ : \ \text{ at least one of } a, b \text{ is irrational}$$

Proof We want to prove that $P \Rightarrow Q$. To do this, show that $\sim Q \Rightarrow \sim P$. Suppose that neither a nor b is irrational. (This is $\sim Q$). Then there exist integers $m_1, m_2 \in \mathbb{Z}$ and $n_1, n_2 \in \mathbb{N}$ such that $a = \frac{m_1}{n_1}, \quad b = \frac{m_2}{n_2}, \quad \text{HCF } (m_i, n_i) = 1, i = 1, 2$

$$\therefore \quad ab = \frac{m_1 m_2}{n_1 n_2}$$

Let $d = \text{HCF}(m_1 m_2, n_1 n_2)$ and let $m_3 = \frac{m_1 m_2}{d}, \quad n_3 = \frac{n_1 n_2}{d}$

$$\therefore ab = \frac{m_3}{n_3} \text{ where } m_3 \in \mathbb{Z}, \quad n_3 \in \mathbb{N}, \quad \text{HCF}(m_3, n_3) = 1$$

$\therefore ab$ is rational, ie. $\sim P$.

So $\sim Q \Rightarrow \sim P$, and therefore $P \Rightarrow Q$.

2.**Theorem** Let $n \in \mathbb{N}$ and $n > 1$. If n is not divisible by any $d \in \mathbb{N}$ such that $2 \leq d \leq \sqrt{n}$, then n is prime.

[*Note*: n is *divisible* by d iff $\frac{n}{d} \in \mathbb{N}$].

Proof Statements:

P: n is not divisible by any $d \in \mathbb{N}$ s.t. $2 \leq d \leq \sqrt{n}$,

Q: n is prime.

Suppose $\sim Q$, ie. n is not prime. Then n has a divisor a that is neither 1 nor n.

Then $n = ab$ where b is neither n nor 1.

If $a \leq b$ then $a^2 \leq ab = n$, and so $2 \leq a \leq \sqrt{n}$

If $a > b$ then $b^2 < ab = n$, so $2 \leq b < \sqrt{n}$

In either case, we have a divisor between 2 and $\sqrt{n}$, so $\sim P$. Therefore $P \Rightarrow Q$.

Although the names are similar, proof by contraposition is quite different from proof by contradiction. The statement $P \Rightarrow Q$ can sometimes be proved by either means.

Contraposition: Suppose $\sim Q$, and prove that this implies $\sim P$

Contradiction: Suppose P is true but Q is not; try to find a conclusion that is a logical inconsistency (a statement R such that R and $\sim R$). It is not always clear how to do this.

Formal Logic - Quantifiers

In many instances, we want to prove that a proposition that involves a variable, x, is true for *every* value of x. Write the proposition as $P(x)$, so we want to show that
$\forall x, P(x)$. Here $\forall$ means "for all".
The negation of this statement is

$$\sim (\forall x, P(x)) \equiv \ \exists\, x \text{ s.t. } \sim P(x)$$

"There exists x such that (s.t.) not P(x)".
Similarly, the negation of $\exists\, x$ s.t. $P(x)$ is

$$\sim (\exists\, x \text{ s.t. } P(x)) \equiv \forall x, (\sim P(x)).$$

Example

Let $x \in \mathbb{N}$. Then if $P(x)$ is the statement $\sum_{k=1}^{x} k = \frac{1}{2}x(x+1)$ the statement $\forall x, P(x)$ is true.
Note that we had to say in advance that $x \in \mathbb{N}$; the sum would not be defined otherwise.
To avoid this difficulty, we usually state any restrictions on the variable, e.g.

$$\forall x \in \mathbb{N}, \quad \sum_{k=1}^{x} k = \frac{1}{2}x(x+1).$$

The negated statement (which is false) is

$$\exists\ x \in \mathbb{N} \text{ s.t. } \sum_{k=1}^{n} k \neq \frac{1}{2}x(x+1).$$

The same idea can be extended to more variables. Be careful - order often matters.

Example

$P(m,n) : \forall m \in \mathbb{N},\ \exists n \in \mathbb{N}$ s.t. $n > m$ is true (every m has a bigger number n).

However $Q(m,n) : \exists n \in \mathbb{N}$ s.t., $\forall m \in \mathbb{N}, \quad n > m$, is false (there is no number n that is bigger than every number m).

The negation $\sim Q(m,n) : \forall n \in \mathbb{N}\ \exists n \in \mathbb{N}$ s.t. $n \leq m$, is true (each number n has a number m that is at least as big).

Note that $P(m,n)$ and $\sim Q(m,n)$ are slightly different true statements.

Note Where no confusion can arise, it is common practice to write $\forall$ after a statement, eg.

$$\sum_{k=1}^{x} k = \frac{1}{2}x(x+1), \quad \forall x \in \mathbb{N}.$$

To prove this type of statement it is a good idea to begin with the words "Let $x \in \mathbb{N}$". This establishes that you have picked an arbitrary value for x; anything that you prove for that x is

proved for *every* x, because no restrictions have been placed on x.

Sets

Rough Definition A *set* A is a collection of *elements* (in no particular order) that can be regarded as a single object.

One way to define a set is to list all of its elements between curly braces, e.g.

$$A = \{a, b\}.$$

Note that each element is listed only once. Order does not matter - we could equally well have written $A = \{b, a\}$.

Definition The *empty set*, denoted $\emptyset$ (Norwegian letter oe - like "dirt") is the set that contains no elements $\emptyset = \{\}$.

Definition Given a set A, a set B is a *subset* of A if evey element of B is an element of A. We write $B \subset A$.

Using $x \in A$ to denote "x is an element of A",

$$B \subset A \quad \text{iff} \quad x \in A, \quad \forall x \in B.$$

Example The set $A = \{a, b\}$ has four distinct subsets; $\emptyset, \{a\}, \{b\}, A$.

Exercise Write out all subsets of $A = \{1, 2, 3\}$.

Definition A set is *finite* if it contains a finite number of elements. Otherewise it is an *infinite set* .

Definition The *cardinality* of a set A, is denoted $|A|$, is

$$\begin{cases} \text{the number of elements that it contains,} & \text{if A is finite;} \\ \text{a measure of the size of A,} & \text{if A is infinite.} \end{cases}$$

For example, if $A = \{a, b\}$ then $|A| = 2$.

Examples So far we have only met finite sets. However the set of all natural numbers, $\mathbb{N} = \{1, 2, 3, ...\}$, is infinite. So are the sets $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$.

Definition The *cardinality* of $\mathbb{N}$ is $|\mathbb{N}| = \aleph_0$ (aleph - null). Any set whose cardinality is $\leq \aleph_0$ is said to be *countable*. We shall show that $\mathbb{Z}$ and $\mathbb{Q}$ are countable, whereas $\mathbb{R}$ is *uncountable*.

Note It can be proved that any set A s.t. $|A| < \aleph_0$ is finite. Sets A s.t. $|A| = \aleph_0$ are said to be *countably infinite*.

Another way to define a set is as a subset that contains all elements that have a particular property. The form is { type of element: property } where the colon : means "such that".

Examples

$$A = \{x \in \mathbb{Z} : \frac{x}{2} \in \mathbb{Z}\} = \text{set of all even integers}$$

$$B = \left\{\text{triangle } PQR : \left|\vec{PQ}\right| = \left|\vec{QR}\right| = \left|\vec{PR}\right|\right\}$$

$$= \text{set of all equilateral triangles.}$$

$$C = \{x \in \mathbb{R} : x > 0\} = \text{set of all positive real numbers}$$

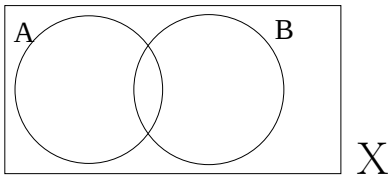
$$D = \{\text{anteater: species name (in English) begins with “aa”}\}$$

$$= \text{set of all aardvarks.}$$

Operators on sets

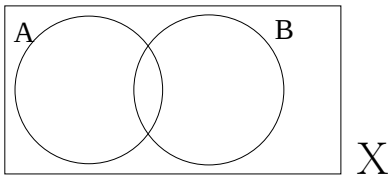
Just as we can define unary and binary operators on propositions, we can do something similar for sets.

In the following, let $A, B \subset X$. In general, A and B might overlap, so a pictorial representation of the sets A, B, X is a *Venn diagram*:-

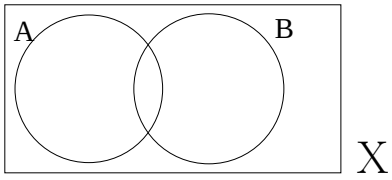


Subsets of X that are obtained by using operators will be shaded, as the following examples show:-

$\mathbf{A \cup B}$ "A *union* B" is the set of all elements that are in at least one of A and B:-



$\mathbf{A \cap B}$ "A *intersection* B" is the set of all elements that are in both A and B:-



Note that

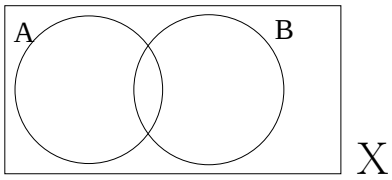
$$A \cup B = \{x \in X : \quad (x \in A) \vee (x \in B)\}$$

$$A \cap B = \{x \in X : \quad (x \in A) \wedge (x \in B)\}$$

Also $A \cap A = A$ and $A \cup A = A$.

In the same way, other operators can be expressed in terms of the propositions $P : x \in A, \quad Q : x \in B$.

$\mathbf{A^c}$ "the *complement* of A" is the set of all elements of X that are *not* in A

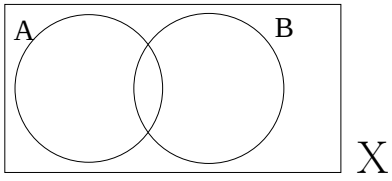


$$A^c = \{x \in X : \quad \sim (x \in A)\}$$

We use $x \notin A$ as a shorthand for $\sim (x \in A)$,

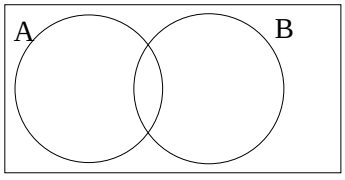
so $A^c = \{x \in X : \ x \notin A\}$.

$\mathbf{B \backslash A}$ "the *set difference*" all things in B but not A



$$\begin{aligned} B\backslash A &= \{x \in X : \quad (x \in B) \wedge (\sim (x \in A))\} \\ &= \{x \in X : \quad (x \in B) \wedge (x \notin A)\} \end{aligned}$$

A$\triangle$B "*the symmetric set difference*" all things in A *or* B but *not both*.

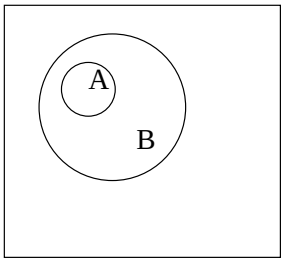


$$A \triangle B = \{x \in X : \quad (x \in A) \triangle (x \in B)\}$$

So, far we have not drawn analogues of $\Rightarrow$ and $\Leftrightarrow$. We need to modify the Venn diagram slightly, as follows.

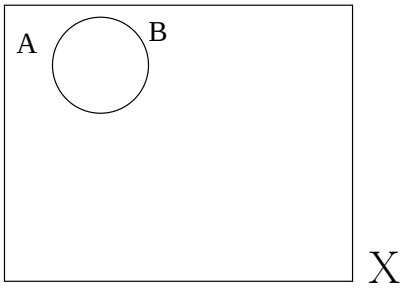
A $\subset$ B If $x \in A$ then $x \in B$ - i.e. A is a subset of B corresponds to $(x \in A) \Rightarrow (x \in B)$.

Note the contrapositive:- if $x \notin B$ then $x \notin A$



$\mathbf{A = B}$ The subsets A and B are identical,

i.e. $(x \in A) \Leftrightarrow (x \in B)$.



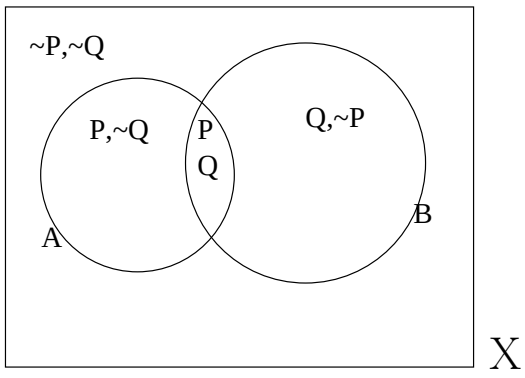
The analogy between operators on sets A, B and on the propositions

$$P \ : \ x \in A$$

$$Q \ : \ x \in B$$

means that we can prove theorems about sets using either truth tables or Venn diagrams.

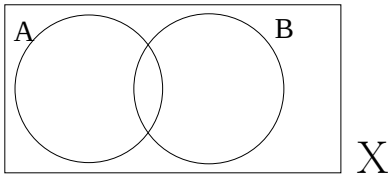
The regions of the Venn diagram are as follows:-



The **de Morgan laws** for sets are

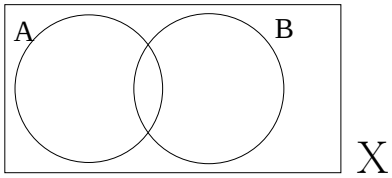
$$\text{i)} \quad (A \cup B)^c \;=\; A^c \cap B^c$$

$$\sim (P \vee Q) \;=\; (\sim P) \wedge (\sim Q)$$

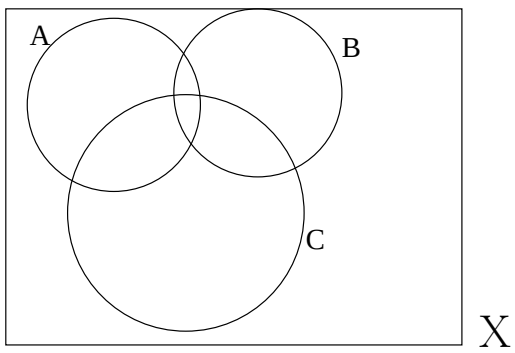


$$\text{ii)} \quad (A \cap B)^c \;=\; A^c \cup B^c$$

$$\text{c.f.} \quad \sim (P \wedge Q) \;=\; (\sim P) \vee (\sim Q)$$



Venn diagrams can easily be extended to 3 sets $A, B, C \subset X$ as follows:-



There are eight regions, corresponding to the eight possible permutations of the truth values for

$$P \ : \ x \in A$$

$$Q \ : \ x \in B$$

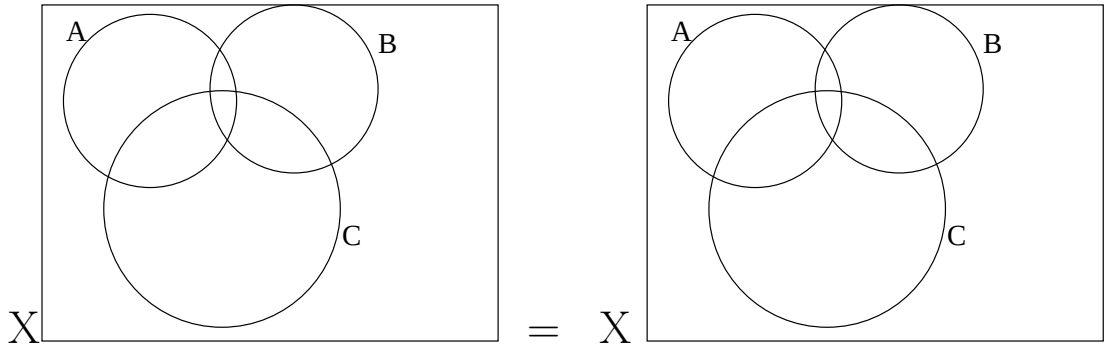
$$R \ : \ x \in C$$

There are two *distributive laws* for union and intersection:

$$\text{a)} \quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$\text{b)} \quad A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

We prove a) using a Venn diagram as follows:-



$$||| = B \cup C \qquad \equiv= A \cap B$$

$$\equiv= A \cap (B \cup C) \qquad ||| = A \cap C$$

Exercises i) Prove distributive law b) using a Venn diagram ii) Which two of the following are identical? (use Venn diagrams)

$$(A^c \cup B) \cap (A \cup B^c)$$

$$(A \backslash B) \cup (B \backslash A)$$

$$(A^c \cup B^c)^c$$

$$(A \cup B) \backslash (A \cap B)$$

Prove your result using truth tables.

iii) Prove that $A = (A \backslash B) \cup (A \cap B)$.

Definition Two sets A, B are *disjoint* if $A \cap B = \emptyset$.

Theorem If A, B are disjoint *finite sets* then

$$|A \cup B| = |A| + |B|$$

Note This result needs some qualification if either of A, B is infinite.

Proof If $|A| = m, \quad |B| = n$, then we can write the elements of A, B as a_i, $i = 1, ...m \quad$ and b_j, $j = 1, ...n$

$$\therefore \quad A \cup B = \{\underbrace{a_1, a_2, ..., a_m}_{m \text{ elements of } A}, \quad \underbrace{b_1, b_2, ..., b_n}_{n \text{ elements of } B}\}.$$

(As A, B are disjoint, there is no duplication of elements). Hence $|A \cup B| = m + n = |A| + |B|$.

Exercise Let A, B be finite sets. Using the fact that $A = (A \backslash B) \cup (A \cap B)$, show that

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Hence show that if A, B, C are finite sets then

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| \\ &\quad + |A \cap B \cup C| \,. \end{aligned}$$

Solution Use the previous theorem:-

$$\begin{aligned} |A \cup B| &= |(A \backslash B) \cup B| = |A \backslash B| + |B| \\ |A| &= |(A \backslash B) \cup (A \cap B)| = |A \backslash B| + |A \cap B| \\ \therefore |A \cup B| &= |A| + |B| - |A \cap B| \\ \therefore \quad |A \cup B \cup C| &= |A| + |B \cup C| - |A \cap (B \cup C)| \\ &= |A| + |B| + |C| - |B \cap C| \\ &\quad - |(A \cap B) \cup (A \cap C)| \\ &= |A| + |B| + |C| - |B \cap C| \\ &\quad -(|A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)|) \\ &= |A| + |B| + |C| - |A \cap B| - |A \cap C| \\ &\quad - |B \cap C| + |A \cap B \cap C| \,. \end{aligned}$$

Another way to combine two sets A, B is to take their *Cartesian product* $A \times B$. This is the set consisting of all pairs (x, y) such that $x \in A$ and $y \in B$:-

$$A \times B = \{(x, y) : \quad x \in A,\ y \in B\}$$

E.g. if $A = \{a, b\}$ and $B = \{1, 2, 3\}$ then

$$\begin{aligned} A \times B &= \{(a,1),(a,2),(a,3),(b,1),(b,2),(b,3)\} \\ B \times A &= \{(1,a),(2,a),(3,a),(1,b),(2,b),(3,b)\} \end{aligned}$$

(Think of elements of $A \times B$ as vectors whose first component is an element of A, and whose second component is an element of B.)

Theorem If A, B are finite then $|A \times B| = |A|\ |B|$

Proof The elements of $A \times B$ are obtained by all permutations of the $|A|$ elements of A with the $|B|$ elements of B.

Note that we can still take unions and intersections, of individual components of $A \times B$. For instance:-

$$\begin{aligned} A \times (B \cup C) &= (A \times B) \cup (A \times C) \\ A \times (B \cap C) &= (A \times B) \cap (A \times C) \end{aligned}$$

The link between Cartesian products and vectors gives the

following familiar spaces:-

$$\text{The plane } \mathbb{R}^2 \;=\; \mathbb{R}\times\mathbb{R} = \{(x,y):\; x\in\mathbb{R},\; y\in\mathbb{R}\}$$

$$\text{3-D space } \mathbb{R}^3 \;=\; \mathbb{R}^2\times\mathbb{R} = \mathbb{R}\times\mathbb{R}\times\mathbb{R} = \{(x,y,z) : x,y,z\in\mathbb{R}\}$$

etc.

More generally $\mathbb{R}^n = \mathbb{R}^{n-1}\times\mathbb{R}$ is called n-dimensional *Euclidean space.*

Maps between sets

Definition Let A, B be sets. A *map* ϕ from A to B (written $\phi : A \to B$) assigns, to each $x \in A$, an element $\phi(x) \in B$.

Definition A *binary operation* is a map $\phi : A \times A \to A$ (e.g. addition, multiplication if $A = \mathbb{R}$)

Examples

a) $\phi : \mathbb{R} \to \mathbb{R}$ defined by $\phi(x) = x^2, \quad \forall x \in \mathbb{R}$

(functions are examples of maps)

b) $\phi : \mathbb{R} \to \mathbb{Z}$ defined by $\phi(x) = [x]$, $\forall x \in \mathbb{R}$

($[x] =$ greatest integer $\leq x$)

c) $\phi : \mathbb{N} \to \mathbb{N}$ defined by $\phi(x) = 2x$, $\forall x \in \mathbb{N}$

d) Let $X = \{1, 2, 3, \}, \quad Y = \{a, b, c\}$ and define

$$\phi : X \to Y \quad \text{by } \phi(1) = c, \quad \phi(1) = a, \quad \phi(3) = 6.$$

In general, a map $\phi : A \to B$ can map two different elements of A to the same element of B, so $\phi(x_1) = \phi(x_2)$ need not mean that $x_1 = x_2$. Moreover, not every $y \in B$ need be $\phi(x)$ for some $x \in A$.

Definition The map $\phi : A \to B$ is *injective* if

$$\phi(x_1) = \phi(x_2) \Rightarrow x_1 = x_2.$$

Injective maps are also called $1:1$ (one-to-one), because no more than *one* element of A can be mapped to any particular element of B. (Maps that are not injective are called *many-to-one*.)

In the examples a), b) are many-to-one whereas c), d), are injective.

Proof: a) $(-x)^2 = x^2, \ \forall x \in \mathbb{R}$;

b) $[x] = 0, \ \forall x \in [0,1]$

c) Let $x_1, x_2 \in \mathbb{N}$ be such that $\phi(x_1) = \phi(x_2)$

$\therefore \quad 2x_1 = 2x_2 \qquad \therefore \quad x_1 = x_2$

d) No two of $\phi(1), \ \phi(2), \ \phi(3)$ are identical.

Definition The map $\phi : A \to B$ is *surjective* if

$$y \in B \Rightarrow \exists\, x \in A \quad s.t. \quad y = \phi(x)$$

Surjective maps are also called *onto*, because the map's *image*

$$\phi(A) = \{\phi(x) : x \in A\}$$

is B (A is taken onto all of B).

In the above examples, only b), d) are surjective.

Proof: a) $\phi(\mathbb{R}) = \{x^2 : \ x \in \mathbb{R}\} = \{z \in \mathbb{R} : \ z \geq 0\} \neq \mathbb{R}$.

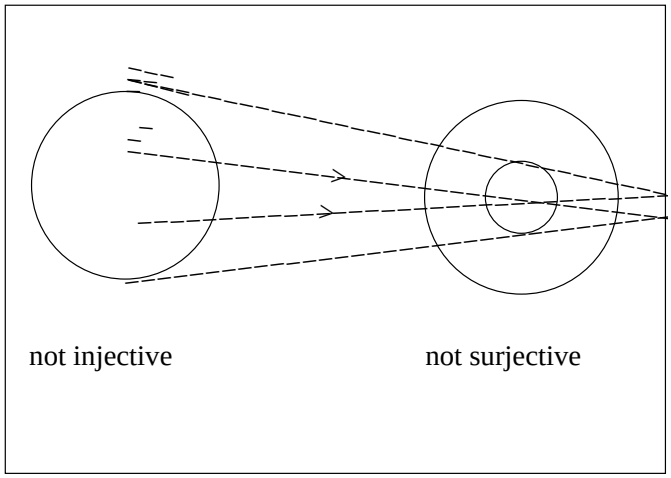
b) Let $y \in \mathbb{Z}$. Then $y \in \mathbb{R}$ and $\phi(y) = [y] = y$. So $\phi(\mathbb{R}) = \mathbb{Z}$.

c) $\phi(\mathbb{N}) = \{2x : \ x \in \mathbb{N}\} = \{m \in \mathbb{N} : \ m \text{ even}\} \neq \mathbb{N}$

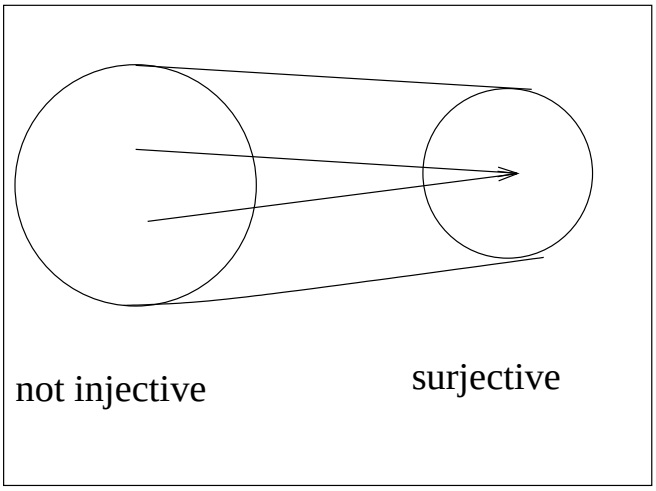
d) $\phi(X) = \{\phi(1), \ \phi(2), \ \phi(3)\} = \{c, a, b\} = \{a, b, c\} = Y$.

Pictorially:

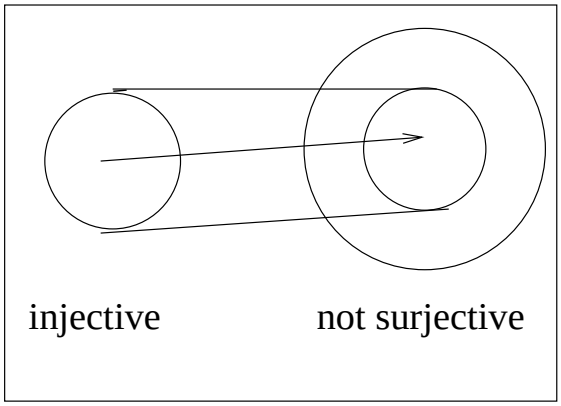
a) $\mathbb{R} \qquad \phi \rightarrow \qquad \mathbb{R}$



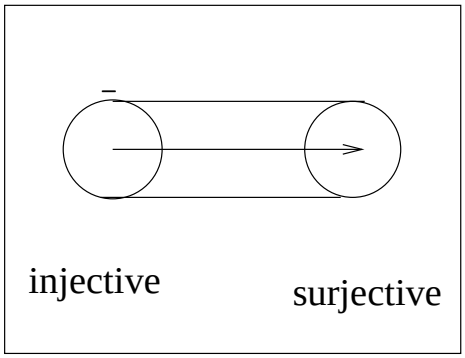
b) $\mathbb{R} \qquad \overrightarrow{\phi} \qquad \mathbb{Z}$


not injective
surjective

c) $\mathbb{N} \xrightarrow{\phi} \mathbb{N}$



d) $X \xrightarrow{\phi} Y$



Definition A *bijection* $\phi : A \to B$ is a map that is both injective and surjective.

In the above example, only d) was a bijection.

Theorem If $\phi : A \to B$ is a bijection then it is *invertible*; its *inverse*, $\phi^{-1} : B \to A$ is a bijection. Here $\phi^{-1}(\phi(x)) = x$.

Proof Let $x \in A$. Then $\phi(x) \in B$.

Furthermore, as ϕ is injective, there is no other element $z \in A, z \neq x$ such that $\phi(x) = \phi(z)$. So $\phi^{-1}(\phi(x)) = x$ (unambiguously).

Hence ϕ^{-1} is surjective.

Now suppose that $\phi^{-1}(y_1) = \phi^{-1}(y_2)$.

As ϕ is surjective, $\exists\, x_1, x_2 \in A$ s.t. $y_1 = \phi(x_1), y_2 = \phi(x_2)$.

$\therefore \phi^{-1}(\phi(x_1)) = \phi^{-1}(\phi(x_2))$, i.e. $x_1 = x_2 \ \therefore \phi(x_1) = \phi(x_2)$

$\therefore y_1 = y_2$

So ϕ^{-1} is injective.

Theorem if A, B are finite sets then any two of the following conditions imply that the third condition also holds:-

i) $\phi : A \to B$ is injective:

ii) $\phi : A \to B$ is surjective:

iii) $|A| = |B|$.

Proof

- Suppose that i), ii) hold. Then ϕ is a bijection, so ϕ and ϕ^{-1} are injective (one-to-one). Hence there are the same number of elements in A, B (because A, B are *finite*).

  $\therefore |A| = |B|$.

- Now suppose that i), iii) hold. Every element of A is mapped to a unique element of B, so
  $|\phi(A)| = |A| = |B|\,. \quad \therefore \phi(A) = B.$
  This can fail if $A < B$ are infinite - see example c) above.

- Now suppose that ii), iii) hold. Then for every $y \in B$ $\exists$ *at least one* $x \in A$ s.t. $y = \phi(x)$. Suppose that $\exists\, y \in B$ s.t. $\phi(x_1) = \phi(x_2) = y$ where $x_1 \neq x_2$ are elements of A. Then the number of elements in A is at least $|B| + 1$, i.e. $|A| \geq |B| + 1 > |B|$. This violates iii).
  Hence no such y exists, i.e. $\phi(x_1) = \phi(x_2) \Rightarrow x_1 = x_2$.
  This can also fail if A, B are infinite.

Exercise Prove that if $\phi : A \to B$ and $\psi : B \to C$ are bijections, so is $\psi \circ \phi : A \to C$ defined by
$\psi \circ \phi(x) = \psi(\phi(x)), \quad \forall x \in A.$
Solution Let $z \in C$. Then $\exists\, y \in B$ s.t. $z = \psi(y)$ (as ψ is surjective), and $\exists\, x \in A$ s.t. $y = \phi(x)$ (as ϕ is surjective). So $\exists\, x \in A$ s.t. $z = \psi(\phi(x)) = \psi \circ \phi(x)$
$\therefore \quad \psi \circ \phi$ is surjective.
Let $\psi \circ \phi(x_1) = \psi \circ \phi(x_2)$. Then $\psi(\phi(x_1)) = \psi(\phi(x_2))$.

$\therefore \quad \phi(x_1) = \phi(x_2)$ (as ψ is injective)

$\therefore \quad x_1 = x_2$ (as ϕ is injective).

So $\psi \circ \phi$ is injective. Hence $\psi \circ \phi$ is a bijection.

Cardinality of Infinite Sets

We are now in a position to define cardinality properly:-

Definition Two sets A, B have the same cardinality iff there exists a bijection $\phi : A \to B$; we then write $|A| = |B|$.

Note In the light of the previous theorem, the existence of a bijection between two *finite* sets implies that they have the same cardinality. The above definition extends this idea to infinite sets.

Examples 1. **Theorem** $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$

Proof Consider the following bijection $\phi : \mathbb{Z} \to \mathbb{N}$

$$\begin{aligned} x &: \quad ..., -3, -2, -1, 0, 1, 2, 3, ... \\ \phi(x) &: \quad ..., 7, 5, 3, 1, 2, 4, 6, ... \end{aligned}$$

Equivalently

$$\phi(x) = \begin{cases} 2x, & x \geq 1; \\ 1 - 2x, & x \leq 0 \end{cases}$$

It is easy to see that ϕ is a bijection; its inverse is

$$\phi^{-1}(y) = \begin{cases} \frac{y}{2}, & y \quad \text{even} : \\ \frac{1-y}{2}, & y \quad \text{odd}. \end{cases}$$

This example shows that if we are to write

$\mathbb{Z} = \{-x : x \in \mathbb{N}\} \cup \{0\} \cup \mathbb{N}$, we obtain

$$|\mathbb{Z}| = 1 + 2\,|\mathbb{N}|$$

so $\aleph_0$ " = "$1+2\aleph_0$, but $\aleph_0 \neq -1$: don't use ordinary arithmetic with non-finite cardinals!

2.**Theorem** $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$

Proof It is easiest to construct a bijection $\psi : \mathbb{Q} \to \mathbb{Z}$ and then to use the above theorem. Let $\psi(0) = 0$. If $q \in \mathbb{Q}$ is *positive* then $\exists m, n \in \mathbb{N}$ s.t. $q = \frac{m}{n}$, $\quad \text{HCF}(m, n) = 1$.

Write out all positive rationals on the following lattice

$$\begin{array}{lccccc}
n \uparrow & & & & & \\
 & \vdots & & & & \\
 & 4 & \cdot_9 & \times & \cdot & \times \\
 & 3 & \cdot_5 & \cdot_8 & \times & \cdot \\
 & 2 & \cdot_3 & \times & \cdot_7 & \times \\
 & 1 & \cdot_1 & \cdot_2 & \cdot_4 & \cdot_6 \\
 & & 1 & 2 & 3 & 4 \quad ... \quad \to m
\end{array}$$

Cross out those for which HCF $(m, n) \neq 1$, and number the others diagonally, as shown. Then each *positive* $q \in \mathbb{Q}$ is

numbered uniquely by N_q. Let $\psi(q) = N_q \quad \forall q > 0$. For $q < 0$, let $\psi(q) = -N_{|q|}$. By construction, ψ is a bijection.

We now turn our attention to $\mathbb{R}$. Note that every real number has a decimal expansion. However, the decimal expansion of a real number is not always unique.

Example $1 = 0 \cdot 99\overline{9}$ (The overbar indicates a recurring digit).

Proof $1 = 9 \times \frac{1}{9} = 9 \times (0 \cdot 11\overline{1}) = 0 \cdot 99\overline{9}$

However, this is essentially the only type of non-uniqueness. Provided that the decimal expansion does not end in an infinite sequence of nines, it is unique.

In the following, we shall always avoid this problem by disallowing any expansion that ends in an infinite sequence of nines. For instance, we would write $0 \cdot 743$, not $0 \cdot 74299\overline{9}$.

Theorem $\mathbb{R}$ is uncountable.

Proof We shall prove that the subset $[0, 1) \subset \mathbb{R}$ is uncountable.

Suppose that $[0, 1)$ is countable. Then there exists a sequence $S = \{x_n : n \in \mathbb{N}\}$ such that *every* element of $[0, 1)$ is a member of the sequence. Write the decimal expansion of each

member of the sequence as follows:-

$$\begin{aligned} x_1 &= 0 \cdot d_{11}d_{12}d_{13}d_{14}... \\ x_2 &= 0 \cdot d_{21}d_{22}d_{23}d_{24}... \\ x_3 &= 0 \cdot d_{31}d_{32}d_{33}d_{34}... \\ x_4 &= 0 \cdot d_{41}d_{42}d_{43}d_{44}... \\ &\vdots \\ x_n &= 0 \cdot d_{n1}d_{n2}d_{n3}d_{n4}... \\ &\vdots \end{aligned}$$

where each $d_{ij} \in \{0, 1..., 8, 9\}$ and infinite strings of nines are disallowed.

Now let $x = 0 \cdot c_1c_2c_3c_4...$ where each $c_i \in \{0, 1, 2, ..., 7, 8\}$ and $c_i \neq d_{ii}$. Note that $x \in [0, 1)$.

[Example: $c_i = d_{ii} - 1$ if $d_{ii} \neq 0$; $\quad c_i = 1$ if $d_{ii} = 0$]

Then x differs from each x_n in the n^{th} decimal place, so $x \notin S$. We have established a contradiction. So $[0, 1)$ is uncountable.

Note The argument used in the proof is called "Cantor's diagonal argument". Georg Cantor laid the foundations for the idea of cardinality.

The Power Set

Definition Given a set A, its *power set* $P(A)$ is the set whose elements are the subsets of A.

Examples i) $A = \{a, b\} \Rightarrow P(A) = \{\phi, \{a\}, \{b\}, A\}$

ii) $B = \{1, 2, 3\}$

$\Rightarrow P(A) = \{\{\phi\}, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, B\}$

Theorem If A is a finite set then $|P(A)| = 2^{|A|}$

Proof Write $A = \{a_1, ..., a_n\}$ where $|A| = n$.

The elements of $P(A)$ are subsets of A that are uniquely identified by an n-digit binary number, whose i^{th} digit is the truth value of the ststement "a_i belongs to this subset".

(For instance, in example i), write the elements of $P(A)$ as $c_{00} = \{\phi\}, c_{10} = \{a\}, c_{01} = \{b\}, c_{11} = \{a, b\} = A$; there is a bijection between the suffices ij and the elements of $P(A)$.)

Consequently there are 2^n possibilities for the binary number, each one corresponding to an element of $P(A)$. Hence $|P(A)| = 2^n = 2^{|A|}$.

Question How is $|P(A)|$ related to $|A|$ if A is infinite?

Theorem There is no bijection between A and $P(A)$. Moreover, $|P(A)| > |A|$.

Proof Consider a function $\phi : A \to P(A)$. Let $B \subset A$ be defined by $B = \{x \in A : \quad x \notin \phi(x)\}$ (recall that $\phi(x)$ is a set).

Suppose that ϕ is a bijection. Then, because $B \in P(A)$ and ϕ is surjective, $\exists\ x \in A$ s.t. $\phi(x) = B$. Therefore for this particular x, the statement

$x \in B \Leftrightarrow x \notin \phi(x)$ (which is true whether or not $x \in B$)

reduces to $x \in B \Leftrightarrow x \notin B$. This is a contradiction.

Hence no bijection ϕ exists.

Note that the above proof uses only surjectivity, so there is no surjection $\phi : A \to P(A)$. Hence $|P(A)| > |A|$.

Example In particular, $|P(\mathbb{N})| > |\mathbb{N}| = \aleph_0$, so $P(\mathbb{N})$ is uncountable. Similarly,$|P(\mathbb{Z})| > |\mathbb{Z}| = \aleph_0$, so $P(\mathbb{Z})$ is uncountable.

Theorem $|\mathbb{R}| = |P(\mathbb{N})| = 2^{|\mathbb{N}|}$.

The entire proof is beyond the scope of this couse.

However, we shall show that $|\mathbb{R}_0^+| = |P(\mathbb{N})|$, where

$|\mathbb{R}_0^+| = \{x \in \mathbb{R} : \ x \geq 0\}$, with the aid of *continued fractions*.

Continued Fractions

Let $r_0 \in \mathbb{R}$ and let $a_0 = [r_0]$. If $a_0 \neq r_0$ (i.e. r_0 is not an integer) then we can write

$$r_0 = a_0 + \frac{1}{r_1} \quad \text{where } r_1 > 1.$$

Let $[r_1] = a_1$. If r_1 is not an integer there exists $r_2 > 1$ s.t. $r_1 = a_1 + \frac{1}{r_2}$, so $r_0 = a_0 + \frac{1}{a_1 + \frac{1}{r_2}}$

By continuing this process, writing $a_i = [r_i]$ and $r_{i+1} = \frac{1}{r_i - a_i}$ if r_i is not an integer, we obtain a sequence of numbers $\{a_0, a_1, a_2, ...\}$. If r_n is an integer for some $n \in \mathbb{N}_0$ then a_n is the last member of the sequence and

$$r_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}$$

Note that $a_n \geq 2$ for otherwise r_{n-1} would be an integer.

For convenience, write this as $r_0 = [a_0, a_1, a_2, ..., a_n]$.

In all other cases, the sequence of $a_i's$ does not terminate and we write $r_0 = [a_0, a_1, a_2, ...]$. In either case, this is called the *continued fraction* representation of $r_0 \in \mathbb{R}$.

Note By construction, $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}$, $\forall i \geq 1$ for which a_i is defined.

To construct the continued fraction expansion of r_0, write

$$\begin{aligned} a_0 &= [r_0], \quad r_1 = \frac{1}{r_0 - a_0} \quad \text{if } r_0 \neq a_0 \\ a_i &= [r_i], \quad r_{i+1} = \frac{1}{r_i - a_i} \quad \text{if } r_i \neq a_i, i = 1, 2, ... \end{aligned}$$

As we have a recipe, the expansion is unique.

Example

$$\begin{aligned} i) \quad \pi &= [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 4, 1, 2, 14, 16, 13, 1, ...] \\ ii) \quad e &= [2, 1, 2, 1, 1, 4, 1, 1, 6, ...] \\ iii) \quad \sqrt{2} &= [1, 2, 2, \overline{2}, ...] \\ iv) \quad \sqrt{3} &= [1, 1, 2, 1, 2, \overline{1, 2}, ...] \\ v) \quad \tfrac{281}{97} &= [2, 1, 8, 1, 2, 3] \\ vi) \quad \tfrac{25}{16} &= [1, 1, 1, 3, 2] \\ vii) \quad \tfrac{9}{7} &= [1, 3, 2] \end{aligned}$$

Proof of $vii)$: $\quad \frac{9}{7} = 1 + \frac{2}{7} = 1 + \frac{1}{\frac{7}{2}} = 1 = \frac{1}{3 + \frac{1}{2}}$

So $a_0 = 1, a_1 = 3, a_2 = 2$, and the series terminates.

Exercise Prove $i) - vi)$

Given an arbitrary infinite continued fraction expansion $r_0 = [a_0, a_1, a_2, ...]$, the quantity $s_n = [a_0, a_1, ..., a_n]$ is called the n^{th} *convergent* to r_0. As n, increases s_n provides an increasingly accurate approximation to r_0. In particular, if one

wishes to obtain a good approximation, it is best to choose an s_n s.t. a_n is *large*, because then $\frac{1}{a_n}$ is "close to" $\frac{1}{a_n+\frac{1}{\ddots}}$.

Example

$\pi = 3.14159265$ to 8 d.p.

$s_0 = [a_0] = [3] = 3$

$s_1 = [a_0, a_1] = [3, 7] = 3 + \frac{1}{7} \approx 3.14285714$

$(|\text{error}| = 1.264 \times 10^{-3})$

$s_2 = [3, 7, 15] = 3 = \frac{1}{7 + \frac{1}{15}} = 3 + \frac{15}{106} = \frac{333}{106} \approx 3.14150943$

$(|\text{error}| = 8.32 \times 10^{-5})$

$s_3 = [3, 7, 15, 1] = 3 + \frac{1}{7 + \frac{1}{15+\frac{1}{1}}} = 3 + \frac{16}{113} = \frac{355}{113} \approx 3.14159292$

$(|\text{error}| = 2.67 \times 10^{-7})$

Exercise Calculate $s_4 = [3, 7, 15, 1, 292]$ and

$s_5 = [3, 7, 15, 1, 292, 1]$ for π and evaluate the error in each case.

Solution $s_4 = \frac{103993}{33102}$ $\quad |\text{error}| = 5.7789 \times 10^{-10}$

$s_5 = \frac{104348}{33215}$ $\quad |\text{error}| = 3.3163 \times 10^{-10}$

This illustrates the point about good approximations.

Note If $r_0 = [a_0, a_0, \overline{a_0}...]$, $\quad a_0 \in \mathbb{N}$, then $r_0 = a_0 + \frac{1}{r_0}$, so

$r_0^2 - a_o r_0 - 1 = 0 \quad \therefore r_o = \frac{1}{2}(a_0 + \sqrt{a_0^2 + 4})$

Examples i) $[2, 2, \overline{2}, ...] = \frac{1}{2}[2 + \sqrt{8}] = 1 + \sqrt{2}$, so $\sqrt{2} = [1, 2, 2, \overline{2}]$;

ii) $[1, 1, \overline{1}...] = \frac{1}{2}(1 + \sqrt{5})$ is called the "Golden Ratio"

Theorem $r_0 \in \mathbb{R}$ is rational iff its continued fraction expansion has finitely many terms.

Proof Clearly, if there are finitely many terms, $r_0 \in \mathbb{Q}$.

To prove the converse, we need prove it only for $r_0 \in \mathbb{Q}\backslash\mathbb{Z}$ as every integer has a 1-term continued fraction expansion.

Then $r_0 = a_0 + \frac{m}{n}$ where $m, n \in \mathbb{N}$, HCF $(m, n) = 1$ and $m < n$.

$\therefore \quad r_1 = \frac{m}{n}$ and so $a_1 = [\frac{n}{m}] \geq 1$. If $a_1 = r_1$, i.e. if $m = 1$, we are finished. Otherwise $r_0 = a_0 = \frac{1}{a_1 + \frac{1}{r_2}}$, where $r_2 = \frac{m}{n - a_1 m}$.

Note that $a_1 < \frac{n}{m} < a_1 + 1$

$\therefore ma_1 < n < ma_1 + m \quad \therefore 0 < n - ma_1 < m.$

Also HCF $(m, n - a_1 m) = 1$ because HCF $(m, n) = 1$

Repeating this process comparing r_2 and r_3, r_2 and r_4, etc., the denominator goes on decreasing, until it reaches 1, which is the final term in the expansion. In other words, the sequence {denom.(r_1), denom.(r_2),...} is a strictly monotonically decreasing sequence of natural numbers, which necessarily

terminate at 1.

Theorem $|\mathbb{R}_0^+| = |\mathcal{P}(\mathbb{N})|$

Proof We have established that each real number r_0 has a continued fraction expansion whose convergents s_n approximate r_0 with increasing accuracy as $n \to \infty$. Define the map $\phi : \mathbb{R}_a^+ \to F^+$ where $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ and $F^+ = \{\text{continued fractions s.t. } a_0 \in \mathbb{N}\} \cup \{\text{continued fractions} : a_0 = 0 \text{ and } a_1 \in \mathbb{N}\}$ by

$\phi(r_0) =$ continued fraction expansion of r_0.

Then ϕ is a bijection. It is surjective because every continued fraction in F^+ is the image of a positive real number. It is injective, because if r_0 and R_0 are two *different* real numbers the convergents of $\phi(r_0)$ will eventually differ from the convergents of $\phi(R_0)$, so $\phi(r_0) \neq \phi(R_0)$. Hence $\phi(r_0) = \phi(R_0) \Rightarrow r_0 = R_0$.

Now define a map $\psi : F^+ \to \mathcal{P}(\mathbb{N})\backslash\emptyset$ as follows:-

$$\psi([a_0]) = \{a_0\};$$

for $n \in \mathbb{N}$

$$\psi([a_0, a_1, ...a_n]) \;=\; \{a_0 + 1,\; a_0 + a_1 + 1,\; a_0 + a_1 + a_2 + 1, ..., \left(\sum_{k=0}^{n-1} a_k\right) + 1, \sum_{k=}^{n} a_k\};$$

$$\psi([a_0, a_1, ...]) = \{a_0 + 1, a_0 + a_1 + 1, a_0 + a_1 + a_2 + 1, ...\}.$$

Then ψ is a bijection. Note that $[a_0] \in F^+ \Rightarrow a_0 \in \mathbb{N}$.

Also $a_i \in \mathbb{N}, \quad \forall i \in \mathbb{N}$ in all cases.

If an element of F^+ is of *finite* length then it is of the form $[a_0, a_1, ..., a_n]$ where $a_n \geq 2$.

Elements of F^+ can have $a_0 = 0$ provided that they do not represent integers. However, by construction, if $x \in F^+$ then $\psi(x) \subset \mathbb{N}$, so $\mathcal{P}(\mathbb{N})$ is in $1:1$ correspondence with F^+. All possible elements of $\mathcal{P}(\mathbb{N})\backslash\emptyset$ are in $\mathrm{im}(\phi)$.

By the composition theorem, $\psi \circ \phi : \mathbb{R}^+ \to \mathcal{P}(\mathbb{N})\backslash\phi$ is a bijection. Define $\chi : \mathbb{R}_0^+ \to \mathcal{P}(\mathbb{N})$ by

$$\chi(x) = \begin{cases} \psi \circ \phi(x), & x \neq 0 \\ \emptyset, & x = 0 \end{cases}$$

By construction, this is a bijection, so

$$\left|\mathbb{R}_0^+\right| = \left|\mathcal{P}(\mathbb{N})\right|.$$

Linear Difference Equations

General Terminology

There are many similarities between linear ordinary difference equations (OΔEs) and linear ODEs.

OΔEs require one to find the dependent variable (usually u) as a function of a discrete independent variable (usually this takes integer values and is denoted by n).

The general **1st order** OΔE is of the form

$$u(n+1) = F(n, u(n))$$

for some given F which depends non trivially on $u(n)$.

The general **2nd order** OΔE is of the form

$$u(n+2) = F(n, u(n), u(n+1)).$$

An OΔE is solved when $u(n)$ is known as a function of n. The general solution of a kth order OΔE depends upon k arbitrary constants. In particular, the general solution of a 1st order OΔE depends upon one arbitrary constant (commonly $u(c)$). We shall restrict attention to linear OΔEs in which each term contains at most one $u(k)$.

The most general 1st order linear OΔE is

$$u(n+1) + a(n)u(n) = b(n), \quad a(n) \neq 0. \tag{1}$$

The most general 2nd order linear OΔE is

$$u(n+2) + p(n)u(n+1) + q(n)u(n) = r(n), \quad q(n) \neq 0. \tag{2}$$

A linear OΔE is *homogeneous* if every term contains exactly one $u(k)$. Otherwise it is inhomogeneous.

So

$$(1) \text{ is homogeneous iff } b(n) = 0;$$

$$(2) \text{ is homogeneous iff } r(n) = 0.$$

N.B. $u(n) = 0 \quad \forall n$ is always a solution of a homogeneous OΔE.

Just as for linear ODEs, the general solutions of a linear inhomogeneous OΔE is the sum of (one **particular** sol) and (the general sol of the related homogeneous difference equation, called the **complementary function**). We restrict attention to OΔEs for which $a(n)$ in (1) and $p(n)$, $q(n)$ in (2) are **constants** (i.e. they do not depend on n).

First-order homogeneous OΔEs.

To find the general solution of

$$u(n+1) + au(n) = 0,$$

note that for all $n \geq 1$

$$\begin{aligned} u(n) &= -au(n-1) \\ &= -a(-au(n-2)) \\ &= (-a)^2 u(n-2) \\ &= \quad \vdots \\ &= (-a)^n u(0). \end{aligned}$$

Here $u(0)$ is the arbitrary constant. If $n \leq -1$ then

$$\begin{aligned} u(n) &= -\frac{1}{a}u(n+1) \\ &= (-\frac{1}{a})^2 u(n+2) \\ &= \quad \vdots \\ &= (-\frac{1}{a})^{|n|} u(n+|n|) \\ &= (-a)^n u(0). \end{aligned}$$

So in all cases,

$$\boxed{u(n) = u(0)(-a)^n.}$$

Examples

(i) Solve $u(n+1) - 2u(n) = 0$.

Solution: Here $a = -2$, so $u(n) = u(0) \times 2^n$ is the general solution.

(ii) Solve $u(n+1) + u(n) = 0, \quad u(0) = 2$.

Solution: Here $a = 1$, so $u(n) = u(0) \times (-1)^n$ is the general solution.

But $u(0) = 2$, so the solution we require is

$$u(n) = 2 \times (-1)^n.$$

(iii) Solve $u(n+1) - 3u(n) = 0, \quad u(1) = 1$.

Solution: Here $a = -3$, so $u(n) = u(0) \times 3^n$ is the general solution.

Hence $u(1) = u(0) \times 3^1 = 3u(0)$.

But $u(1) = 1$, so $u(0) = \frac{1}{3}$.

Therefore $u(n) = \frac{1}{3} \times 3^n = 3^{n-1}$.

Exercises

Solve each of the following

$$\text{(i)} \quad u(n+1) + 4u(n) = 0, \quad u(-1) = 8.$$

$$\text{(ii)} \quad u(n+1) - 5u(n) = 0, \quad u(100) = 0.$$

Nonhomogeneous 1st-order OΔEs

To solve

$$u(n+1) + au(n) = b(n), \quad a \in \mathbb{R} \setminus \{0\},$$

write $u(n) = (-a)^n v(n)$. For simplicity, we shall solve this only for $n \in \mathbb{N}$.

Note: We have written $u(n)$ as a product of a known solution of the *homogeneous* equation and an unknown function $v(n)$.

Then

$$(-a)^{n+1} v(n+1) + a(-a)^n v(n) = b(n)$$

$$\therefore \quad v(n+1) - v(n) = \frac{b(n)}{(-a)^{n+1}}.$$

So

$$\begin{aligned} v(n) &= v(n-1) + \frac{b(n-1)}{(-a)^n} \\ &= v(n-2) + \frac{b(n-2)}{(-a)^{n-1}} + \frac{b(n-1)}{(-a)^n} \\ &= \vdots \\ &= v(0) + \sum_{k=0}^{n-1} \frac{b(k)}{(-a)^{k+1}} \end{aligned}$$

$\therefore$

$$\boxed{u(n) = v(0)(-a)^n + \left(\sum_{k=0}^{n-1} \frac{b(k)}{(-a)^{k+1}} \right) \times (-a)^n.}$$

Here $v(0)$ is the arbitrary constant,

$v(0)(-a)^n$ is the *complementary function*,

and the remaining term on the RHS is the *particular solution*.

Examples:

(i) Solve $u(n+1) + u(n) = 2$.

Solution: Here $a = 1$, $b(n) = 2$, so

$$\begin{aligned} u(n) &= v(0) \times (-1)^n + \left(\sum_{k=0}^{n-1} \frac{2}{(-1)^{k+1}} \right) (-1)^n \\ &= \begin{cases} v(0), & n \quad \text{even} \\ 2 - v(0), & n \quad \text{odd.} \end{cases} \end{aligned}$$

(ii) Solve $u(n+1) - 2u(n) = 2^n, \quad u(0) = 1$.

Here $a = -2$, $b(n) = 2^n$, so

$$\begin{aligned} u(n) &= v(0) \times 2^n + \left(\sum_{k=0}^{n-1} \frac{2^k}{2^{k+1}} \right) \times 2^n \\ &= v(0) \times 2^n + n \times 2^{n-1}. \end{aligned}$$

$$\therefore 1 = u(0) = v(0).$$

So

$$u(n) = 2^{n-1}(2 + n).$$

Exercises: Solve each of the following OΔEs:

$$\text{(i)} \quad u(n+1) + 2u(n) \;=\; -1$$

$$\text{(ii)} \quad u(n+1) + 3u(n) \;=\; n \times 3^n, \quad u(1) = 0.$$

Second-order homogeneous OΔEs

To solve

$$u(n+2) + pu(n+1) + qu(n) = 0,$$

note that the solution of $u(n+1) + au(n) = 0$ is

$$u(n) = u(0)(-a)^n,$$

i.e. it is a *power law* - each term is a constant multiple of the previous one. Try looking for power-law solutions of the 2nd-order OΔE.

Let $u(n) = Am^n$, where $A, m \in \mathbb{R}$.
Then $u(n+2) + pu(n+1) + qu(n) = Am^n(m^2 + pm + q)$.
So a solution exists for arbitrary A if

$$m^2 + pm + q = 0.$$

This is called the *auxiliary equation*.

The solutions are $m = m_+$ and $m = m_-$, where

$$m_\pm = \frac{1}{2}(-p \pm \sqrt{p^2 - 4q}).$$

There are three cases, according to the sign of $p^2 - 4q$.

(i) $p^2 - 4q > 0$:

Here m_+ and m_- are distinct real numbers. So $u(n) = A_1 m_+^n$ and $u(n) = A_2 m_-^n$ are solutions for all $A_1, A_2 \in \mathbb{R}$. As the ODE is *linear* we can superpose these solutions to obtain the *general solution*

$$u(n) = A_1 m_+^n + A_2 m_-^n.$$

(ii) $p^2 - 4q < 0$:

Again the solutions of the auxiliary equation are distinct, but now they are complex: $m_\pm = \alpha \pm i\beta$, where $\alpha = -\frac{p}{2}$ and $\beta = \frac{1}{2}\sqrt{4q - p^2} > 0$. We can still write the general solution as

$$u(n) = A_1 m_+^n + A_2 m_-^n$$

but A_1, A_2 m_+ and m_- are *complex*. It is neater to use polar

coords:

$$r = \sqrt{\alpha^2 + \beta^2}, \qquad \theta = \tan^{-1}\left(\frac{\beta}{\alpha}\right) \in (0, \pi).$$

So $m_+ = re^{i\theta}$ and $m_- = re^{-i\theta}$.

$$\begin{aligned} \therefore u(n) &= A_1 r^n e^{in\theta} + A_2 r^n e^{-in\theta} \\ &= r^n[(A_1 + A_2)\cos(n\theta) + (iA_1 - iA_2)\sin(n\theta)] \\ &= r^n[B_1 \cos(n\theta) + B_2 \sin(n\theta)] \end{aligned}$$

where $B_1, B_2 \in \mathbb{R}$.

(iii) $p^2 - 4q = 0$:

Then the root $m = -\frac{p}{2}$ is repeated, so we only have one family of solutions, $u(n) = Am^n$. To find the other solution, write

$$u(n) = m^n v(n), \quad \text{where } m = -\frac{p}{2}.$$

The difference equation

$$u(n+2) + pu(n+1) + \frac{p^2}{4}u(n) = 0$$

becomes

$$m^{n+2}(v(n+2) - 2v(n+1) + v(n)) = 0.$$

Let

$$w(n) = v(n+1) - v(n)$$

$$\therefore \quad w(n+1) = v(n+2) - v(n+1)$$

$$\therefore \quad w(n+1) - w(n) = v(n+2) - 2v(n+1) + v(n) = 0$$

$$\therefore \quad w(n) = w(0) \quad \forall n$$

$$\therefore \quad v(n+1) - v(n) = w(0).$$

Using our results for 1st-order OΔEs,

$$v(n) = v(0) + \sum_{k=0}^{n-1} w(0) = v(0) + nw(0).$$

Write $v(0) = A$, $w(0) = B$.

So $u(n) = m^n(A + Bn)$.

As this depends on two arbitrary constants, it is the general solution of the OΔE.

Summary

General solution of $u(n+2)+pu(n+1)+qu(n)=0$:

(i) $\underline{p^2-4q>0}$:

$$u(n)=A_1m_+^n+A_2m_-^n,\quad m_\pm=\frac{1}{2}(-p\pm\sqrt{p^2-4q}).$$

(ii) $\underline{p^2-4q<0}$:

$$u(n)=r^n(B_1\cos(n\theta)+B_2\sin(n\theta))$$

where $r=\sqrt{\alpha^2+\beta^2}$, $\theta=\tan^{-1}\left(\frac{\beta}{\alpha}\right)\in(0,\pi)$, given $\alpha=-\frac{p}{2}$, $\beta=\frac{1}{2}\sqrt{4q-p^2}$.

(iii) $\underline{p^2-4q=0}$:

$$u(n)=m^n(A+Bn),\quad m=-\frac{p}{2}.$$

Examples:

1. Solve $u(n+2) - 4u(n+1) + 3u(n) = 0$

Solution: Here $p = -4$, $q = 3$, so the auxiliary equation is

$$m^2 - 4m + 3 = 0.$$

So $m = 3$ or $m = 1$, and hence

$$u(n) = A_1 \times 3^n + A_2.$$

2. Solve $u(n+2) - 4u(n+1) + 4u(n) = 0$, subject to $u(0) = 1$, $u(1) = 0$.

Solution: Here the auxiliary equation is

$$m^2 - 4m + 4 = 0, \quad \text{i.e. } m = 2.$$

So

$$\begin{aligned} u(n) &= 2^n(A + Bn) \\ \therefore \quad u(0) &= A = 1 \\ u(1) &= 2(A + B) = 0 \quad \therefore B = -1 \end{aligned}$$

Therefore the solution is

$$u(n) = 2^n(1 - n).$$

3. Solve $u(n+2)-4u(n+1)+8u(n)=0$, $u(0)=0$, $u(1)=1$.

Solution: $m^2-4m+8=0$, so $m_\pm = 2(1\pm i)$.

$$\therefore \quad \alpha=\beta=2.$$

Hence $r=\sqrt{\alpha^2+\beta^2}=2^{\frac{3}{2}}$ and $\tan^{-1}\left(\frac{\beta}{\alpha}\right)=\frac{\pi}{4}$,

(NB $\theta\in(0,\pi)$).

So the general solution is

$$u(n)=2^{\frac{3n}{2}}\left(B_1\cos\left(\frac{n\pi}{4}\right)+B_2\sin\left(\frac{n\pi}{4}\right)\right).$$

$$\therefore \qquad u(0)=B_1=0$$

$$\begin{aligned} u(1) &= 2\sqrt{2}\left(B_1\cos\left(\frac{\pi}{4}\right)+B_2\sin\left(\frac{\pi}{4}\right)\right) \\ &= 2(B_1+B_2)=1 \end{aligned}$$

$$\therefore \qquad B_1=0, \quad B_2=\frac{1}{2}.$$

Hence $u(n)=2^{\frac{3n-2}{2}}\sin(\frac{n\pi}{4})$.

Exercises:

Solve each of the following:

(i) $u(n+2) - u(n+1) - u(n) = 0$, $u(0) = 0$, $u(1) = 1$.

(ii) $u(n+2) - 2u(n+1) + 4u(n) = 0$, $u(0) = u(1) = 1$.

(iii) $u(n+2) - 2u(n+1) + u(n) = 0$, $u(0) = 1$, $u(1) = 2$.

Note: The second-order homogeneous OΔE

$$u(n+2) + pu(n+1) + qu(n) = 0$$

is often re-written in the form

$$u(n) = -pu(n-1) - qu(n-2).$$

This form is called the *recurrence relation*. It gives $u(n)$ in terms of the previous two values of u.

For instance the OΔE in exercise (i) could be written as the recurrence relation

$$u(n) = u(n-1) + u(n-2), \quad u(0) = 0, \quad u(1) = 1.$$

This relation produces the *Fibonacci numbers*

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$$

Second-order inhomogeneous OΔEs

To solve $u(n+2)+pu(n+1)+qu(n) = b(n)$, write $u(n)=m^n v(n)$, where m is *one* of the roots of the auxiliary equation $m^2+pm+q=0$. For definiteness, let

$$m = m_+ = -\frac{1}{2}p + \frac{1}{2}\sqrt{p^2-4q}.$$

Then

$$m_+^{n+2}v(n+2) + pm_+^{n+1}v(n+1) + qm_+^n v(n) = b(n).$$

Let

$$w(n) = v(n+1) - v(n),$$

so

$$w(n+1) = v(n+2) - v(n+1) = v(n+2) - w(n) - v(n).$$

$$\begin{aligned} \therefore \qquad b(n) &= m_+^{n+2}(w(n+1)+w(n)+v(n)) \\ &\quad + pm_+^{n+1}(w(n)+v(n)) + qm_+^n v(n) \end{aligned}$$

$$\begin{aligned} \therefore \qquad b(n) &= m_+^{n+2}w(n+1) + m_+^{n+1}(m_+ + p)w(n) \\ &\quad + m_+^n(m_+^2 + pm_+ + q)v(n) \end{aligned}$$

$$\therefore \qquad w(n+1) - \frac{m_-}{m_+}w(n) = \frac{b(n)}{(m_+)^{n+2}}.$$

because $m_+ + p = \frac{1}{2}p + \frac{1}{2}\sqrt{p^2-4q} = -m_-$

This is a first-order OΔE which we can solve. Having found $w(n)$ as a function of n, solve

$$v(n+1) - v(n) = w(n)$$

and then write $u(n) = m_+^n v(n)$.

This method of splitting up a 2nd-order linear OΔE into two 1st-order OΔEs by writing $u(n)$ as $v(n)$ times a nonzero solution of the homogeneous equation is called "reduction of order". It works just as well for linear ODEs!

Example:

Solve $u(n+2) - 4u(n+1) + 3u(n) = 3^n$, $u(0) = 0$, $u(1) = 1$.

Solution: We know that $m_+ = 3$ and $m_- = 1$.

Write $u(n) = 3^n v(n)$.

$$\therefore \qquad 3^{n+2}v(n+2) - 4 \times 3^{n+1}v(n+1) + 3 \times 3^n v(n) = 3^n,$$

Let $w(n) = v(n+1) - v(n)$.

$$\begin{aligned} \therefore \qquad 3^n &= 3^{n+2}[w(n+1) + w(n) + v(n)] \\ &\quad -4 \times 3^{n+1}[w(n) + v(n)] + 3 \times 3^n v(n). \\ &= 3^{n+2}w(n+1) - 3^{n+1}w(n) \\ \therefore \qquad & w(n+1) - \frac{1}{3}w(n) = \frac{1}{9}. \end{aligned}$$

Here $a = -\frac{1}{3}$, $b(n) = \frac{1}{9}$.

$$\begin{aligned} \therefore \qquad w(n) &= \left(\frac{1}{3}\right)^n \left[w(0) + \sum_{k=0}^{n-1} \frac{1}{9(\frac{1}{3})^{k+1}}\right] \\ &= \left(\frac{1}{3}\right)^n \left[w(0) + \frac{1}{3}\sum_{k=0}^{n-1} 3^k\right] \\ &= \left(\frac{1}{3}\right)^n \left[w(0) + \frac{1}{6}(3^n - 1)\right] \end{aligned}$$

$$\therefore \quad v(n+1) - v(n) = \left(\frac{1}{3}\right)^n \left[w(0) - \frac{1}{6}\right] + \frac{1}{6}.$$

$$\begin{aligned} \therefore \qquad v(n) &= v(0) + \sum_{k=0}^{n-1} \left[\left(\frac{1}{3}\right)^k \left[w(0) - \frac{1}{6}\right] + \frac{1}{6}\right] \\ &= v(0) + \frac{3}{2}\left(1 - \left(\frac{1}{3}^n\right)\right)\left[w(0) - \frac{1}{6}\right] + \frac{n}{6} \\ &= v(0) + \frac{3}{2}\left[w(0) - \frac{1}{6}\right] - \frac{3}{2}\left[w(0) - \frac{1}{6}\right]\left(\frac{1}{3}\right)^n + \frac{n}{6}. \end{aligned}$$

For simplicity write this as

$$v(n) = A_1 + A_2\left(\frac{1}{3}\right)^n + \frac{n}{6}.$$

Then $u(n) = A_1 \times 3^n + A_2 + \frac{n}{6} \times 3^n$.

$$u(0) = A_1 + A_2 = 0$$

$$u(1) = 3A_1 + A_2 + \frac{1}{2} = 1$$

$$\therefore \qquad A_1 = \frac{1}{4}, \qquad A_2 = -\frac{1}{4}$$

$$\therefore \qquad u(n) = \frac{1}{4}(3^n - 1) + \frac{n}{6} \times 3^n.$$

Number theory - divisibility

For the remainder of the course, we study various properties of the integers $\mathbb{Z}$. The word "number" will mean a *natural* number.

Definition:

Let $a \in \mathbb{Z}$. We say that $d \in \mathbb{Z} \setminus \{0\}$ **divides** a, and write $d|a$, if $\frac{a}{d} \in \mathbb{Z}$. Usually, we restrict attention to $d \in \mathbb{N}$ without loss of generality.

The highest common factor of $a, b \in \mathbb{Z}$ is the greatest $d \in \mathbb{N}$ such that $d|a$ and $d|b$.

Theorem: *If* $a = qb + r$ *then* $HCF(a, b) = HCF(b, r)$.

Proof:

If $d|a$ and $d|b$ then $\exists \quad a_1, b_1 \in \mathbb{Z}$ such that $a = a_1 d$, $b = b_1 d$.

$$\therefore \quad r = a - qb = d(a_1 - qb_1)$$

$$\therefore \quad d|r.$$

Similarly, if $d|b$ and $d|r$ then $d|a$. So every common factor of a, b is a common factor of b, r and vice versa. Hence $HCF(a, b) = HCF(b, r)$.

This result can be turned into an algorithm (called *Euclid's algorithm*) for finding the highest common factor of two numbers $a, b \in \mathbb{N}$. If $a = b$, then $HCF(a, b) = a$. Otherwise, assume without loss of generality that $a > b$.

Step 1:

Given a, b, let $q = [\frac{a}{b}]$.

Let $r = a - qb$. So $a = qb + r$, where $0 \leq r \leq b - 1$.

If $r = 0$, $HCF(a, b) = b$.

Otherwise go to Step 2.

Step 2:

Use the previous theorem to conclude that $HCF(a, b) = HCF(b, r)$.

Now let $\tilde{a} = b$, $\tilde{b} = r$.

Note that $\tilde{a} > \tilde{b} > 0$ and $HCF(a, b) = HCF(\tilde{a}, \tilde{b})$.

Go back to Step 1, using $\tilde{a}$, $\tilde{b}$ in place of a, b.

This process iterates until a zero remainder r is obtained.

Example:

Calculate $HCF(924, 588)$ using Euclid's algorithm.

$$\begin{aligned} 924 = 1 \times 588 + 336 \qquad & q = \left[\frac{924}{588}\right] = 1 \\ 588 = 1 \times 336 + 252 \qquad & q = \left[\frac{588}{336}\right] = 1 \\ 336 = 1 \times 252 + 84 \qquad & q = \left[\frac{336}{252}\right] = 1 \\ 252 = 3 \times 84 \qquad & q = \left[\frac{252}{84}\right] = 3 \end{aligned}$$

$$\begin{aligned} \therefore \quad HCF(924, 588) &= HCF(588, 336) \\ &= HCF(336, 252) \\ &= HCF(252, 84) \\ &= 84. \end{aligned}$$

Exercises:

(i) Calculate $HCF(3367, 2639)$ using Euclid's algorithm.

(ii) Show that the continued fraction representation of $\frac{924}{588}$ is $[1, 1, 1, 3]$. Explain the connection between continued fractions and Euclid's algorithm.

Note:

In the above example, we can write $84 = HCF(924, 588)$ as an *integer* linear combination of 924 and 588, as follows.

$$\begin{aligned} 84 &= 336 - 1 \times 252 \\ &= 336 - 1 \times (588 - 1 \times 336) \\ &= 2 \times 336 - 1 \times 588 \\ &= 2 \times (924 - 1 \times 588) - 1 \times 588 \\ &= 2 \times 924 - 3 \times 588 \end{aligned}$$

In the same way, if $a, b \in \mathbb{N}$ then $\exists \quad u, v \in \mathbb{Z}$ such that

$$HCF(a, b) = ua + vb.$$

This is called *Bezout's identity*. The proof is obtained by "working backwards" up the chain of equations of Euclid's algorithm, as in the example above.

Theorem: Let $a, b \in \mathbb{N}$ and let $d = HCF(a, b)$.

Then $d|c$ iff $\exists \quad x, y \in \mathbb{Z}$ such that $c = xa + yb$.

Proof:

If $d|c$ then $\exists \quad c_1 \in \mathbb{Z}$ such that $c = c_1 d$.

By Bezout's identity, $\exists \quad u, v \in \mathbb{Z}$ such that $d = ua + vb$.

Therefore $c = c_1 ua + c_1 vb$, so if $x = c_1 u$, $y = c_1 v$ then $c = xa + yb$.

Now suppose that $\exists \quad x, y \in \mathbb{Z}$ such that $c = xa + yb$.

As $d|a$ and $d|b$ $\exists \quad a_1, b_1 \in \mathbb{N}$ such that $a = a_1 d$, $b = b_1 d$.

$$\therefore \quad c = (xa_1 + yb_1)d.$$

As $xa_1 + yb_1$is an integer it follows that $d|c$.

The theorem implies that every integer linear combination of a and b is a multiple of $HCF(a, b)$.

Definition:

Two numbers $a, b \in \mathbb{N}$ are **coprime** if $HCF(a, b) = 1$.

Theorem:

$a, b \in \mathbb{N}$ are coprime iff $\exists \quad x, y \in \mathbb{Z}$ such that

$$xa + yb = 1.$$

Proof: Apply the previous theorem with $c = 1$, noting that (for $d \in \mathbb{N}$) $d|1$ iff $d = 1$.

Definition: The *least common multiple* of $a, b \in \mathbb{N}$, denoted $LCM(a, b)$, is the smallest number $l \in \mathbb{N}$ such that $a|l$ and $b|l$.

Theorem: If $a, b \in \mathbb{N}$, $l = LCM(a, b)$, and $d = HCF(a, b)$, then $l = \frac{ab}{d}$.

Proof: Exercise!

Definition:

A **Diophantine equation** is an equation for which **integer** solutions are sought.

Example:

The linear Diophantine equation in two variables x, y is of the form

$$ax + by = c \tag{3}$$

where $a, b, c \in \mathbb{Z}$ are given. The problem is to find all solutions $x, y \in \mathbb{Z}$.

Note: From our earlier results, it is clear that (3) has a solution iff $HCF(a, b)$ divides c. In fact, (3) has an infinite family of solutions if $HCF(a, b)$ divides c.

Exercise: Let $d = HCF(a, b)$, and suppose that $d|c$. Find all solutions of (3), supposing that $a, b \in \mathbb{N}$.

Solution:

Use Euclid's algorithm in reverse to express d in terms of a and b :-

$$d = ua + vb,$$

where $u, v \in \mathbb{Z}$.

As $d|c$, $\exists \quad c_1 \in \mathbb{Z}$ such that

$$c = c_1 d = c_1 ua + c_1 vb.$$

Let $x_0 = c_1 u$, $y_0 = c_1 v$.

So we have found one solution $(x, y) = (x_0, y_0)$ of (3).

For any other solution (x, y), we have

$$ax + by = c = ax_0 + by_0.$$

$$\therefore \quad a(x - x_0) = -b(y - y_0).$$

As $d = HCF(a, b)$, $\exists \quad a_1, b_1 \in \mathbb{N}$ such that

$$a = a_1 d, \quad b = b_1 d \quad \text{and} \quad HCF(a_1, b_1) = 1.$$

So $a_1(x - x_0) = -b_1(y - y_0)$.

As a_1 divides the LHS and $HCF(a_1, b_1) = 1$ it follows that $a_1 | (y - y_0)$.

$\therefore \quad n \in \mathbb{Z}$ such that $y - y_0 = a_1 n$. $\quad \therefore \quad x - x_0 = -b_1 n$.

So the general solution of (3) is the set of *all* solutions of this form, i.e.

$$x = x_0 - \frac{bn}{d}, \quad y = y_0 + \frac{an}{d}, \quad n \in \mathbb{Z}.$$

Number Theory - primes:

To prove various facts about prime numbers, we need to use two forms of proof by induction:

1. The principle of Induction

Let $P(n)$ denote a proposition about $n \in \mathbb{N}$. If $P(1)$ is true and if $P(n)$ implies $P(n+1)$ for all $n \in \mathbb{N}$, then $P(n)$ is true for all $n \in \mathbb{N}$.

In symbols:

$$(P(1) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))) \Rightarrow \forall n \in \mathbb{N}, \quad P(n).$$

2. The principle of Strong Induction

If $P(1)$ is true and if $P(1), P(2), \ldots, P(n)$ together imply $P(n+1)$ for all $n \in \mathbb{N}$, then $P(n)$ is true for all $n \in \mathbb{N}$.

In symbols:

$$\Big(P(1) \wedge \big(\forall n \in \mathbb{N}, (P(1) \wedge P(2) \wedge \ldots \wedge P(n)) \Rightarrow P(n+1)\big)\Big)$$

$$\Rightarrow \forall n \in \mathbb{N}, \quad P(n).$$

Example:

Let $\lg(n)$ denote the logarithm, **base 2**, of $n \in \mathbb{N}$.

So $\lg(2^k) = k$.

Define a function $F(n)$ as follows:

$$F(n) \;=\; \begin{cases} 0, & \text{if } n = 1 \\ F\left(\left[\frac{n}{2}\right]\right) + 1, & \text{if } n \geq 2. \end{cases}$$

Prove that $F(n) \leq \lg(n)$, for all $n \in \mathbb{N}$.

Base step:

$F(1) = 0$ and $\lg(1) = 0$, so $F(n) \leq \lg(n)$ for $n = 1$.

Strong Induction Hypothesis:

Suppose that $F(m) \leq \lg(m)$ for all $m \in \{1, 2, \ldots, n\}$.

Induction step

$$
\begin{aligned}
F(n+1) &= F\left(\left\lceil\frac{(n+1)}{2}\right\rceil\right)+1 \\
&\leq \lg\left(\left\lceil\frac{(n+1)}{2}\right\rceil\right)+1 \qquad \text{because } 1 \leq \left\lceil\tfrac{(n+1)}{2}\right\rceil \leq n \\
&\leq \lg\left(\frac{(n+1)}{2}\right)+1 \\
&\leq \lg(n+1)-\lg(2)+1 \\
&= \lg(n+1).
\end{aligned}
$$

So the result is true for $(n+1)$ if it is true for all $m \in \{1, 2, \ldots, n\}$. $\quad \therefore$ the result holds for all $n \in \mathbb{N}$.

Here are some useful results about primes:

1. If p is prime and $a \in \mathbb{Z}$ then either $p|a$ or $HCF(p, a) = 1$.

Proof:

Because $d = HCF(p, a)$ divides p, it follows that

$$d = p \text{ or } d = 1.$$

2. If p is prime and $a, b \in \mathbb{Z}$ then $p|ab \Rightarrow (p|a \text{ or } p|b)$.

Proof:

Let p divide ab. If p does not divide a then $HCF(p, a) = 1$.

By Bezout's identity, there exists $u, v \in \mathbb{Z}$ such that

$$\begin{aligned} au + pv &= 1. \\ \therefore \qquad bau + bpv &= b. \end{aligned}$$

As $p|ab$ and $p|p$ it follows that $p|b$.

3. If p is prime and p divides $a_1 a_2 \dots a_n$ then p divides one a_i.

Proof: Use induction. If $n = 1$ then $p|a_1$.

Now suppose $n \geq 1$ and the result is true for all products of n terms. Now suppose that $p|a_1 a_2 \dots a_n a_{n+1}$. Then, from **2.** with $a = a_{n+1}$ and $b = a_1 a_2 \dots a_n$,

$$p|a_{n+1} \text{ or } p|a_1 a_1 \dots a_n.$$

In the second case p divides one of $a_1, \dots, a_n$ by the induction hypothesis. So in either case, p divides one of $a_1, \dots, a_n, a_{n+1}$. So the result is true for $n + 1$ terms. Hence it is true for all $n \in \mathbb{N}$.

4. The Fundamental Theorem of Arithmetic.

Every integer $n > 1$ has a prime-power factorization

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

where $p_1, \dots, p_k$ are distinct primes and $e_1, \dots, e_k \in \mathbb{N}$. This factorization is unique (up to a reordering of the factors).

Examples:

$$(i) \quad 12 = 2^2 \times 3^1 = 3^1 \times 2^2$$

$$(ii) \quad 60 = 2^2 \times 3^1 \times 5^1 = 2^2 \times 5^1 \times 3^1 = \text{etc.}$$

$$(iii) \quad 11 = 11^1$$

Proof:

Use strong induction to prove that a factorization exists. Base step: for $n = 2$, $n = 2^1$. Note also that if n is any prime then $n = n^1$ is a factorization. Now suppose that a factorization exists for each $n \leq N$. If $N + 1$ is prime, we have shown that a factorization exists, so suppose that $N + 1 = ab$, where $a > 1$ and $b > 1$. Clearly $a < N$ and $b < N$ so, by the induction hypothesis, they each have a factorization . Combining these two factorizations together gives a

factorization for $N+1$. So a factorization exists for each $n > 1$.

Now we prove that the factorization is unique.

Suppose that n has factorizations

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \dots q_l^{f_l}.$$

The first factorization shows that $p_1 | n$, so p_1 divides one of the primes $q_1, \dots, q_l$. By rearranging the order of the second factorization, we can say $p_1 | q_1$ w.l.o.g. As q_1 is prime, $q_1 = p_1$. So we can divide both factorizations by p_1 exactly $\min\{e_1, f_1\}$ times.

If $e_1 > f_1$ then this gives

$$p_1^{e_1 - f_1} p_2^{e_2} \dots p_k^{e_k} = q_2^{f_2} \dots q_l^{f_l}.$$

The LHS is divisible by p_1 but the RHS is not, which is a contradiction.

Similarly, we can obtain a contradiction if $e_1 < f_1$.

$$\therefore \quad f_1 = e_1, \qquad \text{so } q_1^{f_1} = p_1^{e_1}$$

$$\therefore \quad p_2^{e_2} \dots p_k^{e_k} = q_2^{f_2} \dots q_l^{f_l}.$$

Repeat the above process to show that $q_i^{f_i} = p_i^{e_i}$ for $i = 1, \ldots, k$. At this stage if $l > k$ then

$$1 = q_{k+1}^{f_{k+1}} \ldots q_l^{f_l}.$$

But 1 has no prime factors. Therefore $l = k$.

So the two factorizations are identical (up to a reordering of the terms).

Distribution of primes

Euclid's Theorem (that there are infinitely many primes) does not tell us how they are distributed.

There are

$$\begin{aligned} 168 &\quad \text{primes between} \quad 1 \text{ and } 1000 \\ 135 &\quad \text{primes between} \quad 1001 \text{ and } 2000 \\ 127 &\quad \text{primes between} \quad 2001 \text{ and } 3000 \end{aligned}$$

which suggests that primes become more widely-spaced as one looks at larger numbers.

It can be proved that $\mathbb{N}$ contains a string of consecutive non-prime numbers of *any* length.

For instance,

$$\begin{aligned} &\text{the numbers} \quad 8, 9, 10 \quad \text{form such a string of length } 3 \\ &\text{the numbers} \quad 90 - 96 \quad \text{form such a string of length } 7 \\ &\text{the numbers} \quad 888 - 906 \quad \text{form such a string of length } 19 \end{aligned}$$

These are the longest prime-free strings $\leq 10, 100$ and 1000 respectively.

The largest-known primes are separated by millions of digits. Most of these primes are of the form $2^p - 1$, where p is a prime. Any number of this form is called a **Mersenne number**; if it is prime, it is called a **Mersenne prime**.

The first few Mersenne numbers are

$$\begin{aligned} 3 &= 2^2 - 1 && \text{prime} \\ 7 &= 2^3 - 1 && \text{prime} \\ 31 &= 2^5 - 1 && \text{prime} \\ 127 &= 2^7 - 1 && \text{prime} \\ 2047 &= 2^{11} - 1 = 23 \times 89. \end{aligned}$$

The 41st Mersenne prime was discovered in May 2004. It is $2^{24036583} - 1$ and has 7,235,733 decimal digits.

Definition:

A *perfect number* is a number whose factors (apart from itself) sum to itself.

Examples:

$$\begin{aligned} 6 &= 1+2+3 \\ 28 &= 1+2+4+7+14 \end{aligned}$$

Exercise:

Show that 496 is perfect.

Theorem:

An *even* number is perfect iff it is of the form $\frac{1}{2}m_p(m_p+1)$ where $M_p = 2^p - 1$ is a Mersenne prime.

Examples:

$$\begin{aligned} 6 &= 2\times 3 &&= \frac{1}{2}\times 3\times 4 &&= \frac{1}{2}M_2(M_2+1) \\ 28 &= 4\times 7 &&= \frac{1}{2}\times 7\times 8 &&= \frac{1}{2}M_3(M_3+1) \\ 496 &= 16\times 31 &&= \frac{1}{2}\times 31\times 32 &&= \frac{1}{2}M_5(M_5+1) \end{aligned}$$

No odd perfect number is known. It has been shown that any odd perfect number must exceed 10^{300} and must have at least 47 prime factors. It is conjectured that there are no odd perfect numbers.

Proof:

Any even number n can be written in the form

$$n = 2^{p-1}q$$

where $p \geq 2$ and q is odd.

Introduce the function $\sigma(n) =$ sum of *all* factors of n.

If m is prime then $\sigma(m) = 1 + m$.

If m is perfect then $\sigma(m) = 2m$.

It can be proved that if $HCF(x, y) = 1$ then $\sigma(xy) = \sigma(x)\sigma(y)$. (Exercise - do this!)

So

$$\begin{aligned}\sigma(n) &= \sigma(2^{p-1}q) \\ &= \sigma(2^{p-1})\sigma(q) \\ &= (1+2+2^2\ldots+2^{p-1})\sigma(q) \\ &= (2^p-1)\sigma(q).\end{aligned}$$

But n is perfect iff $\sigma(n) = 2n$, i.e. iff

$$2^p q = (2^p-1)\sigma(q).$$

This is satisfied iff $(2^p-1)|q$, i.e. iff $\exists\, r \in \mathbb{N}$ such that

$$q = (2^p-1)r \text{ and } \sigma(q) = 2^p r = q + r.$$

We know that $r|q$ and $q|q$, so $r = 1$ and q is prime (for otherwise $\sigma(q)$ would exceed $q + r$).

Hence n is a perfect even number iff

$$n = 2^{p-1}(2^p-1)$$

where $2^p - 1$ is prime.

Note that if $p = ab$, where a, b are greater than 1, then

$$2^p - 1 = 2^{ab} - 1 = (2^a-1)[2^{(b-1)a} + 2^{(b-2)a} + \ldots + 2^{2a} + 2^a + 1]$$

which is not prime.

Therefore p is prime whenever $2^p - 1$ is prime. So n is an

even perfect number iff it is of the form $\frac{1}{2}M_p(M_p + 1)$, where $M_p = 2^p - 1$ is a Mersenne prime.

The *average* distribution of the primes is given by the Prime Number Theorem. One version of it states:

$$\frac{\text{no. of primes} \leq n}{(n \div \ln(n))} \to 1 \text{ as } n \to \infty.$$

In other words, the proportion of primes in the numbers from 1 to n is roughly $\frac{1}{\ln(n)}$ (for n sufficiently large).

Congruences

Q.1. What time of day will it be 100 hours from now?

A. 100 hrs = 4 hrs + 4×24 hrs, so the time will be 4 hrs later than it is now.

Q.2. A fairground roundabout spins anticlockwise at a rate of 10°/sec for $2\frac{1}{4}$ minutes. If a horse on the roundabout originally faces north, in which direction does it end up facing?

A. The roundabout rotates through $10 \times 135 = 1350$ degrees. But $1350 = 270 + 3 \times 360$, so the horse faces the direction 270° anticlockwise from north, i.e. east.

In each example, we ignored any part of the number that produced no change (adding complete days or turns respectively). We were interested only in the *remainder*.

More generally, given any two integers x, y, we can add them or multiply them *modulo* n to give an answer between 0 and $n-1$, as follows.

$$x + y (\text{mod } n) = x +_n y = x + y - n \left[\frac{x+y}{n} \right]$$

$$x \cdot_n y = xy - n \left[\frac{xy}{n} \right]$$

e.g.

$$\begin{aligned} 0 +_{24} 100 &= 100 - 24 \left[\frac{100}{24} \right] \\ &= 100 - 24 \times 4 \\ &= 4. \end{aligned}$$

$$\begin{aligned} 10 \cdot_{360} 135 &= 1350 - 360 \times \left[\frac{1350}{360} \right] \\ &= 1350 - 360 \times 3 \\ &= 270. \end{aligned}$$

It can be shown that addition and multiplication modulo n satisfy the same axioms as ordinary addition and multiplication.

Exercise: Prove that addition and multiplication modulo n are associative.

Definition:

We say that x is congruent to $y \pmod{n}$ and write

$$x \equiv y \pmod{n}$$

if $x - y$ is an integer multiple of n.

Examples:

$$\begin{aligned} 100 &\equiv 4 \pmod{24} \\ 1350 &\equiv 270 \pmod{360} \\ -3 &\equiv 1 \pmod{2} \end{aligned}$$

The following identities hold modulo *every* $n \in \mathbb{N}$:

(i) $a \equiv a$

(ii) $a \equiv b$ iff $b \equiv a$

(iii) ($a \equiv b$ and $b \equiv c$) $\Rightarrow a \equiv c$.

(iv) ($a' \equiv a$ and $b' \equiv b$) $\Rightarrow$
$$\begin{aligned} a' + b' &\equiv a + b, \\ a' - b' &\equiv a - b, \\ a'b' &\equiv ab. \end{aligned}$$

(v) Let n have the factorization into primes

$$n = p_1^{e_1} \dots p_k^{e_k}.$$

Then $a \equiv b \pmod{n}$ iff $a \equiv b \pmod{p_i^{e_i}}$, $i = 1, \dots, k$.

(vi) $x + y = z \Rightarrow x + y \equiv z$.

Exercise: Prove each of the above.

By choosing n appropriately, we can derive some useful results about numbers.

Theorem:

If x is odd, $x^2 \equiv 1 \pmod{4}$.

If x is even, $x^2 \equiv 0 \pmod{4}$.

Proof:

If x is odd, $\exists\ k \in \mathbb{Z}$ such that $x = 2k + 1$.

$\therefore \quad x^2 = (2k+1)^2 = 1 + 4(k^2 + k) \equiv 1 \pmod{4}$.

If x is even, $\exists\ k \in \mathbb{Z}$ such that $x = 2k$.

$\therefore \quad x^2 = 4k^2 \equiv 0 \pmod{4}$.

Theorem: If x is not divisible by 5 then

$$x^4 \equiv 1 \pmod 5 \ .$$

Proof:

$$\begin{aligned}
x \equiv 1 \pmod 5 \quad &\Rightarrow \ x^2 \equiv 1 \times 1 \equiv 1 \Rightarrow x^4 \equiv 1 \times 1 \equiv 1 \\
x \equiv 2 \pmod 5 \quad &\Rightarrow \ x^2 \equiv 2 \times 2 \equiv 4 \Rightarrow x^4 \equiv 4 \times 4 \equiv 1 \\
x \equiv 3 \pmod 5 \quad &\Rightarrow \ x^2 \equiv 3 \times 3 \equiv 4 \Rightarrow x^4 \equiv 1 \\
x \equiv 4 \pmod 5 \quad &\Rightarrow \ x^2 \equiv 4 \times 4 \equiv 1 \Rightarrow x^4 \equiv 1
\end{aligned}$$

Definition: A *linear congruence* in one unknown variable x is an expression of the form

$$ax \equiv b \pmod n, \tag{4}$$

where a, b and n are given.

This is equivalent to the linear Diophantine equation

$$ax + ny = b.$$

We know that it has solutions iff $d = HCF(a, n)$ divides b. If $d|b$ then (4) is solved as follows.

If x_0 is a particular solution then the general solution is

$$x = x_0 + \frac{kn}{d},$$

where $k \in \mathbb{Z}$.

Therefore x is congruent to one of the following:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}.$$

In other words, there are d solutions between 0 and $n - 1$.

Examples:

(i) Solve $10x \equiv 3 \pmod{12}$.

Here $HCF(10, 12) = 2$ does not divide 3, so there are no solutions.

(ii) Solve $7x \equiv 3 \pmod{12}$

Here $HCF(7, 12) = 1$, so there is one solution between 0 and 11:

Note that $7 \times 9 = 63 = 3 + 5 \times 12$, so $x = 9$ is that solution.

The general solution is $x \equiv 9 \pmod{12}$.

(iii) Solve $10x \equiv 6 \pmod{12}$.

Here $HCF(10, 12) = 2$, so there are 2 solutions between 0 and 11:

Note that $10 \times 3 = 6 + 2 \times 12$ and $10 \times 9 = 6 + 7 \times 12$.

So the general solution is $x \equiv 3 \pmod{12}$ or $x \equiv 9 \pmod{12}$.

Equivalently $x \equiv 3 \pmod{6}$.

In the last example, we could have written

$$\begin{aligned} 10x + 12y &= 6 \\ \text{i.e. } 5x + 6y &= 3 \\ \text{i.e. } 5x &= 3 \pmod{6} \end{aligned}$$

whose solution is $x \equiv 3 \pmod{6}$.

More generally, if $d = HCF(a, n) > 1$ and $d|b$, let $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $n_1 = \frac{n}{d}$. Then

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

is equivalent to

$$a_1 x \equiv b_1 \pmod{n_1.}$$

So we can reduce any solvable linear congruence down to one for which a, n are coprime, so there is *one* solution (modulo n). One further simplification is possible.

Theorem: If $HCF(a, n) = 1$ and m divides a and b, let $a_1 = \frac{a}{m}$, $b_1 = \frac{b}{m}$. Then

$$ax \equiv b \text{ (mod n) iff } a_1 x \equiv b_1 \text{ (mod n) .}$$

Proof: $ax \equiv b \pmod{n}$ iff $\exists\, k \in \mathbb{Z}$ such that $ax - b = kn$.
But $ax - b = kn$ iff $a_1 x - b_1 = k_1 n$ where $k_1 = \frac{k}{m} \in \mathbb{Z}$, iff $a_1 x \equiv b_1 \pmod{n}$.
(As m divides kn and $1 \leq HCF(m, n) \leq HCF(a, n) = 1$, it follows that $HCF(m, n) = 1$, so m divides k.)

Example: The solution of
$12x \equiv 4 \pmod{22}$ is the solution of
$6x \equiv 2 \pmod{11}$, which is the solution of
$3x \equiv 1 \pmod{11}$.
This is $x \equiv 4 \pmod{11}$.

Simultaneous linear congruences

Just as we can solve simultaneous linear equations, we can also solve a set of linear congruences.

Theorem: (The Chinese Remainder Theorem)
Let $n_1, n_2, \ldots, n_k \in \mathbb{N}$ satisfy $HCF(n_i, n_j) = 1$ for all $i \neq j$, and let $a_1, \ldots, a_k \in \mathbb{Z}$. Then there is one solution of the simultaneous congruences

$$x \equiv a_1 \pmod{n_1}, \ldots, x \equiv a_k \pmod{n_k}$$

modulo $n = n_1 n_2 \ldots n_k$.

Proof:
We shall construct the solution, and show that it is unique (modulo n).
Let $c_i = \frac{n}{n_i}$. Note that the $HCF(c_i, n_i) = 1$ because each factor n_j of c_i is coprime to n_i.
So there is a unique solution of $c_i d_i \equiv 1$(modulo n_i) for each $i = 1, \ldots, k$.
Let $x_0 = a_1 c_1 d_1 + a_2 c_2 d_2 + \ldots a_k c_k d_k$.

Note that for each i, n_i divides every c_j with $j \neq i$,

$$\begin{aligned} \therefore \quad x_0 &\equiv a_i c_i d_i \pmod{n_i} \\ &\equiv a_i \pmod{n_i} . \end{aligned}$$

So x_0 satisfies the system of simultaneous congruences.

To show that this solution is unique (mod n), let x be any solution of the congruences.

Then $x \equiv a_i \equiv x_0 \pmod{n_i}$ for each i.

$$\therefore \quad n_i | (x - x_0) \text{ for each } i.$$

As the numbers n_i are coprime, their product n must divide $x - x_0$.

$$\therefore \quad x \equiv x_0 \pmod{n} .$$

Example

Solve $x \equiv a_1 \pmod 3$, $x \equiv a_2 \pmod 5$, $x \equiv a_3 \pmod 7$.

Solution:

Here $n = 3 \times 5 \times 7 = 105$.

$c_1 = 35$, $c_2 = 21$, $c_3 = 15$.

The solution of $35d_1 \equiv 1 \pmod 3$ is $d_1 \equiv 2 \pmod 3$

The solution of $21d_2 \equiv 1 \pmod 5$ is $d_2 \equiv 1 \pmod 5$

The solution of $15d_3 \equiv 1 \pmod 7$ is $d_3 \equiv 1 \pmod 7$

$\therefore x \equiv 70a_1 + 21a_2 + 15a_3 \pmod{105}$ is the solution of the simultaneous congruences.

The Chinese Remainder Theorem leads to a general strategy for solving simultaneous linear congruences whose moduli are mutually coprime:

(i) Solve each individual congruence to obtain a set of congruences of the form

$$x \equiv a_i \pmod{n_i}$$

(ii) Use the Chinese Remainder Theorem to obtain x that satisfies *all* of the congruences in (i).

Example:

Solve $3x \equiv 6 \pmod{12}$, $2x \equiv 5 \pmod{7}$, $3x \equiv 1 \pmod{5}$.

Solution:

Step (i):

The first of these is equivalent to $x \equiv 2 \pmod{4}$.

The second can be rewritten as $2x \equiv 12 \pmod{7}$

$$\therefore \quad x \equiv 6 \pmod{7}.$$

The third can be rewritten as $3x \equiv 6 \pmod{5}$

$$\therefore \quad x \equiv 2 \pmod{5}.$$

Step (ii):

Solve $x \equiv 2 \pmod{4}$, $x \equiv 2 \pmod{5}$, $x \equiv 6 \pmod{7}$.

Here $n_1 = 4$, $n_2 = 5$, $n_3 = 7$, so $n = 140$ and $c_1 = 35$, $c_2 = 28$, $c_3 = 20$.

$$\text{The solution of } 35d_1 \equiv 1 \pmod 4 \text{ is } d_1 \equiv 3 \pmod 4$$

$$\text{The solution of } 28d_2 \equiv 1 \pmod 5 \text{ is } d_2 \equiv 2 \pmod 5$$

$$\text{The solution of } 20d_3 \equiv 1 \pmod 7 \text{ is } d_3 \equiv 6 \pmod 7$$

Also $a_1 = 2$, $a_2 = 2$, $a_3 = 6$.

$$\begin{aligned} \therefore \quad x &\equiv 2 \times 35 \times 3 + 2 \times 28 \times 2 + 6 \times 20 \times 6 \pmod{140} \\ &\equiv 1042 \pmod{140} \\ &\equiv 62 \pmod{140} \end{aligned}$$

The theorems that we have proved so far can simplify the problem of solving a large non-prime congruence, by factorizing n, as the following example shows.

Example:

Solve $13x \equiv 71 \pmod{380}$.

Solution:

Note that $380 = 2^2 \times 5 \times 19$, so we must solve

$$\begin{aligned} 13x &\equiv 71 \pmod 4 , \qquad \text{i.e. } x \equiv 3 \pmod 4 \\ 13x &\equiv 71 \pmod 5 , \qquad \text{i.e. } 3x \equiv 1 \pmod 5 \\ 13x &\equiv 71 \pmod{19} , \qquad \text{i.e. } 13x \equiv 14 \pmod{19} \end{aligned}$$

The solution of $3x \equiv 1 \pmod 5$ is $x \equiv 2 \pmod 5$.

Note that $13x \equiv 14 \pmod{19}$ is equivalent to

$$-6x \equiv 14 \pmod{19}, \text{ i.e. } 3x \equiv -7 \pmod{19}.$$

This is equivalent to $3x \equiv 12 \pmod{19}$, $\therefore \quad x \equiv 4 \pmod{19}$.

So we must solve

$x \equiv 3 \pmod 4$, $x \equiv 2 \pmod 5$, $x \equiv 4 \pmod{19}$.

In the Chinese Remainder Theorem,

$n_1 = 4$, $n_2 = 5$, $n_3 = 19$, so $n = 380$,

$a_1 = 3$, $a_2 = 2$, $a_3 = 4$, $c_1 = 95$, $c_2 = 76$, $c_3 = 20$.

$95d_1 \equiv 1 \pmod 4$ reduces to $3d_1 \equiv 1 \pmod 4$,

so $d_1 \equiv 3 \pmod 4$.

$76d_2 \equiv 1 \pmod 5$ reduces to $d_2 \equiv 1 \pmod 5$

$20d_3 \equiv 1 \pmod{19}$ reduces to $d_3 \equiv 1 \pmod{19}$.

$$\begin{aligned} \therefore \quad x &\equiv 3 \times 95 \times 3 + 2 \times 76 \times 1 + 4 \times 20 \times 1 \pmod{380} \\ &\equiv 1087 \pmod{380} \\ &\equiv 327 \pmod{380}. \end{aligned}$$

Exercises:

(i) Solve $x \equiv 2 \pmod 7$, $x \equiv 7 \pmod 9$, $x \equiv 3 \pmod 4$.

(ii) Solve $7x \equiv 3 \pmod{12}$, $10x \equiv 6 \pmod{14}$.

(iii) Solve $91x \equiv 419 \pmod{440}$

The Chinese Remainder Theorem deals only with congruences that are mutually coprime. There is a fairly simple generalization to arbitrary congruences.

Theorem:

Let $n_1, \ldots, n_k \in \mathbb{N}$ and $a_1, \ldots, a_k \in \mathbb{Z}$. The simultaneous linear congruences

$$x \equiv a_i \pmod{n_i}, \quad i = 1, \ldots, k$$

have a solution iff for each $i \neq j$, $HCF(n_i, n_j)$ divides $a_i - a_j$. Where this condition is satisfied, the solution is unique modulo n, where n is the least common multiple of $n_1, \ldots, n_k$.

Note: If $n_1, .., n_k$ are mutually coprime, this theorem reduces to the Chinese Remainder Theorem.

We shall not prove this theorem (the proof is long), but the method of constructing the solution is as follows:

Step (i)

Write down the prime-power factorization of each n_i and thus write each $x \equiv a_i \pmod{n_i}$ as a set of congruences with prime-power moduli.

Step (ii)

Use the Chinese Remainder Theorem to solve only those congruences whose moduli are the *highest* power of each prime.

Example:

Solve $x \equiv 11 \pmod{36}$, $x \equiv 7 \pmod{40}$, $x \equiv 32 \pmod{75}$.

Solution:

First check that a solution exists:

$HCF(36, 40) = 4$, which divides 11-7=4.

$HCF(36, 75) = 3$, which divides 11-32=-21.

$HCF(40, 75) = 5$, which divides 7-32=-25.

So the conditions for a solution to exist are satisfied.

Now factorize the congruences.

$36 = 2^2 \times 3^2$, so $x \equiv 11 \pmod{2^2}$ and $x \equiv 11 \pmod{3^2}$

$40 = 2^3 \times 5$, so $x \equiv 7 \pmod{2^3}$ and $x \equiv 7 \pmod{5}$

$75 = 3 \times 5^2$ so $x \equiv 32 \pmod{3}$ and $x \equiv 32 \pmod{5^2}$.

So we must solve

$$x \equiv 7 \pmod{2^3}\ , x \equiv 11 \pmod{3^2}\ , x \equiv 32 \pmod{5^2}.$$

Note that all of the other congruencies are automatically satisfied - this always happens.

Equivalently, we must solve

$$x \equiv 7 \pmod{8}\ , x \equiv 2 \pmod{9}, x \equiv 7 \pmod{25}.$$

In the Chinese Remainder Theorem, we have

$a_1 = 7$, $a_2 = 2$, $a_3 = 7$

$n_1 = 8$, $n_2 = 9$, $n_3 = 25$, $\quad \therefore \quad n = 1800.$

$\therefore \quad c_1 = 225$, $c_2 = 200$, $c_3 = 72.$

$225d_1 \equiv 1 \pmod{8}$ reduces to $d_1 \equiv 1 \pmod{8}$

$200d_2 \equiv 1 \pmod{9}$ reduces to $2d_2 \equiv 1 \pmod{9}$

$$\therefore \quad 2d_2 \equiv 10 \pmod{9} \ \therefore d_2 \equiv 5 \pmod{9}.$$

$72d_3 \equiv 1 \pmod{25}$ reduces to $-3d_3 \equiv 1 \pmod{25}$

$$\therefore \quad 3d_3 \equiv 24 \pmod{25} \qquad \therefore d_3 \equiv 8 \pmod{25}.$$

$$\begin{aligned} \therefore \quad x &\equiv 7 \times 225 \times 1 + 2 \times 200 \times 5 + 7 \times 72 \times 8 \pmod{1800} \\ &\equiv 7607 \pmod{1800} \\ &\equiv 407 \pmod{1800} \end{aligned}$$

Exercises:

(i) Solve $x \equiv 1 \pmod 6$, $x \equiv 5 \pmod{14}$, $x \equiv 19 \pmod{21}$

(ii) A gang of eight thieves steal 500 gold bars. The leader immediately claims some of them and leaves the others to split the remainder equally between them. Unfortunately they have one bar too few, a fight breaks out, and one of the gang is killed. Now they have two bars left over, so they fight and another is killed. This improves things slightly - only one bar is left over. After one more death, they share out the bars equally. How many did the leader take?

Congruences with a prime modulus

Now we examine congruences (mod p), where p is prime. We already know that

$$ax - b \equiv 0 \pmod{p}$$

has:

$$\begin{aligned} \text{one solution (mod } p\text{) if } HCF(a,p) &= 1 \\ \text{no solutions if } HCF(a,p) &= p \text{ and } \frac{b}{p} \notin \mathbb{Z} \\ p \text{ solutions (mod } p\text{) if } HCF(a,p) &= p \text{ and } \frac{b}{p} \in \mathbb{Z}. \end{aligned}$$

In the last case, p divides both a and b, i.e. $a \equiv 0 \pmod{p}$ *and* $b \equiv 0 \pmod{p}$. Otherwise, there is at most *one* solution (mod p) to the linear congruence.

This result can be generalized to all polynomials, as follows.

Theorem: Let p be prime and let

$$f(x) = a_k x^k + \ldots + a_1 x + a_0,$$

where $a_i \in \mathbb{Z}$, $\forall\ i = 0, \ldots, k$, and p does not divide every a_i. Then

$$f(x) \equiv 0 \pmod{p}$$

has at most k solutions (mod p).

Proof: Use induction on k.

Base step: if $k = 0$, then $f(x) = a_0$ where p does not divide a_0. Thus there are no solutions of $f(x) \equiv 0 \pmod{p}$.

Induction hypothesis: Suppose that the result is true for all polynomials of order $k \leq K$.

Induction step: Let $k = K + 1$.

If $f(x) \equiv 0$ has no solutions, the result is true for $k = K + 1$. Therefore we need only look at the case when $f(x) \equiv 0$ has at least one solution. Let $x = x_0$ be such a solution.

$$\therefore \quad p \text{ divides } f(x_0).$$

Note that

$$\begin{aligned} f(x) - f(x_0) &= \sum_{i=0}^{K+1} a_i(x^i - x_0^i) \\ &= \sum_{i=1}^{K+1} a_i(x^i - x_0^i). \end{aligned}$$

For each i,

$$x^i - x_o^i = (x - x_0)(x^{i-1} + x^{i-2}x_0 + \ldots + xx_0^{i-2} + x_0^{i-1}).$$

So $x - x_0$ divides $f(x) - f(x_0)$, i.e. $\exists$ a polynomial $g(x)$ of order K such that

$$f(x) = f(x_0) + (x - x_0)g(x) \equiv (x - x_0)g(x) \pmod{p} .$$

As p does not divide all coefficients of $f(x)$, it cannot divide all coefficients of $g(x)$. By the induction hypothesis, there are $\leq K$ solutions of $g(x) \equiv 0 \pmod{p}$. So the only solutions of $f(x) \equiv 0 \pmod{p}$ are $x \equiv x_0 \pmod{p}$ and the solutions of $g(x) \equiv 0 \pmod{p}$. This makes $\leq K + 1$ solutions in total, so the theorem holds.

The contrapositive of the previous theorem is also useful:

Theorem: Let p be prime and let $f(x) = a_k x^k + \ldots + a_1 x + a_0$, where each $a_i \in \mathbb{Z}$. Then if $f(x) \equiv 0 \pmod{p}$ has more than k solutions $\pmod{p}$ it follows that

$$a_i \equiv 0 \pmod{p}, \quad i = 1, \ldots, k.$$

One of the most useful theorems in number theory enables us to reduce high-order polynomials:

Theorem: (Fermat's Little Theorem)
If p is prime and $x \not\equiv 0 \pmod{p}$ then

$$x^{p-1} \equiv 1 \pmod{p}.$$

Proof: If $x \not\equiv 0 \pmod{p}$ then $ax \equiv bx \Rightarrow a \equiv b$.

$\therefore$ $x, 2x, \ldots, (p-1)x$ are distinct numbers $\pmod{p}$, none of which is congruent to 0.

In other words, they are congruent to the numbers $1, 2, \ldots, p-1$ (but not necessarily in that order).

$\therefore$ $x \times 2x \times \ldots \times (p-1)x \equiv 1 \times 2 \times \ldots \times (p-1) \pmod{p}$

$$\text{i.e. } (p-1)! x^{p-1} \equiv (p-1)! \pmod{p}.$$

As p is coprime to every factor of $(p-1)!$, this congruence reduces to

$$x^{p-1} \equiv 1 \pmod{p}.$$

Example:

If $p = 5$ and $x = 3$ then

$$x \equiv 3, \quad 2x \equiv 1, \quad 3x \equiv 4, \quad 4x \equiv 2,$$

so $4!x^4 \equiv 4! \pmod{5}$, i.e.

$$x^4 \equiv 1 \qquad \pmod{5}.$$

By direct calculation, $3^4 = 81 = 1 + 16 \times 5$, so $3^4 \equiv 1 \pmod{5}$.

Whilst Fermat's Little Theorem applies only if $x \not\equiv 0 \pmod{p}$, we can easily derive a corollary that applies to all x:

Corollary: If p is prime than $x^p \equiv x \pmod{p}$ $\forall\, x \in \mathbb{N}$.

Proof: If $x \not\equiv 0 \pmod{p}$ the result comes directly from

Fermat's Little Theorem. If $x \equiv 0 \pmod{p}$ then $x^p \equiv 0 \pmod{p}$.

Fermat's Little Theorem and its corollary can be used to calculate congruences with large powers.

Example: Find the least nonnegative integer congruent to $2^{68} \pmod{19}$.

Solution: As $2 \not\equiv 0 \pmod{19}$, then $2^{18} \equiv 1 \pmod{19}$.

$$\begin{aligned} \therefore \qquad 2^{68} = 2^{14+3\times 18} &\equiv 2^{14} \qquad \pmod{19} \\ &\equiv 2^2 \times (2^4)^3 \\ &\equiv 4 \times (-3)^3 \\ &\equiv (-3) \times 36 \\ &\equiv (-3) \times (-2) \equiv 6 \end{aligned}$$

Example: Show that $x^{25} - x$ is divisible by 30 for every integer x.

Solution: We shall show that $x^{25} - x$ is divisible by 5,3 and 2.

Use the corollary, as this does not put restrictions on x.

$$\begin{aligned} x^{25} - x = (x^5)^5 - x &\equiv x^5 - x \pmod 5 \\ &\equiv x - x \equiv 0 \pmod 5 \end{aligned}$$

$$\begin{aligned} x^{25} - x = x(x^3)^8 - x &\equiv xx^8 - x \pmod 3 \\ \equiv (x^3)^3 - x &\equiv x^3 - x \\ \equiv x - x &\equiv 0 \pmod 5. \end{aligned}$$

If x is odd, so is x^{25}, so $x^{25} - x \equiv 0 \pmod 2$.

If x is even, so is x^{25}, so $x^{25} - x \equiv 0 \pmod 2$.

Exercises:

(i) Find the least nonnegative integer congruent to $3^{91} \pmod{23}$.

(ii) Solve $f(x) = x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \pmod 5$.

It is easy to use the corollary to test whether a given number n is prime. Pick $x \in \mathbb{N}$ and work out $x^n \pmod n$. If this is not congruent to $x \pmod n$ then n is not prime. The simplest choice is $x = 2$. Every non-prime number below 341 has $2^n \not\equiv 2 \pmod n$. However, $2^{341} \equiv 2 \pmod{341}$ even

though $341 = 31 \times 11$ is not prime. Any number passing the $x = 2$ test is called a pseudoprime, so 341 is the smallest non-prime pseudoprime.

However, the $x = 3$ test reveals that 341 is not prime, because $3^{341} \not\equiv 3 \pmod{341}$.

It is *not* true that every non-prime number fails the test for some x. Composite numbers that pass the test for every x are called Carmichael numbers. There are infinitely many of these; the smallest is $561 = 3 \times 11 \times 17$.

Fermat's Little Theorem and its corollary do not guarantee that a number is prime. The following theorem does.

Theorem: (Wilson's Theorem)
A number n is prime iff $(n-1)! \equiv -1 \pmod{n}$.

Proof: Suppose that n is prime.
If $n = 2$ then $(n-1)! = 1 \equiv -1 \pmod{2}$.
Otherwise, n is odd, and so the polynomial

$$f(x) = (1-x)(2-x)\ldots(n-1-x) + 1 - x^{n-1}$$

is of degree $k < n-1$, because the x^{n-1} terms cancel.

If $x \in \{1, 2, \ldots, n-1\}$ then

$$f(x) = 1 - x^{n-1} \equiv 0 \pmod{n}$$

by Fermat's Little Theorem.

So $f(x)$ has more than k roots and hence, if we write

$$f(x) = \sum_{i=0}^{k} a_i x^i,$$

every $a_i \equiv 0 \pmod{n}$.

In particular, $a_0 = (n-1)! + 1$, so

$$(n-1)! \equiv -1 \pmod{n}$$

Conversely, suppose that $n \in \mathbb{N}$ satisfies

$$(n-1)! \equiv -1 \pmod{n}.$$

If $d|n$ then

$$(n-1)! \equiv -1 \pmod{d}.$$

If $d \neq n$, then d is a factor of $(n-1)!$ and so

$$0 \equiv -1 \pmod{d}.$$

i.e. $d = 1$. So we have shown that if $d|n$ then either $d = n$ or $d = 1$. In other words, n is prime.

Exercise: Prove that n is prime iff $(n-2)! \equiv 1 \pmod{n}$.

To finish the section on number theory, we shall construct the general solution of

$$x^2 + y^2 = z^2$$

where $x, y, z \in \mathbb{N}$.

First note that if d divides any two of x, y, z, it divides the third. For example, if $x = dx_1$, $z = dz_1$ then

$$y^2 = d^2(z_1^2 - x_1^2) \qquad \therefore \quad d|y.$$

For the time being, assume that x, y, z are mutually coprime (we will put back a common factor d at the end). In particular, no two of x, y, z are even. Recall that

$$x^2 \equiv \begin{cases} 0 \pmod{4}, & \text{if } x \text{ is even} \\ 1 \pmod{4}, & \text{if } x \text{ is odd.} \end{cases}$$

So the only way to satisfy $x^2 + y^2 \equiv z^2 \pmod{4}$ is if z is odd and one of x, y is odd, the other is even.

Without loss of generality, let x be odd and y be even.

So $y = 2n$ for some $n \in \mathbb{N}$.

$$\therefore \quad 4n^2 = y^2 = z^2 - x^2 = (z+x)(z-x)$$

$$\therefore \quad n^2 = \left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right).$$

If $HCF\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = a$ then

$$a \quad \text{divides } \left(\frac{z+x}{2}\right) + \left(\frac{z-x}{2}\right) = z$$

and

$$a \quad \text{divides } \left(\frac{z+x}{2}\right) - \left(\frac{z-x}{2}\right) = x.$$

As $HCF(x, z) = 1$ it follows that $a = 1$.

Therefore $\exists\, p, q \in \mathbb{N}$ such that

$$\frac{z+x}{2} = p^2, \qquad \frac{z-x}{2} = q^2 \qquad \text{and } n = pq.$$

Note that $p^2 = q^2 + x$, so $p > q$.

Also $HCF(p^2, q^2) = 1$, so $HCF(p, q) = 1$.

Having found that

$$x = p^2 - q^2, \qquad y = 2pq, \qquad z = p^2 + q^2$$

s every solution for which x, y, z are mutually coprime, we can write down the general solution

$$x = d(p^2 - q^2), \qquad y = 2dpq, \qquad z = d(p^2 + q^2).$$

Examples:

(with $d = 1$ in the above formula)

p	2	3	3	4	4	...	100	...
q	1	1	2	1	3	...	51	...
x	3	8	5	15	7	...	7399	...
y	4	6	12	8	24	...	10200	...
z	5	10	13	17	25	...	12601	...

Note that if p, q are both odd then $p^2 - q^2$, $2pq$ and $p^2 + q^2$ are all even, so that as well as requiring $p > q$ and $HCF(p, q) = 1$, we need $p + q \equiv 1 \pmod 2$.

Exercise:

Show that the above conditions are all that are required to ensure that $x = p^2 - q^2$, $y = 2pq$ and $z = p^2 + q^2$ are mutually coprime.

Permutations

A permutation of a set of objects is a rearrangement of the objects. More precisely,

Definition: A **permutation** of a set X is a bijection from X to itself; this bijection is often written as

$$\pi : X \to X.$$

We can write the effect of the permutation on a *finite* set X as a two-row array. The first row denotes each object $x \in X$; underneath is the image of each x under the permutation: If $X = \{x_1, x_2, x_3, \ldots, x_k\}$ then the array is

$$\begin{bmatrix} x_1 & x_2 & x_3 & \ldots & x_k \\ \pi(x_1) & \pi(x_2) & \pi(x_3) & \ldots & \pi(x_k) \end{bmatrix}$$

For example, let $X = \{a, b, c\}$ and let π be the permutation that exchanges b and c. This is

$$\begin{bmatrix} a & b & c \\ a & c & b \end{bmatrix}$$

The composition of two successive permutations is a permutation. (Recall: if $\phi : A \to B$ and $\psi : B \to C$ are bijections, then $\psi \circ \phi : A \to C$ is a bijection).

There are only two possible permutations of two objects:

$$\begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix} \text{ and } \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

There are $3! = 6$ permutations of three objects:

$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$
$$\begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

More generally, there are $n!$ permutations of n objects:

There are	n	places in which the first object can go
	$n-1$	remaining places for the second object
	$\vdots$	
	1	remaining place for the nth object.

A useful shorter notation uses *cycles* (or *cyclic permutations*). Ignore any object which is unchanged, i.e. for which $\pi(x) = x$. Take the first object x for which $\pi(x) \neq x$, and write (within parentheses) the cycle

$$(x \quad \pi(x) \quad \pi(\pi(x)) \quad \dots \quad \pi^{-1}(x))$$

Note that $\pi(\pi^{-1}(x)) = x$, so we return to the beginning of the cycle. Repeat this process with any elements that have not been used, until every element that changes has been written down.

Examples:

(i)

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 8 & 9 & 3 & 6 & 2 & 7 & 5 & 4 \end{bmatrix} = (2 \quad 8 \quad 5 \quad 6)(3 \quad 9 \quad 4)$$

(ii)

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 6 & 7 & 3 & 5 & 4 & 2 \end{bmatrix} = (1 \quad 8 \quad 2)(3 \quad 6 \quad 5)(4 \quad 7)$$

The *trivial* permutation, for which $\pi = id$ (i.e. $\pi(x) = x$, $\forall\, x \in X$), is denoted by ε.

Therefore the permutations of $\{1, 2\}$ are ε and $(1 \quad 2)$. The permutations of $\{1, 2, 3\}$ are

$$\varepsilon, \quad (1 \quad 2 \quad 3), \quad (1 \quad 3 \quad 2), \quad (2 \quad 3), \quad (1 \quad 2), \quad (1 \quad 3).$$

Exercise: Write down all permutations of $\{1, 2, 3, 4\}$ in cycle notation.

If π_1 and π_2 are permutations then their product $\pi_1 \circ \pi_2$ consists of applying π_2 first, then applying π_1 to the result. The same idea carries over to products of any number of permutations.

Examples:

(i) If π_1 produces $(1 \quad 2)$ and π_2 produces $(1 \quad 3)$ then $\pi_1 \circ \pi_2$ sends

$$1 \overset{\pi_2}{\longmapsto} 3 \overset{\pi_1}{\longmapsto} 3 \qquad \pi_1 \text{ does not change } 3$$

$$3 \overset{\pi_2}{\longmapsto} 1 \overset{\pi_1}{\longmapsto} 2$$

$$2 \overset{\pi_2}{\longmapsto} 2 \overset{\pi_1}{\longmapsto} 1 \qquad \pi_2 \text{ does not change } 2$$

So $\pi_1 \circ \pi_2$ is the permutation $(1 \quad 3 \quad 2)$.

In short, $(1 \quad 2)(1 \quad 3) = (1 \quad 3 \quad 2)$.

More generally, $(c \quad a)(c \quad b) = (c \quad b \quad a)$.

Note that $(1 \quad 3)(1 \quad 2) = (1 \quad 2 \quad 3) \neq (1 \quad 2)(1 \quad 3)$.

(ii) $(c \quad a)(c \quad b)(c \quad a) = (c \quad b \quad a)(c \quad a) = (a \quad b)$.

(Note: $c \mapsto a \mapsto c, \qquad a \mapsto c \mapsto b, \qquad b \mapsto c \mapsto a$).

(iii)

$$(1 \quad 2 \quad 3 \quad 4)(1 \quad 2)(4 \quad 3 \quad 2 \quad 1) = (2 \quad 3)$$

$$(1 \quad 2 \quad 3 \quad 4)(2 \quad 3)(4 \quad 3 \quad 2 \quad 1) = (3 \quad 4)$$

$$(1 \quad 2 \quad 3 \quad 4)(3 \quad 4)(4 \quad 3 \quad 2 \quad 1) = (4 \quad 1)$$

$$(1 \quad 2 \quad 3 \quad 4)(4 \quad 1)(4 \quad 3 \quad 2 \quad 1) = (1 \quad 2)$$

(iv)

$$\begin{aligned} & (1 \quad 2 \quad 4)(3 \quad 5 \quad 7 \quad 9)(1 \quad 3 \quad 9)(2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 8) \\ = \ & (1 \quad 5 \quad 6 \quad 8 \quad 4 \quad 7 \quad 9 \quad 2 \quad 3) \end{aligned}$$

The set of all permutations of n objects is denoted by S_n. The simplest nontrivial permutations exchange two elements; these are called *transpositions*.

Theorem:

Every permutation $\pi \in S_n$ can be written as a product of transpositions.

Proof:

Every permutation is a product of cycles. A cycle containing k elements can be written as a product of transpositions as follows:

$$(a_1 \quad a_2 \quad \ldots \quad a_k) = (a_1 \quad a_k)(a_1 \quad a_{k-1}) \ldots (a_1 \quad a_3)(a_1 \quad a_2).$$

[Note: we have not missed out the trivial transposition, because $\varepsilon = (1 \quad 2)(1 \quad 2)$].

Theorem:

Every permutation $\pi \in S_n$ can be written as a product of the $(n-1)$ transpositions

$$(1 \quad 2), (1 \quad 3), \ldots, (1 \quad n).$$

Proof:

Every transposition $(a \quad b)$ can be written as $(1 \quad a)(1 \quad b)(1 \quad a)$ if neither a nor b is 1. Otherwise, $(a \quad 1) = (1 \quad a)$ and $(1 \quad b)$ is already in the required form.

Definition: The **parity** of a permutation $\pi \in S_n$ is:
even, if π is a product of an even number of transpositions
odd, if π is a product of an odd number of transpositions.

The product of two permutations has parity:
odd, if one is odd and the other is even
even, otherwise.

In particular, the product of any two even permutations is even.

Exercise: Write $(3 \quad 4 \quad 2 \quad 1)$ as a product of as few of $\{(1 \quad 2), (1 \quad 3), (1 \quad 4)\}$ as possible. What is its parity?

Solution:

$(3 \quad 4 \quad 2 \quad 1) = (1 \quad 3 \quad 4 \quad 2) = (1 \quad 2)(1 \quad 4)(1 \quad 3)$, which is odd.

Order relations:

Throughout this module, we have repeatedly used the fact that integers can be arranged in order $\ldots -1 < 0 < 1 < 2 \ldots$. For natural numbers, this ordering means that $\mathbb{N}$ has a least element (which is the starting-point for proof by induction). We have also used the *highest* common factor and *least* common multiple. We now show that these ideas are well-founded.

Definition: A **partial order**, denoted $\leq$, on a set S is a relation between elements of S, with the following properties:

(i) $a \leq a, \qquad \forall\, a \in S$;

(ii) ($a \leq b$ and $b \leq a$)$\Rightarrow a = b$;

(iii) ($a \leq b$ and $b \leq c$)$\Rightarrow a \leq c$.

Definition: A **partially ordered set** (or **poset**) is a set S on which a partial order is defined.

Examples:

(i) $S = \mathbb{Z}$, where $\leq$ is the usual "less than or equal to" ordering. The same ordering also works for $\mathbb{N}$, $\mathbb{Q}$ and $\mathbb{R}$, but *not* for $\mathbb{C}$.

(ii) Let $X = \{a, b, c\}$ and let $S = \mathcal{P}(X)$. Define $\leq$ by

$$A \leq B \quad \text{iff } A \subset B.$$

For instance $\{a\} \leq \{a, c\} \leq \{a, b, c\}$.

Note that, unlike the previous example, we cannot relate every pair of elements of S by $\leq$. For instance neither $\{a, b\} \leq \{a, c\}$ nor $\{a, c\} \leq \{a, b\}$ is true.

Definition: A **totally ordered set** is a poset S such that for each $x, y \in S$, either $x \leq y$ or $y \leq x$ is true. (Note: both are true iff $x = y$).

Example:

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ are all totally ordered by $\leq$.

Definition: A **well-ordered** set is a totally ordered set S in which every nonempty subset A has a least element. In other words

$$((A \subset S)_{\wedge}(A \neq \emptyset)) \Rightarrow \exists\ a \in A \text{ such that } a \leq b, \quad \forall\ b \in A.$$

Example: $\mathbb{N}$ is well-ordered; $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ are not.

We used the fact that $\mathbb{N}$ is well-ordered to prove theorems by induction. The following theorem shows that well-ordering on $\mathbb{N}$ is equivalent to both induction and strong induction.

Theorem:

The following statements are logically equivalent:

1. $\mathbb{N}$ is well-ordered.

2. Suppose that $A \subset \mathbb{N}$, $1 \in A$ and

$$n \in A \Rightarrow n+1 \in A, \quad \forall\, n \in \mathbb{N}.$$

Then $A = \mathbb{N}$.

3. Suppose that $B \subset \mathbb{N}$, $1 \in B$, and

$$1, 2, \ldots, n \in B \Rightarrow n+1 \in B, \quad \forall n \in \mathbb{N}.$$

Then $B = \mathbb{N}$.

Proof:

We shall show that $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 1$.

$1 \Rightarrow 2$**:** If $\mathbb{N}$ is well-ordered, every nonempty $C \subset \mathbb{N}$ has a least element. Suppose that $A \subset \mathbb{N}$ satisfies the conditions of 2, and let $C = \mathbb{N} \setminus A$.

If $C \neq \emptyset$ then C has a least element $x \in C$.

Note that $x \neq 1$ because $1 \in A$.

So $x - 1 \in \mathbb{N}$ and hence $x - 1 \in A$, as x is the least element of C.

But $x - 1 \in A \Rightarrow (x - 1) + 1 = x \in A, \quad \therefore \quad x \notin C$.

This contradiction implies that $C = \emptyset$ and so $A = \mathbb{N}$.

$2 \Rightarrow 3$**:** Suppose that $B \subset \mathbb{N}$ satisfies the conditions of 3, and let $A = \{n \in \mathbb{N} : 1, 2, \ldots, n \in B\}$.

Clearly $A \subset \mathbb{N}$. As $1 \in B$, it follows that $1 \in A$.

Let $n \in A$, so that $1, 2, \ldots, n \in B$.

But

$$1, 2, \ldots, n \in B \Rightarrow n + 1 \in B,$$

and so $1, 2, \ldots, n, n + 1 \in B$. Therefore, $n + 1 \in A$.

In short, we have shown that $n \in A \Rightarrow n + 1 \in A$.

From statement 2 it follows that $A = \mathbb{N}$.

So $1, 2, \ldots, n \in B, \quad \forall\, n \in \mathbb{N}$.

In particular $n \in B, \quad \forall\, n \in \mathbb{N}$. Hence $B = \mathbb{N}$.

$3 \Rightarrow 1$**:** We show that if $C \subset \mathbb{N}$ has no least element then $C = \emptyset$. Suppose that C has no least element. Let $B = \mathbb{N} \setminus C$. Clearly $1 \in B$ (for otherwise C would have the least element 1). Moreover if $1, 2, \ldots, n \in B$ then $n+1 \in B$ (for otherwise C would have the least element $n+1$). Hence $B = \mathbb{N}$.

$\therefore \quad C = \emptyset$.

The principle of induction is:
If $P(1)$ is true and $P(n) \Rightarrow P(n+1)$, $\forall\, n \in \mathbb{N}$, then $P(n)$ is true $\forall\, n \in \mathbb{N}$.

This is equivalent to statement 2 in the previous theorem. To derive 2 from the principle of induction, let $P(n)$ be the statement "$n \in A$".
To derive the principle of induction from statement 2, let $A = \{n \in \mathbb{N} : P(n) \text{ is true}\}$.

In the same way, statement 3 is equivalent to the principle of strong induction.

Consequently "strong" induction really assumes nothing more than ordinary induction.