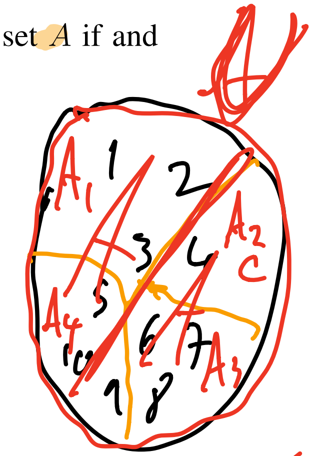
- Sets $A_1, A_2, \ldots, A_n$ are **mutually disjoint** (or **pairwise disjoint**) if and only if for all pairs of sets A_i and A_j with $i \neq j$, their intersection is empty; that is, if and only if $A_i \cap A_j = \emptyset$ for all $i, j = 1, 2, \ldots, n$ with $i \neq j$.

- A collection of non-empty sets $\{A_1, A_2, \ldots, A_n\}$ is a **partition** of a set A if and only if

  (1) $A = \boxed{A_1 \cup A_2 \cup \cdots \cup A_n}$ and $\bigcup_{i=1}^{n} A_i$

  (2) the sets $A_1, A_2, \ldots, A_n$ are mutually disjoint.



$A_i \cap A_j = \emptyset$

$i \neq j$

Example 24. *Determine whether the following statements are true or false.*

(a) $\emptyset = \{\emptyset\}$ F

(b) $A \cup \emptyset = A$ T

(c) $\boxed{A \cap A^c} = \emptyset$ T

(d) $A \cup A^c = \emptyset$ F

(e) $\boxed{A \cap \emptyset} = \emptyset$ T $A \cap (B^c \cap B)$

(f) $(A - B) \cap B = \emptyset$ T $\emptyset$

(g) $\{a, b, c\}$ *and* $\{d, e\}$ *are disjoint sets.* T

(h) $\{1, 2\}$, $\{5, 7, 9\}$ *and* $\{3, 4, 5\}$ *are mutually disjoint sets.* F

$\boxed{\bigcup A_i = A}$

Example 25. *Let*

$$A_1 = \{n \in \mathbb{Z} : n < 0\}, \qquad A_2 = \{n \in \mathbb{Z} : n > 0\}.$$

Is $\{A_1, A_2\}$ a partition of $\mathbb{Z}$? If so, explain why; if not, see if you can turn it into a partition with a small change.

Example 26. *Find a partition of $\mathbb{Z}$ into four parts such that none of the four parts is finite in size.*

Definition 9. *Given a set X, the* **power set** *of X is the set of all subsets of X. It is denoted by $\mathcal{P}(X)$.* 2^X

Example 27. *If $B = \boxed{\{1, 2, 3\}}$ write down the set $\mathcal{P}(B)$.* $= 2^B = \{\emptyset, \{1\}, \{2\}, \{3\}, \{2,3\}, \{1,2\}, \{1,3\}, \{1,2,3\}\}$

Example 28. *Let $X = \emptyset$. Write down $\mathcal{P}(X)$, and $\mathcal{P}(\mathcal{P}(X))$.*

If $|S| = n$, how many elements does the power set $\mathcal{P}(S)$ have?

$|2^B| = 2^{|B|}$

Subset relations

- For all sets A and B, $\quad A \cap B \subseteq A$ and $A \cap B \subseteq B$.

- For all sets A and B, $\quad A \subseteq A \cup B$ and $B \subseteq A \cup B$.

$A = \{\cancel{1}, \cancel{2}, \cancel{3}, 4, \cancel{5}, \dots, n\}$

$P(A) \equiv 2^{A} =$ Set of all subsets

$|2^{A}| = 2^{|A|}$

Binary numbers

$\underbrace{0001011001\dots1}_{n \text{ digits}}$

$\underbrace{2 \times 2 \times 2 \times \dots \times 2}_{n}$

$A \subset B$

$x \in A \Rightarrow x \in B$

$\boxed{\emptyset \subset B}$

$\cancel{x \in \emptyset}$ $\quad x \in B$

$\boxed{\emptyset} \leftarrow 00000\dots0$

$\underline{A \in 2^{B}} \Longleftrightarrow \underline{A \subset B}$

$A = \{-1, +1\}$

$2^A = \{\emptyset, \{-1\}, \{+1\}, \{-1, +1\}\}$

$\cancel{(2^{2^A})}\, B = 2^{(2^A)} = \wp(\wp(A))$

$|B| = 16$

$B = \{\emptyset, \{\emptyset\}, \{\{-1\}\}, \{\{+1\}\},$

$\cancel{\{-1, +1\}}$

$\}$

- For all sets A, B and C,

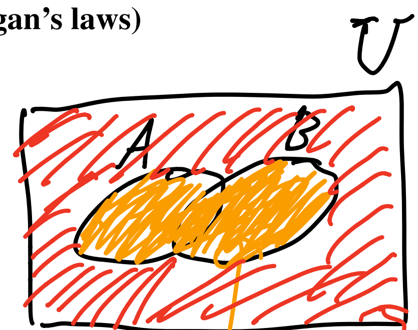
  if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

In the following, U denotes some universal set, and A, B and C are any subsets of U.

Set Identities

- $A \cup B = B \cup A$ and $A \cap B = B \cap A$. **(commutative)**
- $(A \cup B) \cup C = A \cup (B \cup C)$ and $(A \cap B) \cap C = A \cap (B \cap C)$. **(associative)**
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. **(distributive)**
- $A \cup \emptyset = A$; $A \cap U = A$; $A \cup A^c = U$; $A \cap A^c = \emptyset$; $(A^c)^c = A$; $A \cup A = A$; $A \cap A = A$.
- $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$. **(De Morgan's laws)**

Do yourself



To prove $X = Y$:

First show that $X \subseteq Y$, and then that $Y \subseteq X$.

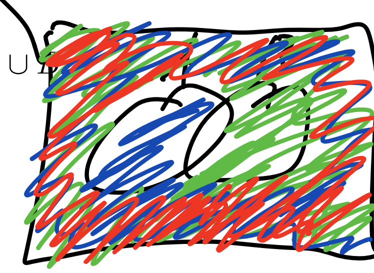
So take any x in X, and show that then $x \in Y$. This shows $X \subseteq Y$.

Next take any $y \in Y$, and show that then $y \in X$. This shows $Y \subseteq X$.

From these results we conclude that $X = Y$.

Note that: $(A \cap B)^c = A^c \cup B^c$ (one of De Morgan's laws).

Use De Morgan's law to show that: For all sets A and B, $(A \cap B)^c = A^c \cup B^c$



First, let $x \in (A \cap B)^c$. Then $x \notin A \cap B$.

So it is *false* that "x is in A and x is in B".

Thus $x \notin A$ or $x \notin B$ (since $\sim (p \wedge q) \Leftrightarrow (\sim p) \vee (\sim q)$).

So $x \in A^c$ or $x \in B^c$.

Therefore $x \in A^c \cup B^c$. This shows that $(A \cap B)^c \subseteq A^c \cup B^c$.

To complete this example, we must show that $A^c \cup B^c \subseteq A \cap B)^c$:

- Note that $(x, y) \in A \times B$ is equivalent to "$(x \in A)$ and $(y \in B)$".

Example 29. *If $A \subseteq C$ and $B \subseteq D$, prove that $A \times B \subseteq C \times D$.*

$$X = Y \iff \boxed{X \subseteq Y \text{ and } Y \subseteq X}$$

$a\in \quad a\in$

$b\in \quad b$

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

---

proof: $(A\cup B)^c \subseteq A^c \cap B^c$

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

$$\Downarrow$$

$$x \notin A\cup B$$

$$x \notin A \text{ and } x \notin B$$

$$\Downarrow \qquad \Downarrow$$

$$x \in A^c \text{ and } x \in B^c$$

$$\Downarrow$$

$$x \in A^c \cap B^c$$

Next Direction

$$\boxed{x \in A^c \cap B^c}$$

$$\Downarrow$$

$x \in A^c$ and $x \in B^c$

$\Downarrow \qquad \Downarrow$

$x \notin A$ and $x \notin B$

$$x \notin (A \cup B)$$

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

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

QED $\blacksquare$

$\mathbb{N}$ natural numbers $\{1, 2, 3, \ldots\}$

$\mathbb{N}_0$ $\{0, 1, 2, 3, \ldots\}$

2.2 Complex numbers

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$

You may have heard that it is not possible to take the square root of a negative number. This is false. More precisely,

$\boxed{i = \sqrt{-1}}$

> The square root of a negative number is not real; e.g. $\sqrt{-17} \notin \mathbb{R}$.

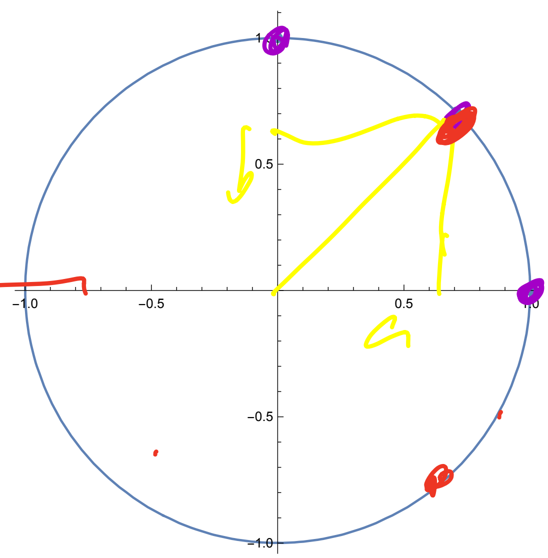
We deal with such numbers differently and refer to them as **imaginary numbers**. We use i to denote the square root of -1. For example, $\sqrt{-17} = \sqrt{17}i$, where $i^2 + 1 = 0$. A natural extension of the set of real numbers $\mathbb{R}$ is the set of **complex numbers**, $\mathbb{C}$, given by

$i \cdot i = -1$

$$\mathbb{C} = \{a + bi \ : \ a, b \in \mathbb{R}, i^2 + 1 = 0\}. \tag{2}$$

This is an extension of degree 2 over the real numbers, essentially meaning that this is structurally equivalent to the Cartesian product $\mathbb{R} \times \mathbb{R}$. To facilitate the description of complex numbers and their properties, we often represent these numbers geometrically as points in a 2-dimensional space with the real part of $z = a + bi$, a on the horizontal axis and the imaginary part b on the vertical axis. See Figure 13.

Im



Re

Figure 13: The complex plane where we plot $a + bi$, the circle $a^2 + b^2 = 1$, and the three complex numbers $1 + 0i$, $0 + 1i$, and $\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$, all on the unit circle.

Definition 10. *The modulus and argument of the complex number $z = a + bi$ are respectively $|z| = \sqrt{a^2 + b^2}$, the distance from 0 also the absolute value of z, and the angle θ between the position of the point (a, b) and the real axis. We denote $\Re(z) = a$ and $\Im(z) = b$, the real and imaginary parts of z respectively. The* **conjugate** *of $z = a + bi$ is $\overline{z} = a - bi$.*

Complex numbers have the following important properties among several more:

1. $z_1 = z_1$ if and only if $\Re(z_1) = \Re(z_2)$ and $\Im(z_1) = \Im(z_2)$;

$\mathbb{Z}$ integers

$$\mathbb{N} \subseteq \mathbb{Z}$$

$\mathbb{Q}$ Rational

$$x \in \mathbb{Q} \Longleftrightarrow \exists\, m, n \in \mathbb{Z} \text{ with } x = \frac{m}{n}$$

$n \neq 0$

There exist

$\frac{5}{3} \in \mathbb{Q}$

$\frac{10}{6} \in \mathbb{Q}$

$\sqrt{2} \notin \mathbb{Q}$

$\mathbb{R}$ reals

1.414

$z = a + bi$ $\quad$ $w = c + di$

complex #

$Re(z) = a$

Real numbers

$Im(z) = b$

$\boxed{z + w} = \boxed{a + bi} + c + di$

$= \boxed{a + c} + (b + d)i$

~~FOIL~~

$u = z \times w = (a + bi) \times (c + di)$

$= \boxed{ac + adi + bci + bdi^2}$

$z = a + bi$ $\quad$ $= \boxed{ac - bd + (ad + bc)i}$

$z \times \bar{z} = \boxed{a^2 + b^2}$ $\quad$ $(a + bi)(a - bi)$

$|z| = \sqrt{z\bar{z}}$

$\mathbb{R}$

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ $\sqrt{2}$

$\frac{1414}{1000}$

$x \in \mathbb{R} \setminus \mathbb{Q}$

irrational numbers

$\pi \neq \frac{c}{d}$

$\boxed{\mathbb{R} \setminus \mathbb{Q} \neq \emptyset}$

$\frac{1}{7} = 0.\boxed{142857}\boxed{142857}14\ldots \in \mathbb{Q}$

$x^2 = -1$

$\boxed{\begin{matrix} x = i \\ x = -i \end{matrix}}$ $i^2 = -1$

$(-i)(-i) = (-1 \times -1) \times i^2$
$= -1$

$x^2+1=0$

2. $z+\overline{z}=2\Re(z)$;

3. $z_1+z_2=z_2+z_1$ and $z_1z_2=z_2z_1$;

4. Euler's formula: If $r=|z|$ and θ is the argument of z, then $\boxed{z=re^{i\theta}}=\boxed{r\cos\theta}+\boxed{ir\sin\theta}$. This is also known as polar form.

$a+bi$

$re^{c\theta}$

An important result in algebra states essentially that are all we need when solving equations

$\boxed{f(x)=0}$

Theorem 4 (Fundamental theorem of algebra)**.** *Every non-constant polynomial $f(x)$ with complex coefficients has at least one complex root. Further, if the degree of $f(x)$ is equal to n, then there are exactly n such roots of $f(x)$, provided we count these as distinct when they are repeated.*

Example 30. *Find all of the roots in $\mathbb{C}$ of the polynomial $f(x)=x^5-3x^4-7x^3-13x^2-9x-5$ determine the number of such roots according to Theorem 4. How many real roots of $f(x)$ are there? Can $f(x)$ be factorised over $\mathbb{R}$? Express each of the complex roots of $f(x)$ in polar form.*

These x values are called roots.

Try in Mathematica.

2.3 Counting and elementary combinations

In this chapter we give an introduction to counting and probability. At first thought counting may seem a fairly simple exercise. However, when we are counting certain things it can turn out to be quite an involved process.

Counting subsets of a set: combinations

In this section we'll investigate questions of the following form.

> Given a set S with n elements, how many subsets of size r can be chosen from S?

- Let n and r be nonnegative integers with $r\leqslant n$. An r-**combination** of a set of n elements is a subset of the n elements of size r.

  The symbol $\binom{n}{r}$, which is read "n **choose** r," denotes the number of subsets of size r (so the number of r-combinations) which can be chosen from a set of n elements.

  Alternative notation for $\binom{n}{r}$ includes: $C(n,r)$, or ${}_nC_r$, or $C_{n,r}$, or ${}^nC_r$.

Theorem 5. *The number of subsets of size r (or r-combinations) which can be chosen from a set of n elements, $\binom{n}{r}$, is given by the formula*

$$\binom{n}{r}=\frac{P(n,r)}{r!}$$

or, equivalently,

$$\binom{n}{r}=\frac{n!}{r!(n-r)!}$$

where n and r are nonnegative integers with $r\leqslant n$.

$A = \{1, 2, \dots, n\}$ $|2^A| = 2^n = 2^{|A|}$

Balls into Bins

$n = 4$ Bins

$k = 2$ Balls

n bins / k balls	Limit of 1 ball max per bin	Unlimited
identical		
distinguished (different)	$n\cdot(n-1)(n-2)\cdots(n-k+1)$ $= 12$ $\frac{n!}{(n-k)!}$	$\le$ $\boxed{n^k}$ $= 16$

$= n!$ if $n=k$

$n(n-1)(n-2)\cdots 3\cdot 2\cdot 1$

$n!$

$n = 1000$

$k = 30$

!

$n = 4$
$k = 2$

$4 \cdot \ldots \cdot (4 - \cancel{2} + 1) = 4 \cdot 3$

$\frac{\boxed{n!}}{(n-k)!} = n\cdot(n-1)(n-2)\cdots(n-k+1)\cancel{(n-k)(n-k-1)\cdots 2\cdot 1}$

$x!$

$4! = 4\times3\times2\times1 = 24$

Factorial

$1! = 1$

$0! = 1$

Defined to be 1

~~$(n-1)(n-1-1)$~~ # of ways to organize

$\{1, 2, 3\}$

"permutations"

$3!\ 2!\ 1$

$\{1, \ldots, 10\}$

$10! = 3,628,800$

recursive

$$n! = \begin{cases} n\cdot(n-1)! & \text{if } n\geq 1 \\ 1 & n=0 \end{cases}$$

Mathematica

$\boxed{2.3!}$ Gamma[2.3+1]

Gamn[3.3]

$10! = 10\cdot\boxed{9\cdot8\cdot7\cdot6\cdot5\cdot4\cdot3\cdot2}$

$\boxed{\text{Gamma}(x) = \Gamma(x) = (x-1)!}$

for x integer

<u>Thm:</u> $\boxed{\mathbb{R} \setminus \mathbb{Q} \neq \emptyset.}$

<u>Proof:</u> We will show there are not $m, n \in \mathbb{Z}$ with $\sqrt{2} = \frac{m}{n}$ and m, n having no common factors. Hence $\sqrt{2} \notin \mathbb{Q}$. $\boxed{\text{But } \sqrt{2} \in \mathbb{R}}$

$\cancel{A} = \boxed{\sqrt{2}}$ $\quad$ $\boxed{\cancel{A}^2 = 2}$

$\cancel{A} > 0$

$\boxed{-\sqrt{2}}$

$\binom{n+k-1}{n-1}$

Q8 in ASS1

$n=6$
$k=3$

n bins \ k balls	Limit of 1	Unlimited
Same	$\dfrac{n!}{(n-k)!\,k!} = \dbinom{n}{k}$	$\dbinom{n+k-1}{k}$
Different	$\dfrac{n!}{(n-k)!} = \dbinom{n}{k}k!$	n^k

ABC
ACB
BAC
BCA
CAB
CBA

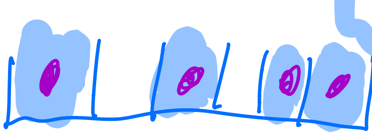
$3!$

a b c

$$\boxed{\binom{n}{k}} = \frac{n!}{(n-k)!\,k!}$$

Binomial Coefficient

$\binom{n}{k}$ with $n=1000$, $k=10$ $=$ # of subsets of size k (4) from a set of size n (6)



n box ~~k~~ balls

$$\boxed{2^n = \sum_{k=0}^{n} \binom{n}{k}}$$

$$2^6 = \binom{6}{0} + \binom{6}{1} + \binom{6}{2} + \binom{6}{3} + \binom{6}{4} + \binom{6}{5} + \binom{6}{6}$$

Algebra

$$(a+b)^2 = (a+b)(a+b)$$

$$= a^2 + 2ab + b^2$$

$$(a+b)^3 = \boxed{(a+b)(a+b)(a+b)}$$

$$= (a+b)(a^2 + 2ab + b^2)$$

$$= \binom{n}{0} a^3 b^0 + 3a^2b^1 + 3ab^2 + 1a^0b^3$$

$$\boxed{(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}}$$

$$\binom{3}{1} \quad \binom{3}{\;}$$

- An **ordered selection** of r elements from a set of n elements is an r-permutation of the set (use $P(n,r)$).
- An **unordered selection** of r elements from a set of n elements is the same as a subset of size r, or an r-combination of the set (use $\binom{n}{r}$).

Example 31. *Calculate the value of:*

(a) $\binom{9}{3}$;

(b) $\binom{200}{198}$;

(c) $\binom{8}{4}$.

Example 32. *A student has a maths assignment with five questions on it, but only has enough time to complete three of them. How many combinations of questions could the student complete?*

Example 33. *Imagine a word game in which a sentence has to be made using three words drawn out of a bag containing ten words.*

(a) How many possible ways are there to choose three words from a bag of ten words?

(b) Suppose that the rules of the game change so that the sentence has to use the three words in the order in which they are chosen. How many possible combinations are there now?

(c) What is the relationship between the answers to parts (a) and (b)?

Example 34. *In a game of straight poker, each player is dealt five cards from an ordinary deck of 52 cards, and each player is said to have a* 5*-card hand.*

(a) How many 5*-card poker hands contain four cards of the one denomination? (So e.g. four aces, or four threes, etc.)*

(b) Find the error in the following calculation of the number of 5*-card poker hands which contain at least one jack. Then calculate the true number of* 5*-card poker hands which contain at least one jack.*

Consider this in two steps:

Choose one jack from the four jacks.

Choose the other four cards in the hand.

Thus there are $\binom{4}{1}\binom{51}{4} = 999600$ *such hands.*

$A = \{1, 2, 3, 4, 5, 6\}$

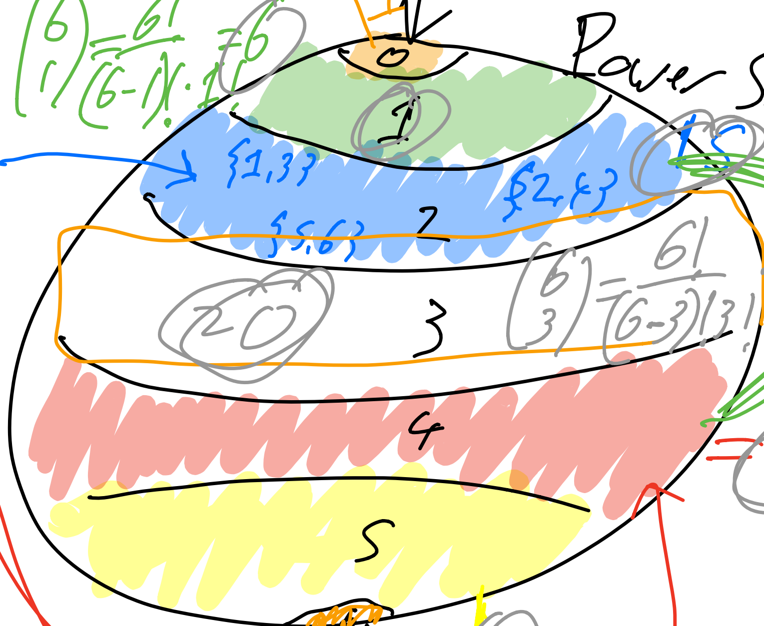
$n = |A| = 6.$

$|2^A| = 2^6 = 64$

$2^A = \{\phi, \ldots\ldots, A\}$

$\binom{n}{0} = \frac{n!}{(n-0)!\,0!} = 1$

$\binom{6}{1} = \frac{6!}{(6-1)!\cdot 1!} = 6$



$\binom{6}{2} = \frac{6!}{\boxed{(6-2)!}\,\boxed{2!}}$

$= \frac{6\cdot 5\cdot \cancel{4!}}{\cancel{4!}\,2!}$

$= 3\cdot 5 = 15$

$\binom{6}{3} = \frac{6!}{(6-3)!\,3!} = \frac{6\cdot 5\cdot 4}{3\cdot 2} = 20$

$\binom{6}{4} = \frac{6!}{\boxed{(6-4)!}\,\boxed{4!}} = 15$

$\binom{6}{6} = 1$

$$\boxed{\binom{n}{k} = \binom{n}{n-k}}$$

$$\frac{n!}{(n-k)!\,k!} = \frac{n!}{(n-\cancel{n}+k)!\,(n-k)!}$$

$\binom{n}{1} = n$

$\binom{n}{n-1} = n$

Assume $\boxed{\sqrt{2} = \frac{m}{n}}$ and

m and n have no common factors.

$n\sqrt{2} = m$

$\boxed{2n^2 = m^2}$

so m^2 is even.

Hence $\boxed{m \text{ is even}}$ ||| check

$m = 2k$

$\cancel{2}n^2 = (2k)^2 = \cancel{4}^{2}k^2$

$\boxed{n^2 = 2k^2} \Rightarrow n^2$ is even

Proof by negation.

21

$\mathbb{Z} = \text{Even} \cup \text{Odd}$

$\text{Even} \cap \text{Odds} = \emptyset$

Watch out for the common error of counting things twice.

We will now work with some useful relationships involving $\binom{n}{r}$.

n is even

Theorem 6. *Let n and r be positive integers with $r \leqslant n$. Then*

$$\binom{n}{r} = \binom{n}{n-r}.$$

Example 35. *Given that* $\binom{n}{2} = \dfrac{n(n-1)}{2}$, *find an expression for* $\binom{x+3}{x+1}$.

common factor of 2

Pascal's Formula Let n and r be positive integers with $r \leqslant n$. Then

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}. \quad (3)$$

Example 36. *Use Pascal's formula* (3) *to calculate:*

(a) $\binom{7}{5} + \binom{7}{6}$

(b) $\binom{9}{6} + \binom{9}{5}$

(c) $\binom{4}{2} + \binom{4}{3}$

(d) $\binom{6}{1} + \binom{6}{2}$

2.4 Cardinality

In this section we shall investigate the concept of the *cardinality* of a set and show that there are *infinite* sets that are larger than other infinite sets. This concept has applications in determining what can and what cannot be computed on a computer.

- A **finite** set is either one which has no elements at all, or one for which there exists a one-to-one correspondence (bijection) with a set of the form $\{1, 2, 3, \ldots, n\}$ for some fixed positive integer n.
- An **infinite** set is a nonempty set for which there does *not* exist any one-to-one correspondence (bijection) with a set of the form $\{1, 2, 3, \ldots, n\}$ for any positive integer n.
- Let $\mathcal{A}$ and $\mathcal{B}$ be any sets. Sets $\mathcal{A}$ and $\mathcal{B}$ are said to have the **same cardinality** if and only if there exists a one-to-one correspondence (bijection) from $\mathcal{A}$ to $\mathcal{B}$.

  In other words, $\mathcal{A}$ has the **same cardinality** as $\mathcal{B}$ if and only if there is a function f from $\mathcal{A}$ to $\mathcal{B}$ that is one-to-one (injective) and onto (surjective).

- A set is called **countably infinite** if and only if it has the same cardinality as the set of positive integers $\mathbb{Z}^+$.
- A set is called **countable** if and only if it is finite or it is countably infinite.

Example Consider: $f : \mathbb{Z} \mapsto \mathbb{Z}^2 \qquad f(x) = x^2$

Here we can see f is surjective but not injective, so not a bijection.

Example 37. *Show that the following is bijective:* $f : \mathbb{Z}^+ \mapsto \mathbb{Z}^2 \qquad f(x) = x^2$

Start by assuming $f(x_1) = f(x_2)$. Then $x_1^2 = x_2^2$, and taking square roots gives $x_1 = x_2$ since $\mathbb{Z}^+$ contains only positive integers. To show surjective, let $x^2 \in \mathbb{Z}^2$, then $x \in \mathbb{Z}^+$ and $f(x) = x^2$.

Example 38. *The sets* $\{1, 4, 5, 6, b\}$, $\mathbb{Z}^{>0}$, $\mathbb{Z}$, *and* $\mathbb{Q}$ *are all countable.*

- A set that is not countable is called **uncountable**.

Example 39. *The sets* $\mathbb{R}$, *and* $\mathcal{P}(\mathbb{Z}(>0))$ *are both uncountable.*

Example 40. *Show that the set of all odd integers is countable.*

Theorem 7. *Let* $\mathcal{X}$ *and* $\mathcal{Y}$ *be* **finite** *sets with the same number of elements, and suppose that* f *is a function from* $\mathcal{X}$ *to* $\mathcal{Y}$. *Then* f *is one-to-one if and only if* f *is onto.*

- This theorem does *not* hold for infinite sets of the same cardinality.

  In fact if $\mathcal{A}$ and $\mathcal{B}$ are infinite sets with the same cardinality, then there exist functions from $\mathcal{A}$ to $\mathcal{B}$ that are one-to-one and not onto, and functions from $\mathcal{A}$ to $\mathcal{B}$ that are onto and not one-to-one.

Example 41. *Given that* $\mathbb{Z}$ *has the same cardinality as the set of even integers,* $\mathbb{Z}^{even}$,

(a) *find a map from* $\mathbb{Z}^{even}$ *to* $\mathbb{Z}$ *that is one-to-one but not onto, and*

(b) *find a map from* $\mathbb{Z}$ *to* $\mathbb{Z}^{even}$ *that is onto but not one-to-one.*

Example 42. *Verify that the set* $\mathcal{P}(\mathbb{Z}^+)$ *is uncountable.*

2.5 Application: The set cover problem

$B = \boxed{\{\emptyset\}} \neq \emptyset$

$\mathbb{N} = \{1, 2, 3, 4, \ldots$

$= \{0, 1, 2, 3, 4, \ldots$

$x \in A$ $x \in A^c$

3 Foundations in logic

$A \cap A^c = \emptyset$

3.1 Proof methods

In this section we will focus on the basic structure of simple mathematical proofs, and see how to disprove a mathematical statement using a counterexample.

To illustrate these proof techniques we will use the properties of *even* and *odd* integers, and of *prime* and *composite* integers.

- An integer n is **even** if and only if n is equal to two times some integer.
- An integer n is **odd** if and only if n is equal to two times some integer plus 1.
- An integer n is **prime** if and only if $n > 1$, and for all positive integers r and s, if we have $n = r \cdot s$, then $r = 1$ or $s = 1$.
- An integer is **composite** if and only if $n > 1$, and $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.

Example 43. *Prove that for all* $x \in \{0, 1, 2, 3, 4, 5\}$, *the integer* $x^2 + x + 41$ *is a prime number.*

Method of Direct Proof:

To show that "$\forall x \in D$, if $P(x)$ then $Q(x)$" is **true**:

1. Suppose for a particular but *arbitrarily chosen* element x of D that the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
2. Show that the conclusion $Q(x)$ is true using definitions, previously established results, and the rules for logical inference.

Example 44. *Prove that for all integers* a, b, c *and* m, *if*

$$a - b = rm \quad \textit{and} \quad b - c = sm, \quad \textit{then} \quad a - c = tm$$

for some integers r, s *and* t.

The following are common **mistakes** that are often made in proofs; they should be avoided.

- Arguing from examples.
- Using the same letter to mean two different things.
- Jumping to a conclusion.
- Begging the question (assuming the thing you are trying to prove).