

## Introduction

This book is aimed at students studying A level or IB mathematics in their last year or two at school, teachers looking for ideas to stretch their bright students and anyone who enjoys mathematics and is looking for something interesting to read.

This is not a text book. It will not help you pass exams. The topics covered are not usually taught at school. But it will show you some of the breadth of mathematics from the first chapter where we see the difficulties in designing voting systems to the last chapter where we see that some infinite numbers are bigger than others.

Each chapter is short. It is just a starting point. If you find a chapter interesting then an internet search will give you lots more information about that topic. See Appendix 3.

You will need to think hard when reading this book. There are exercises (with solutions) for you to do. You will need a pencil, some paper and a waste-paper-basket.

The chapters cover different topics and you don't need to read them in order. Roughly speaking, the easier chapters are nearer the front of the book. If there is something you don't understand then just skip over it.

## A Nice Proof

### Theorem

$$1+2^1+2^2+2^3+\dots+2^n=2^{n+1}-1$$

### Proof

There are 64 competitors in a knock-out tennis tournament. How many matches will there be during this tournament?

#### Method 1

First round	32 matches	Second round	16 matches	Third round	8 matches
Fourth round	4 matches	Fifth round	2 matches	Sixth round	1 match

$$\text{Answer: } 1+2+4+8+16+32$$

#### Method 2

Each match knocks-out one competitor. By the end, 63 competitors have been knocked-out

$$\text{Answer: } 63$$

$$\text{Comparing our answers we have: } 1+2+4+8+16+32=63$$

In general:

$$1+2^1+2^2+2^3+\dots+2^n=2^{n+1}-1$$

A useful result and nothing to do with tennis.

## A Nice Sum

E	D	C	B	A
D	E	D	C	B
C	D	E	D	C
B	C	D	E	D
A	B	C	D	E

In the above table we have:

1 letter A, two letter B, three letter C, four letter D, five letter E, four letter D, three letter C, two letter B and one letter A.

How many letters have we got?

We have got  $1+2+3+4+5+4+3+2+1$  letters. But we have got  $5^2$  letters.

So  $1+2+3+4+5+4+3+2+1=5^2$

In general:

$$1+2+3+\dots+n+\dots+3+2+1=n^2$$

Now let's add up all the numbers in this table:

$1 \times 1$	$1 \times 2$	$1 \times 3$	$1 \times 4$
$2 \times 1$	$2 \times 2$	$2 \times 3$	$2 \times 4$
$3 \times 1$	$3 \times 2$	$3 \times 3$	$3 \times 4$
$4 \times 1$	$4 \times 2$	$4 \times 3$	$4 \times 4$

First method:

The numbers in the table add up to  $(1+2+3+4)^2$  (check by multiplying out the brackets)

Second method:

W	X	Y	Z
X	X	Y	Z
Y	Y	Y	Z
Z	Z	Z	Z

The number in the W cell:

$$1 \times 1 = 1$$

The numbers in the X cells:

$$(2 \times 1) + (2 \times 2) + (1 \times 2) = 2(1+2+1) = 2(2^2) = 2^3$$

The numbers in the Y cells:

$$(3 \times 1) + (3 \times 2) + (3 \times 3) + (2 \times 3) + (1 \times 3) = 3(1+2+3+2+1) = 3(3^2) = 3^3$$

The numbers in the Z cells:

$$(4 \times 1) + (4 \times 2) + (4 \times 3) + (4 \times 4) + (3 \times 4) + (2 \times 4) + (1 \times 4) = 4(1+2+3+4+3+2+1) = 4(4^2) = 4^3$$

So the numbers in the table add up to  $1^3 + 2^3 + 3^3 + 4^3$

So comparing our results using the first method and the second method:

$$(1+2+3+4)^2 = 1^3 + 2^3 + 3^3 + 4^3$$

In general:

$$(1+2+3+\dots+n)^2 = 1^3 + 2^3 + 3^3 + \dots + n^3$$

## Appendix 1

### A Few Short Programs – written in Python

1) Print the first 10 Fibonacci numbers

Program:

x=1

y=1

for j in range(1,9):

    z=x+y

    print(z)

    x=y

    y=z

Notes:

a) for j in range(1,9):

This means

Put j=1 and perform the indented statements

Put j=2 and perform the indented statements

...

Put j=8 and perform the indented statements

Confusingly, for j in range(1,9) means j=1, 2, ... 8 but not j=9

b) x=y

This means put x equal to the current value of y. So, for example

x=3

y=7

x=y

We now have x=7 and y=7

y=x     This means put y equal to the current value of x. So, for example

x=3

y=7

y=x

We now have x=3 and y=3

So x=y and y=x do not mean the same thing!

c) We can run this program by keeping track of the values of j, z, x, y and see what gets printed.

j	z	print	x	y
			1	1
1	2	2	1	2
2	3	3	2	3
3	5	5	3	5
4	8	8	5	8
5	13	13	8	13
...				

This program will print the 2<sup>nd</sup>, 3<sup>rd</sup>, 4<sup>th</sup>, ... 10<sup>th</sup> Fibonacci numbers which is almost what we wanted!

2) Use Euclid's algorithm to find the highest common factor of 3458 and 651

Program:

r=1

a=3458

b=651

while r!=0:

    r=a%b

    a=b

    b=r

print(a)

Notes:

a) while r!=0:

This means while r does not equal 0

Perform the indented statements

Perform the indented statements

... until r=0

Then continue with the rest of the program

When we start this while loop r has to have a value so we gave it a value in line 1

b)  $r=a \% b$

This means put r equal to the remainder when  $a$  is divided by  $b$ . So, for example

$a=17$

$b=5$

$r=a \% b$

We now have  $r=2$

c) We can run this program

r	a	b	print
1	3458	651	
203	651	203	
42	203	42	
35	42	35	
7	35	7	
0	7	0	7

d) We can change lines 2 and 3 to find the highest common factor of any two positive integers.

3) Test if 28 a perfect number

Program:

```
n=28  
c=0  
for j in range(1,n):  
    if n%j==0:  
        c=c+j  
    if c==n:  
        print("perfect")  
    else:  
        print("non-perfect")
```

Notes:

a) if  $n \% j == 0$ :

This means if the remainder when n is divided by j is zero

In other words, if j is a factor of n

We have to use == and not = in an if statement.

b)  $c=c+j$

This means c adds up all the factors of n

c) if  $c==n$ :

This means if the sum of the factors of n (including 1 but excluding n) is equal to n

In other words, if n is a perfect number

4) Test if 17 is a prime number

Program:

```
n=17  
prime=1  
for j in range(2,n):  
    if n%j==0:  
        prime=0  
        break  
print(p)
```

Notes:

a) Once we have run the program, prime=1 if m is a prime number and prime=0 if m is not a prime number.

b) if  $n \% j == 0$ :

This means if j is a factor of n

In other words, if n is not a prime number.

c) break

This means jump out of the for loop and continue with the rest of the program

d) We can make this program part of a larger program to print out all the prime numbers less than, say 100

for n in range(3,100):

    prime=1

    for j in range(2,n):

        if  $n \% j == 0$ :

            prime=0

            break

    if prime==1:

        print(n)

5) Test if 21 is the sum of two squares

Program:

N=21

flag=0

for j in range(0,N+1):

    for k in range(j,N+1):

        if  $N == j * j + k * k$ :

            flag=1

            break

print(flag)

Notes:

a) We set flag=0 at the start. We only enact flag=1 if N is the sum of two squares.

b) print(flag)

This means we print 1 if N is the sum of two squares. Otherwise we print 0.

c) try running this program by hand.

6) Calculate  $f(17)$  where  $f(x)=2x+7$

Program:

```
def f(x):
    return (2*x)+7
y=f(17)
print(y)
```

Notes:

Lines 1 and 2 define the function  $f(x)$ . We can put this at the start of the program and then refer to it later in the program.

7) Calculate  $u_{12}$  in the sequence  $u_1=3 \quad u_{n+1}=2u_n+3n$

Program:

```
def u(n):
    if n==1:
        return 3
    else:
        return 2*u(n-1)+3*(n-1)
t=u(12)
print(t)
```

Notes:

a) Line 3 tells us that  $u(1)=3$

Line 5 tells us that  $u(n)=2u(n-1)+3(n-1)$

$u_{n+1}=2u_n+3n$  and  $u_n=2u_{n-1}+3(n-1)$  mean the same thing.

For example, if we put  $n=7$  in the first version we get  $u_8=2u_7+21$  and if we put  $n=8$  in the second version we get  $u_8=2u_7+21$

8) Calculate the 10<sup>th</sup> derangement number using the recurrence relation

Remember  $D_1=0$  and  $D_2=1$  and  $D_{n+2}=(n+1)D_n+(n+1)D_{n+1}$

Program:

```
def D(n):
    if n==1:
        return 0
    if n==2:
        return 1
    else:
        return (n-1)*D(n-2)+(n-1)*D(n-1)
```

```
h=D(10)
```

```
print(h)
```

9) Toss a coin 5 times and count the number of heads and tails

Program:

```
import random
h=0
t=0
for j in range(1,6):
    c=random.randint(0,1)
    if c==0:
        h=h+1
    else:
        t=t+1
print(h,t)
```

Notes:

a) import random

This means the program can generate random numbers

b)  $c=\text{random.randint}(0,1)$

This means  $c$  is randomly set to 0 or 1.

Think of  $c=0$  as tossing a coin and getting a head and  $c=1$  as getting a tail.

10) Play the game Chuck – a – Luck a million times and find the average winnings per game

Program:

```
import random
T=0
for j in range(1,1000001):
    D=0
    dice1=random.randint(1,6)
    dice2=random.randint(1,6)
    dice3=random.randint(1,6)
    if dice1==6:
        D=D+1
    if dice2==6:
        D=D+1
    if dice3==6:
        D=D+1
    if D==0:
        W=-1
    else:
        W=D
    T=T+W
print(T/1000000)
```

Notes:

- a) dice 1 is the score on the first dice, etc
- b) D is the total number of sixes on the three dice in one game
- c) W is how much I win in one game.
- d) T is my total winnings in 1,000,000 games
- e) If you work it out exactly, you will find that:

my average winnings, per game, in the long run, is £-17/216

Most(?) people are surprised by this as they would guess my average winnings, per game, in the long run would be positive. This, therefore gives you the opportunity, to extort money from people who have not read this book!

11) Estimate  $\frac{\pi}{4}$  using random numbers      see chapter: Pi      CHECK

```
import random
```

```
N=1000000
```

```
T=0
```

```
for j in range(1,N+1):
```

```
    x=random.uniform(0,1)
```

```
    y=random.uniform(0,1)
```

```
    if x*x+y*y<1:
```

```
        T=T+1
```

```
print(T/N)
```

Notes:

a) N is the number of points we will generate in the unit square.

b) T is the number of these points that are inside the quarter circle.

c) x=random.uniform(0,1)

This means  $x$  is a random number between 0 and 1

d)  $x^2 + y^2 < 1$

This is true if the point  $(x, y)$  is inside the quarter circle.

## NOTE

To run these programs, go online and find an online IDE. Choose Python as the language, type in the program and run it.

This is not a course in programming. These examples are here to entice you into learning some programming if you have not done any before. These programs could be improved. For example, in program (4) we do not need the range of the for loop to be (2,m) Why not?

Program (4) Test if 17 is a prime number. We can easily adapt this program to test any positive integer to see if it is a prime number. Or we could print out a list of the first 100 prime numbers.

Or ...

## Appendix 2

### 1) Arithmetic Sequences

Here is an arithmetic sequence: 7, 10, 13, 16, 19, 22, 25, ...

The first term is 7 and the difference between consecutive terms is 3

$$u_1=7 \quad u_2=7+(3)=10 \quad u_3=7+(2\times 3)=13 \quad u_4=7+(3\times 3)=16 \quad \dots \quad u_n=7+(n-1)3$$

In general:

Arithmetic sequence:  $a+(a+d)+(a+2d)+(a+3d)+(a+4d)+\dots$

The  $n$ th term is  $u_n=a+(n-1)d$

### 2) Geometric Sequences

Here is a geometric sequence:

$$2, 6, 18, 54, 162, 486, 1458, \dots$$

The first term is 2 and the ratio of consecutive terms is 3

$$u_1=2 \quad u_2=2\times(3)=6 \quad u_3=2\times(3^2)=18 \quad u_4=2\times(3^3)=54 \quad \dots \quad u_n=2(3^{n-1})$$

In general:

Geometric sequence:

$$a, ar, ar^2, ar^3, ar^4, \dots$$

The  $n$ th term is:

$$(ar^{n-1})$$

Summing an infinite geometric series:

$$S=a+ar+ar^2+ar^3+ar^4+\dots$$

So:

$$rS=ar+ar^2+ar^3+ar^4+ar^5+\dots$$

So:

$$S-rS=(a+ar+ar^2+ar^3+ar^4+\dots)-(ar+ar^2+ar^3+ar^4+ar^5+\dots)=a$$

So:

$$S(1-r)=a$$

So:

$$S=\frac{a}{1-r} \text{ this result is only valid if } -1 < r < 1$$

### 3) Indices

examples

$$3^2 \times 3^4 = (3 \times 3) \times (3 \times 3 \times 3 \times 3) = 3^6$$

in general

$$(x^m)(x^n) = x^{m+n}$$

$$\frac{3^6}{3^2} = \frac{3 \times 3 \times 3 \times 3 \times 3 \times 3}{3 \times 3} = 3^4$$

$$\frac{x^m}{x^n} = x^{m-n}$$

$$\frac{3^6}{3^5} = \frac{3 \times 3 \times 3 \times 3 \times 3 \times 3}{3 \times 3 \times 3 \times 3 \times 3} = 3 \quad \text{but} \quad \frac{3^6}{3^5} = 3^1$$

$$x^1 = x$$

$$\frac{3^6}{3^6} = \frac{3 \times 3 \times 3 \times 3 \times 3 \times 3}{3 \times 3 \times 3 \times 3 \times 3 \times 3} = 1 \quad \text{but} \quad \frac{3^6}{3^6} = 3^0$$

$$x^0 = 1$$

$$(3^4)^2 = (3 \times 3 \times 3 \times 3) \times (3 \times 3 \times 3 \times 3) = 3^8$$

$$(x^m)^n = x^{mn}$$

$$3^{-4} \times 3^4 = 3^0 = 1 \quad \text{so} \quad 3^{-4} = \frac{1}{3^4}$$

$$x^{-m} = \frac{1}{x^m}$$

$$3^{1/2} \times 3^{1/2} = 3^1 = 3 \quad \text{so} \quad 3^{1/2} = \sqrt{3}$$

$$x^{1/2} = \sqrt{x}$$

$$3^{\frac{5}{2}} = \left(3^{\frac{1}{2}}\right)^5$$

$$x^{\frac{m}{n}} = \left(x^{\frac{1}{n}}\right)^m$$

### 4) Logarithms

If  $125=5^3$  then  $\log_5 125=3$

In general:

If  $c=a^b$  then  $\log_a c=b$

Now

$$8=2^3 \quad \text{so} \quad \log_2 8=3 \quad \text{and} \quad 32=2^5 \quad \text{so} \quad \log_2 32=5$$

examples

$$8 \times 32 = 2^{3+5} \quad \text{so} \quad \log_2(8 \times 32) = \log_2 8 + \log_2 32$$

in general

$$\log_a(xy) = \log_a(x) + \log_a(y)$$

$$\frac{32}{8} = 2^{5-3} \text{ so } \log_2\left(\frac{32}{8}\right) = \log_2 32 - \log_2 8$$

$$\log_a\left(\frac{x}{y}\right) = \log_a(x) - \log_a(y)$$

$$32^4 = (2^5)^4 = 2^{4 \times 5} \text{ so } \log_2(32^4) = 4 \log_2 32$$

$$\log_a(x^n) = n \log_a(x)$$

## 5) Factor theorem

example

$$f(x) = x^2 - 5x + 6$$

So:

$$f(2) = 2^2 - (5 \times 2) + 6 = 0$$

The factor theorem tells us that if  $f(2) = 0$  then  $(x-2)$  is a factor of  $f(x)$

So:

$$f(x) = (x-2)(...)$$

In general:

If  $f(a) = 0$  then  $(x-a)$  is a factor of  $f(x)$

## 6) Factorials

$$1! = 1$$

$$2! = 1 \times 2$$

$$3! = 1 \times 2 \times 3$$

$$4! = 1 \times 2 \times 3 \times 4 \text{ etc}$$

## 7) Binomial theorem for multiplying out brackets

$$(1+x)^1 = 1+x$$

$$(1+x)^2 = 1+2x+x^2$$

$$(1+x)^3 = 1+3x+3x^2+x^3$$

$$(1+x)^4 = 1+4x+6x^2+4x^3+x^4$$

In general: if  $n$  is a positive integer

$$(1+x)^n = (nC0) + (nC1)x + (nC2)x^2 + (nC3)x^3 + \dots + (nCn)x^n$$

## Appendix 3 – Where to find out more.

### 1) Online resources

a) A good place to start is the Plus Magazine website. Here you will find lots of interesting articles, written at roughly the same level as this book.

b) If you are interested in the history of mathematics, then I would recommend the MacTutor website.

Biographies - Alphabetical Index this will take you to articles about mathematicians.

History Topics - Alphabetical List this will take you to articles about mathematical topics.

c) Search YouTube for:

Numberfile

Mathologer

d) Online searches

Penrose tiles

M. C. Escher

### 2) Books

Number Theory: A Very Short Introduction R. Wilson

Combinatorics: A Very Short Introduction R. Wilson

Mathematics: A Very Short Introduction T. Gowers

Cryptography: A Very Short Introduction F. Piper, S. Murphy

The Code Book S. Singh

The Annotated Alice M. Gardner

Lewis Carroll in Numberland R. Wilson

How Music Works J. Powell

Golden Ratio M. Livio

The Code Book S. Singh

Enigma, The Battle For The Code H. Sebag-Montefiore

Taking Chances	J. Haigh
The Drunkard's Walk	L. Mlodinow
Euler's Gem	D. S. Richeson
The Annotated Alice	M. Gardner
Logic And Its Limits	P. Shaw

## Arrangements and Selections

### Rule 1

In how many ways can you arrange the people Alice, Bill and Carol, in a line?

You have 3 choices for the first person in the line:

A                    B                    C

For each of these choices, you have 2 choices for the second person in the line:

AB        AC        BA        BC        CA        CB

For each of these choices, you have 1 choice for the third person in the line:

ABC      ACB      BAC      BCA      CAB      CBA

Answer:  $3 \times 2 \times 1$

We can write  $3 \times 2 \times 1$  as  $3!$

(See Appendix 2 - Factorials)

In general:

In how many ways can you arrange  $n$  different items in a line?

Answer:  $n!$

example

In how many ways can you arrange 10 people in a line?

Answer:  $10!$

### Rule 2

In how many ways can you arrange 3 people chosen from Alice, Bill, Carol, David, Eric, in a line?

You have 5 choices for the first person in the line.

For each of these choices, you have 4 choices for the second person in the line.

For each of these choices, you have 3 choice for the third person in the line.

Answer:  $5 \times 4 \times 3$

We can write  $5 \times 4 \times 3$  as  $\frac{5 \times 4 \times 3 \times 2 \times 1}{2 \times 1} = \frac{5!}{2!}$

We write this as  $(5P3)$ . The  $P$  stands for permutation.

In general:

In how many ways can you arrange  $r$  items chosen from  $n$  different items, in a line?

Answer:  $(nP_r) = \frac{n!}{(n-r)!}$

example

In how many ways can you arrange 3 people in a line if there are 17 people to choose from?

Answer:  $(17P3) = 4080$

### Rule 3

In how many ways can you select 3 people chosen from Alice, Bill, Carol, David and Eric?

You have 5 choices for the first person.

For each of these choices, you have 4 choices for the second person.

For each of these choices, you have 3 choice for the third person.

Answer:  $5 \times 4 \times 3$  No!  $5 \times 4 \times 3$  is the answer to the question:

In how many ways can you arrange 3 people chosen from Alice, Bill, Carol, David, Eric, in a line?

For each selection of 3 people there are  $3!$  arrangements.

BCE is one selection.

BCE, BEC, CBE, CEB, EBC, ECB are the  $3!$  possible arrangements.

The answer  $5 \times 4 \times 3$  has counted each selection  $3!$  times.

Answer:  $\frac{5 \times 4 \times 3}{3!}$

We can write  $\frac{5 \times 4 \times 3}{3!}$  as  $\frac{5 \times 4 \times 3 \times 2 \times 1}{3! \times 2 \times 1} = \frac{5!}{3! 2!}$

We write this as  $(5C3)$  The  $C$  stands for combination.

In general:

In how many ways can you select  $r$  items chosen from  $n$  different items?

Answer:  $(nCr) = \frac{n!}{r!(n-r)!}$

example

In how many ways can you select 3 people from a group of 17 people?

Answer:  $(17C3) = 680$

### Rule 4

You start each day with a cup of tea or a cup of coffee. In how many ways can you select your drinks for a week?

Note: if you choose tea on the first day then you are allowed to choose tea on the second day – so repetitions are allowed.

You have 2 choices of drink on the first day.

You have 2 choices of drink on the second day

...

You have 2 choices of drink on the seventh day.

Answer:  $2^7 = 128$

In general:

In how many ways can you arrange  $r$  items chosen from  $n$  different items if repetitions are allowed?

Answer:  $n^r$

example

In how many ways can you make a 4 letter word?

Answer:  $26^4$

of course, most of these won't be real words

## Rule 5

A sweet shop sells 5 varieties of sweets. The varieties are called A, B, C, D, E.

For £1 you can buy any 12 sweets. In how many ways can you make your selection?

You can record a selection like this:

sweet	A	B	C	D	E
number	✓ ✓	✓ ✓ ✓	✓ ✓		✓ ✓ ✓ ✓ ✓

This selection is, two As, three Bs, two Cs, no Ds and five Es

You could record this selection as:

✓ ✓ | ✓ ✓ ✓ | ✓ ✓ | | ✓ ✓ ✓ ✓ ✓

So the question becomes:

In how many ways can you arrange 12 ✓ symbols and 4 | symbols in a line?

There are 16 places in the line and we need to choose 12 of these places for the ✓ symbols.

Answer:  $(16C12)$

In general:

In how many ways can you select  $r$  items chosen from  $n$  different items if repetitions are allowed?

Answer:  $((n+r-1)Cr)$

example

A shop sells 6 varieties of bread rolls. In how many ways can I select 20 rolls?

Answer:  $(25C20)$

Note: independent choices and multiplication

There are 5 men and 4 women in a room. In how many ways can you select 2 men and 3 women?

There are  $(5C2)=10$  ways to select the men. There are  $(4C3)=4$  ways to select the women.

For each of the 10 ways you can select the men there are 4 ways you can select the women. The choice of men is independent of the choice of women. Under these circumstances:

Answer:  $(5C2) \times (4C3)$

### Example 1

In how many ways can you arrange 7 boys and 3 girls in a line if:

- a) the girls are at the front?
- b) the girls stand next to each other?
- c) no two girls stand next to each other?

Solutions

a) There are  $3!$  ways to arrange the girls and there are  $7!$  ways to arrange the boys.

Answer:  $3! \times 7!$

b) We have 8 items to arrange in a line. A block of girls and 7 boys. We can do this in  $8!$  ways.

But for each of these arrangements, we can shuffle the girls in  $3!$  ways.

Answer:  $8! \times 3!$

c) We can arrange the boys in  $7!$  ways. Then we add the girls. There are 8 places where we can put the first girl. At the front, at the back or between two boys. There are 7 places we can put the next girl and there are 6 places we can put the third girl.

Answer:  $7! \times 8 \times 7 \times 6$

### Example 2

In how many ways can you arrange 10 Physics, 4 French and 7 Biology books in a line if books of the same subject must be kept together?

Solution

We can arrange the 3 subjects in  $3!$  ways. We can then shuffle the Physics books in  $10!$  ways, the French books in  $4!$  ways and the Biology books in  $7!$  ways.

Answer:  $3! \times 10! \times 4! \times 7!$

### Example 3

There are 8 boys and 5 girls in a class. In how many ways can you arrange 4 boys and 3 girls in a line?

Solution

We can select the pupils in  $(8C4) \times (5C3)$  ways.

Having selected the pupils, we can arrange them in  $7!$  ways.

Answer:  $(8C4) \times (5C3) \times 7!$

#### Example 4

There are 10 boys and 12 girls in a class. In how many ways can you select 5 pupils if you must include at least one boy and at least one girl?

Solution

There are  $(22C 5)$  ways to select 5 pupils. But some selections are no good.

There are  $(10C 5)$  selections which are all boys and  $(12C 5)$  selections that are all girls.

Answer:  $(22C 5) - (10C 5) - (12C 5)$

#### Example 5

In how many ways can you arrange the letters A, A, A, B, B, B, B, in a line?

Solution

There are 8 places and we need to choose 3 of these places for the A's

Answer:  $(8C 3)$

Or

There are 8 places and we need to choose 5 of these places for the B's

Answer:  $(8C 5)$

#### Example 6

A pack of cards has 52 cards. Each card has a suit (spade, heart, diamond or club) and a rank (ace, two, three, ... king). In a game of poker, a hand consists of 5 cards. How many hands are:

- a) Straight-flush                5 consecutive cards all in the same suit
- b) 4 of a kind                4 cards of one rank and 1 other card
- c) Full-house                3 cards of one rank and 2 cards of another rank
- d) Flush                5 non-consecutive cards all in the same suit
- e) Straight                5 consecutive cards not all in the same suit
- f) 3 of a kind                3 cards of one rank and 2 other cards of different ranks

Solutions

a) Straight-flush:

There are 10 ways you can get 5 consecutive cards:

ace, 2, 3, 4, 5

2, 3, 4, 5, 6

3, 4, 5, 6, 7

...

10, jack, queen, king, ace

There are 4 choices for the suit.

Answer:  $10 \times 4 = 40$

b) 4 of a kind:

There are 13 choices for the rank of the 4 cards and 48 choices for the 1 other card.

Answer:  $13 \times 48 = 624$

c) Full-house:

There are 13 choices for the rank of the 3 cards and  $(4C3)$  choices for the 3 cards of that rank.

There are 12 choices for the rank of the 2 cards and  $(4C2)$  choices for the 2 cards of that rank.

Answer:  $13 \times (4C3) \times 12 \times (4C2)$

d) Flush:

There are 4 choices for the suit of the 5 cards and  $(13C5)$  choices for the 5 cards of that suit.

But we have included the 40 straight-flushes.

Answer:  $4 \times (13C5) - 40$

e) Straight:

There are 10 ways you can get 5 consecutive cards:

For each card in the straight there are 4 choices for its suit.

But we have included the 40 straight-flushes.

Answer:  $10 \times 4 \times 4 \times 4 \times 4 \times 4 - 40$

f) 3 of a kind:

There are 13 choices for the rank of the 3 cards and  $(4C3)$  choices for the 3 cards of that rank.

There are  $(12C2)$  ways to choose the ranks of the other 2 cards.

For each of the other 2 cards there are 4 choices for their suits

Answer:  $13 \times (4C3) \times (12C2) \times 4 \times 4$

### Example 7

There are 20 people at a party. Everyone shakes hands once with every-one else. How many hand-shakes take place?

It can be fun to think of different ways to answer the same question.

Solution 1

There are 20 people and everyone has 19 hand-shakes.

Answer:  $20 \times 19$  No! We have counted every handshake twice. Can you see why?

Answer:  $\frac{20 \times 19}{2}$

Solution 2

Alice does 19 hand-shakes and then goes home.

Bill then does 18 hand-shakes and goes home.

Jane then does 17 hand-shakes and goes home.

etc

Answer:  $19+18+17+\dots+1$

Solution 3

There are  $(20C2)$  ways to select a pair of people. For every pair of people there is a hand-shake.

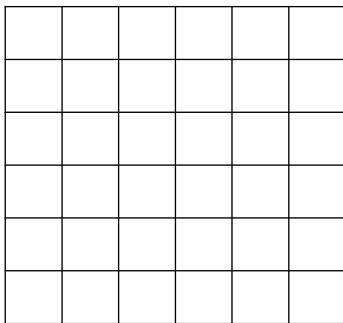
Answer:  $(20C2)$

see EXERCISE

### EXERCISE

- 1) I have 12 pens, 8 pencils and 4 crayons. In how many ways can you select one of each?
- 2) On a restaurant menu there are 3 choices for the first course, 10 choices for the second course and 5 choices for the third course. In how many ways can you select a meal?
- 3) Each day I buy a coffee, a tea or a beer at my local cafe. In how many ways can I select my drinks for a week?
- 4) In how many ways can you arrange the letters A, B, C, D, E?
- 5) In how many ways can you arrange 20 people in a line?
- 6) In how many ways can you arrange 3 of the letters A, B, C, D, E, F, G, H?
- 7) In how many ways can I arrange 7 ornaments in a line if I have 18 ornaments to choose from?
- 8) In how many ways can you arrange the digits 1, 2, 3, 4, 5, 6, 7 to form an odd number?
- 9) There are 10 runners in a race. In how many ways can the gold, silver and bronze medals be awarded if there are no dead-heats?
- 10) In how many ways can you select 3 of the letters A, B, C, D, E, F, G, H?
- 11) In how many ways can you select 13 cards from a pack of 52 cards?
- 12) In a lottery, you have to select 6 numbers from 1, 2, 3, ..., 49  
In how many ways can you select your lottery numbers?
- 13) In a class of 25 pupils, everyone shakes hands exactly once with everyone-else. How many hand-shakes take place?
- 14) 10 points are marked around a circle. A line is drawn between every pair of points. How many lines will be drawn?
- 15) In how many ways can you split a class of 28 pupils into a group of 20 and a group of 8?
- 16) In how many ways can you split a class of 28 pupils into a group of 18, a group of 6 and a group of 4?

- 17) In how many ways can you split a class of  $(x+y+z)$  pupils into a group of  $x$  pupils, a group of  $y$  pupils and a group of  $z$  pupils if  $x$  and  $y$  and  $z$  are different numbers?
- 18) There are 16 boys and 18 girls in a class. In how many ways can you select 6 boys and 9 girls?
- 19) I have 30 letters and 30 envelopes. In how many ways can I place one letter in each envelope?
- 20) In how many ways can you select some (or none) people from a group of 7 people?
- 21) How many hands of 13 cards have 4 spades, 4 hearts, 4 diamonds and 1 club?
- 22) Here is the street plan of a city. The lines represent the streets.



All roads run north-south or east-west. I want to walk from the bottom left-hand corner to the top right-hand corner. I only want to walk north or east. In how many ways can I select my route?

23) Brag

In a game of Brag, a hand consists of 3 cards. How many hands are:

- |                   |  |
|-------------------|--|
| a) 3 of a kind    | 3 cards of one rank                          |
| b) Straight-flush | 3 consecutive cards all in the same suit     |
| c) Straight       | 3 consecutive cards not all in the same suit |
| d) Flush          | 3 non-consecutive cards all in the same suit |
| e) 2 of a kind    | 2 cards of one rank and 1 other card         |

## SOLUTIONS

- 1) Answer:  $12 \times 8 \times 4$
- 2) Answer:  $3 \times 10 \times 5$
- 3) Answer:  $3 \times 3 \times 3 \times 3 \times 3 \times 3$
- 4) Answer:  $5!$
- 5) Answer:  $20!$
- 6) Answer:  $(8P3)$
- 7) Answer:  $(18P7)$

- 8) There are 4 choices for the last digit because the last digit must be odd. The other 6 digits can be arranged in  $6!$  ways.

Answer:  $4 \times 6!$

9) We want to arrange 3 of the 10 runners on the podium.

Answer:  $(10P3)$

10) Answer:  $(8C3)$

11) Answer:  $(52C13)$

12) Answer:  $(49C6)$

13) For each way we can choose two pupils there is a hand-shake.

Answer:  $(25C2)$

14) For each way we can choose two points there is a line.

Answer:  $(10C2)$

15) Once you have chosen 20 pupils from 28 pupils there is nothing-else to do.

Answer:  $(28C20)$

16) Once you have chosen 18 pupils from 28 pupils and then chosen 6 pupils from the remaining 10 pupils there is nothing-else to do.

Answer:  $(28C18) \times (10C6)$

17) Once you have chosen  $x$  pupils from  $(x+y+z)$ pupils and then chosen  $y$  pupils from the remaining  $(y+z)$ pupils there is nothing-else to do.

Answer:  $((x+y+z)Cx) \times ((y+z)Cy)$

This answer simplifies to:  $\frac{(x+y+z)!}{x!y!z!}$

18) Answer:  $(16C6) \times (18C9)$

19) Answer:  $30!$

20) For each person you have a choice of 2 options – select that person or don't select that person.

Answer:  $2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$

21) You have to choose 4 of the 13 spades and ...

Answer:  $(13C4) \times (13C4) \times (13C4) \times (13C1)$

22) I need to walk 6 blocks north and 6 blocks east.

A possible route is: N, N, E, E, E, N, E, E, N, N, N, E

There are 12 letters in the line and we need to choose 6 positions for the N letters.

Answer:  $12C6$

23)

a) 3 of a kind:

There are 13 choices for the rank of the 3 cards and  $(4C3)$  choices for the 3 cards of that rank.

Answer:  $13 \times (4C3)$

b) Straight-flush:

There are 12 ways you can get 3 consecutive cards:

ace, 2, 3

2, 3, 4

3, 4, 5

...

queen, king, ace

There are 4 choices for the suit.

Answer:  $12 \times 4 = 48$

c) Straight:

There are 12 ways you can get 3 consecutive cards:

For each card in the straight there are 4 choices for its suit.

But we have included the 48 straight-flushes.

Answer:  $12 \times 4 \times 4 \times 4 - 48$

d) Flush:

There are 4 choices for the suit of the 3 cards and  $(13C3)$  choices for the 3 cards of that suit.

But we have included the 48 straight-flushes.

Answer:  $4 \times (13C3) - 48$

e) 2 of a kind:

There are 13 choices for the rank of the 2 cards and  $(4C2)$  choices for the 2 cards of that rank.

There are 48 choices for the 1 other card.

Answer:  $13 \times (4C2) \times 48$

## Choosing a Pub

Three students, Bill, Alice and Jane decide to go to the pub for a drink. There are four pubs to choose from; The Crown, The Bear, The Cross Keys, and The Eight Bells. Each student has put the pubs in order of preference:

Bill: The Cross Keys, The Bear, The Crown, The Eight Bells

Alice: The Bear, The Crown, The Eight Bells, The Cross Keys

Jane: The Crown, The Eight Bells, The Cross Keys, The Bear

Jane says: Let's go to The Crown, it's my favourite pub.

However two students prefer The Bear to The Crown so they decide to go to The Bear.

However two students prefer The Cross Keys to The Bear so they decide to go to The Cross Keys.

However two students prefer The Eight Bells to The Cross Keys so they decide to go to The Eight Bells.

So off they go to The Eight Bells.

After a few pints, Bill says: I prefer The Crown to The Eight Bells and the other two both agree.

## Contents

0. Introduction

1. Voting Systems

2. Squares

a) Magic Squares

b) Latin Squares

c) Euler Squares

3. Knight Tours

4. Tiling

6. Triangle Problem

7. Grid Puzzles

8. Wason Test

9. Pigeonhole Principle

10. Multiples

11. Paradoxes

12. Quotes

13. Heron's Theorem

15. Three Games

16. Möbius Strip

18. Choosing a Pub

19. Lewis Carroll

20. Codes

a) Error Detecting Codes  
b) Error Correcting Codes

22. Rationals and Irrationals

23. A Nice Proof

24. A Nice Sum

25. Logic

a) Propositions  
b) If ... Then  
c) Arguments with If ... Then  
d) Arguments with All, None, Some  
e) Hat Puzzles

26. Switching Circuits

27. Venn Diagrams

28. Snowflake Curve

29. Arrangements and Selections

30. Proof

a) Proof by Contradiction  
b) Proof by Induction  
c) Proving The Contrapositive  
d) Proof using Selections

33. Pascal's Triangle

34. How to Tune a Piano

35. Dodgy Algebra

36. Graph theory

- a) Graphs
  - b) Euler Tours
  - c) Hamilton Tours
  - d) Euler's Formula
  - e) Map Colouring
  - f) Tessellations
  - g) Polyhedrons
  - h) Points and Regions
  - i) Sprouts
37. Probability Theory
- a) Dodgy Probability
  - b) Probability
  - c) Probability Fallacies
  - d) Probability Paradoxes
  - e) Coins
  - f) Tennis
  - g) Collecting Cards
  - h) Party Game
38. Number Theory:
- a) Fundamental Theorem of Arithmetic
  - b) Euclid's Algorithm
  - c) Prime Numbers
  - d) Modulo Arithmetic
  - e) Chinese Remainder Theorem
  - f) Fermat's Last Theorem
  - g) Fermat's Little Theorem
  - h) Card Shuffles
  - i) Casting Out Nines
  - j) Perfect Numbers
  - k) Sums of Squares
39. Recurrence Relations:
- a) Recurrence relations
  - b) Cutting a Pizza
  - c) Tower of Hanoi
  - d) Derangements
  - e) Fibonacci Numbers
  - f) Polygonal Numbers
  - g) A Nice Integral
40. Group Theory:
- a) Groups
  - b) Group Theorems
  - c) Symmetries of a Rectangle
  - d) Symmetries of a Triangle
  - e) Rearrangements
  - f) Friezes
41. Encryption
43. e
44. pi
45. Dodgy Integrals
46. Lanchester's Model
47. Paint Pot

- 48. Infinite Series
- 49. Maclaurin Series
- 50. Complex Numbers
  - a) Complex Numbers
  - b) Euler's Identity
  - c) Using Complex Numbers
  - d) Julia Sets

52. Infinite Numbers

Appendix 1

A Few Short Programs

Appendix 2

- 1) Arithmetic Sequences
- 2) Geometric Sequences
- 3) Indices
- 4) Logarithms
- 5) Factor Theorem
- 6) Factorials

Appendix 3

- a) Online resources
- b) Books

Appendix 4

- a) Euler's Sine Formula
- b) Euler's Zeta Function
- c) Euler's Prime Sum
- d) Euler's Constant

## Dodgy Algebra

### Example 1

$$3 > 2$$

$$3 \log\left(\frac{1}{2}\right) > 2 \log\left(\frac{1}{2}\right)$$

$$\log\left(\frac{1}{2}\right)^3 > \log\left(\frac{1}{2}\right)^2$$

$$\log\left(\frac{1}{8}\right) > \log\left(\frac{1}{4}\right)$$

$$\frac{1}{8} > \frac{1}{4}$$

### Example 2

$$x > 3$$

$$3x > 9$$

$$3x - x^2 > 9 - x^2$$

$$x(3-x) > (3+x)(3-x)$$

$$x > 3+x$$

$$0 > 3$$

### Example 3

$$x = 3$$

$$x^2 = 3x$$

$$x^2 - 9 = 3x - 9$$

$$(x+3)(x-3) = 3(x-3)$$

$$(x+3) = 3$$

$$x = 0$$

$$3 = 0$$

### Example 4

$$x + y = 2$$

$$(x+y)(x-y) = 2(x-y)$$

$$x^2 - y^2 = 2x - 2y$$

$$x^2 - y^2 + (y^2 - 2x + 1) = 2x - 2y + (y^2 - 2x + 1)$$

$$x^2 - 2x + 1 = y^2 - 2y + 1$$

$$(x-1)^2 = (y-1)^2$$

$$x-1 = y-1$$

$$x = y$$

Example 5

$$\sin 70^\circ = \sin 110^\circ$$

$$70^\circ = 110^\circ$$

Example 6

$$3 - \frac{x+4}{x-2} = \frac{2x-10}{x-3}$$

$$\frac{3(x-2)-(x+4)}{x-2} = \frac{2x-10}{x-3}$$

$$\frac{2x-10}{x-2} = \frac{2x-10}{x-3}$$

$$2=3$$

## EXERCISE

So where did it all go wrong?

## SOLUTIONS

1)

We multiplied both sides of an inequality by  $\log(1/2)$

But  $\log(1/2)$  is negative so we should reverse the inequality sign.

2)

We divided both sides of an inequality by  $(3-x)$

But  $(3-x)$  is negative so we should reverse the inequality sign.

3)

We divided both sides of an equation by  $(x-3)$

But  $(x-3)=0$

4)

If  $(x-1)^2 = (y-1)^2$  then either  $(x-1) = (y-1)$  or  $(x-1) = -(y-1)$

5)

Look at the graph  $y = \sin x$

6)

$$\frac{2x-10}{x-2} = \frac{2x-10}{x-3}$$

So:

$$(2x-10)(x-3) = (2x-10)(x-2) \text{ provided } x \neq 3 \text{ and } x \neq 2$$

Either:

$$(2x-10)=0 \text{ so } x=5$$

Or:

$$(x-3)=(x-2) \text{ which has no solution}$$

## Dodgy Integrals

if you know about integration ...

1. Find the area under the curve:

$$y = \frac{1}{x^2} \text{ between } x = -1 \text{ and } x = 1$$

DIAGRAM?

The area is above the  $x$  axis, so the integral will be positive.

Show that:

$$\int_{-1}^1 \frac{1}{x^2} dx = \dots = -2$$

2. Now:

$$\int (\sin x \cos x) dx = \frac{1}{2} \sin^2 x \quad \text{check by differentiation}$$

And:

$$\int (\sin x \cos x) dx = -\frac{1}{2} \cos^2 x \quad \text{check by differentiation}$$

So:

$$\frac{1}{2} \sin^2 x = -\frac{1}{2} \cos^2 x$$

So:

$$\sin^2 x + \cos^2 x = 0$$

3. Now:

$$\int \left( \frac{1}{7x} \right) dx = \frac{1}{7} \ln x \quad \text{check by differentiation}$$

And:

$$\int \left( \frac{1}{7x} \right) dx = \frac{1}{7} \ln 7x \quad \text{check by differentiation}$$

So:

$$\ln x = \ln 7x$$

4. Using integration by parts, show that:

$$\int \left( \frac{1}{x} \right) dx = \int 1 \times \left( \frac{1}{x} \right) dx = x \frac{1}{x} + \int \left( \frac{1}{x} \right) dx$$

So:

$$\int \left( \frac{1}{x} \right) dx = 1 + \int \left( \frac{1}{x} \right) dx$$

So:

$$0 = 1$$

5. Now:

$$\int 2 \sin 2x dx = -\cos 2x \quad \text{check by differentiation}$$

And:

$$\int 2 \sin 2x dx = 2 \sin^2 x \quad \text{check by differentiation}$$

So:

$$-\cos 2x = 2 \sin^2 x$$

6. Let:

$$I = \int_0^{\pi} \cos^2 x dx$$

So:

$$I = \int_0^{\pi} \cos x \cos x dx = \int_0^{\pi} \sqrt{1 - \sin^2 x} \cos x dx$$

Use the substitution:

$$\sin x = t$$

Show:

$$\cos x dx = dt$$

Show that:

$$I = \int_0^0 \sqrt{1-t^2} dt = 0$$

7. Now:

$$\sec^2 x \geq 0$$

So:

$$\int_0^{\pi} \sec^2 x dx > 0$$

But:

$$\int_0^{\pi} \sec^2 x dx = [\tan x]_0^{\pi} = 0$$

## Encryption

### Part 1.

Alice wants to send a secret message to Bill. Eve wants to read this message. Alice writes the message on a piece of paper and puts the piece of paper in a box. Then she puts a padlock on the box and sends it to Bill. Eve might be able to intercept the box but she can't open it as she does not have a key to the padlock. Bill receives the box and unlocks the padlock with his key. Alice and Bill will have to make arrangements, in advance, so that they each have a copy of the padlock key. This example is a bit like private-key encryption.

### Private-key encryption

Alice wants to send a secret message to Bill using email. Eve wants to read this message. Alice decides that she can't prevent Eve intercepting the email but she can prevent Eve reading the message. She can use encryption.

We will look at two private-key encryption methods - substitution and addition. In both methods, each letter in the message is replaced by a different (or perhaps the same) letter.

#### 1. Substitution

##### Example 1

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
G	C	R	K	Q	W	P	F	I	T	A	J	X	R	B	Z	N	Y	O	V	H	D	M	E	U	L

Method: replace a letter in the top row by the corresponding letter in the second row

Key: the above table (we could use any rearrangement of the alphabet)

We will assume that Eve knows the method being used but she does not have the key.

The message Alice wants to send is: meet me tonight

message	M	E	E	T	M	E	T	O	...
encryption	X	Q	Q	V	X	Q	V	B	...

### EXERCISE 1

Alice encrypts a message using the above key and sends it to Bill.

Bill receives: VFQXBRQUIOIRVFQOFQK

Can you decrypt this message for Bill?

Alice and Bill will have to make arrangements, in advance, to use substitution encryption and to agree on the key. How are they going to do this?

There are  $26! - 1$  different ways we can rearrange the letters of the alphabet, so there are  $26! - 1$  possible keys. Eve might not be able to try all these keys. However this method of encryption has a serious flaw. Every time there is an A in the message it is replaced by a G in the encryption. Every time there is an B in the message it is replaced by a C in the encryption ...etc

This means that Eve can use frequency analysis.

In a piece of text, written in English, some letters will appear more often than others.

The list of letters in order of how often they appear is roughly:

E, T, A, O, I, N, S, H, R, D, L, C, U, M, W, F, G, X, P, B, V, K, J, Q, Y, Z

So Eve can count how many times each letter appears in the encryption. The letter with the highest frequency will probably correspond to an E in the message. The letter with the second highest frequency might correspond to a T or perhaps an A ... etc

This technique works well for long messages.

## 2. Addition

How do you add two letters? What is  $P+U$  ?

We give each letter a number:

$$A=0 \quad B=1 \quad C=2 \quad D=3 \quad \dots \quad Z=25$$

and then add the numbers, mod 26 (see chapter, Modulo Arithmetic)

$$\text{So } P+U=15+20=35=9=J$$

Or we can use a Vigenere square (see footnote)

We can use this idea for encryption.

Method: add the letters of the message to the letters of the key

Key: see examples below

We will assume that Eve knows the method being used but she does not have the key.

The message Alice wants to send is: meet me tonight

### Example 2

key: D (we could use any letter)

message	M	E	E	T	M	E	T	O	...
	12	4	4	19	12	4	19	14	...
key	D	D	D	D	D	D	D	D	...
	3	3	3	3	3	3	3	3	...
addition	15	7	7	22	15	7	22	17	...
encryption	P	H	H	W	P	H	W	R	...

### Example 3

key: ERIC (we could use any word)

message	M	E	E	T	M	E	T	O	...
	12	4	4	19	12	4	19	14	...
key	E	R	I	C	E	R	I	C	...
	4	17	8	2	4	17	8	2	...
addition	16	21	12	21	16	21	27	16	...
encryption	Q	V	M	V	Q	V	B	Q	...

### Example 4

key: GEUKAQPTY (we could use any random list of letters)

message	M	E	E	T	M	E	T	O	...
	12	4	4	19	12	4	19	14	...
key	G	E	U	K	A	Q	P	T	...
	6	4	20	10	0	16	15	19	...
addition	18	8	24	29	12	20	34	33	...
encryption	S	I	Y	D	M	U	I	H	...

### EXERCISE 2

Alice encrypts a message using the key: DRMPKZTQDF and sends it to Bill.

Bill receives: IIQSSRTISD

Can you decrypt this message for Bill?

Alice and Bill will have to make arrangements, in advance, to use addition encryption and to agree on the key. How are they going to do this?

Some comments:

Example (2) is known as Caesar encryption.

There are only 25 possible keys. Eve could easily try them all, so this method is a bit rubbish.

Example (3) is known as key-word encryption.

The first E in the message is replaced by a V in the encryption but the second E in the message is replaced by an M in the encryption. This gets around the problem of frequency analysis.

Unfortunately, there are clever statistical techniques that Eve can use to find the length of the key-word. If Eve has discovered that the key-word is four letters long then:

1<sup>st</sup>, 5<sup>th</sup>, 9<sup>th</sup>, 13<sup>th</sup>, ... letters of the message have all been added to the same letter (in my example, E)  
2<sup>nd</sup>, 6<sup>th</sup>, 10<sup>th</sup>, 14<sup>th</sup>, ...letters of the message have all been added to the same letter (in my example, R)  
etc

So Eve can now do a frequency analysis on the 1<sup>st</sup>, 5<sup>th</sup>, 9<sup>th</sup>, 13<sup>th</sup>, ... letters of the encryption.

Then Eve can do a frequency analysis on the 2<sup>nd</sup>, 6<sup>th</sup>, 10<sup>th</sup>, 14<sup>th</sup>, ...letters of the encryption.

etc

Example (4) is known as one time-pad-encryption.

Imagine a note-pad. On each page is a random list of letters. You use the letters on page one of the note-pad as the key for your first message. You use the letters on page two of the note-pad as the key for your second message. etc Every time you encrypt a new message, you use a new page of random letters. As the lists of letters in the note-pad are random then the string of letters in the encryption is random and the encryption is uncrackable.

## Part 2.

Alice wants to send a secret message to Bill. Eve wants to read this message. Alice writes the message on a piece of paper and puts the piece of paper in a box. Bill has lots of identical padlocks which he makes available to anyone who wants to send him a message. There is just one key that fits all these padlocks and Bill has got it. Alice gets one of these padlocks and puts it on the box and sends it to Bill. Eve might be able to intercept the box but she can't open it. Bill receives the box and unlocks it with his key. Alice and Bill do not have to make arrangements, in advance. Anyone can send a message to Bill.

This example is a bit like public-key encryption.

## Public-key encryption

### Example 5

#### RSA encryption

Bill picks  $p$  and  $q$  where  $p$  and  $q$  are two different prime numbers.

Bill picks  $e$  where  $e$  and  $(p-1)(q-1)$  have no common factor.

Bill solves  $ed=1 \pmod{(p-1)(q-1)}$  to find  $d$

Bill publishes the numbers  $e$  and  $pq$  in a public directory for all to see, but he keeps the number  $d$  secret.

for example:

Bill picks  $p=5$   $q=11$  as 5 and 11 are two different prime numbers.

Bill picks  $e=7$  as 7 and 40 have no common factor.

Bill solves  $7d=1 \pmod{40}$  to get  $d=23$

Bill publishes the numbers 7 and 55 in a public directory for all to see, but he keeps the number 23 secret.

Alice wants to send a message to Bill. She looks-up the numbers  $e$  and  $pq$  in the public directory. She uses these numbers to encrypt her message.

(don't worry about how she does this)

When he receives the message, Bill uses the number  $d$  to decrypt it.

(don't worry about how he does this)

Eve intercepts the message. She knows the numbers  $e$  and  $pq$  because she (like anyone-else) can look them-up in the public directory.

But she needs to know  $p$  and  $q$  so she can solve  $ed=1 \pmod{(p-1)(q-1)}$  to find  $d$

So Alice's message appears to be safe, unless Eve can factorise  $pq$  to find  $p$  and  $q$

If  $p$  and  $q$  are large enough then factorising  $pq$  will be difficult.

Now don't worry about the details! Here are some important points:

- a) With private-key encryption, Alice and Bill need a way to get together, in advance, and agree upon a key. With public key encryption, anyone can send an encrypted message to Bill. Even someone Bill has never met.
- b) The security of RSA encryption relies on the difficulty of factorising large numbers.
- c) RSA encryption enables you to buy stuff online. I type-in my credit card number and this is encrypted. Anyone can do it.
- d) How does Bill know that the message really came from Alice?

e) My example with  $p=5$  and  $q=11$  is to illustrate the method. In practise Eve will be able to factorize 55. But if  $p$  and  $q$  are hundreds of digits long then Eve has a problem.

Encryption is used ...

- when you withdraw money from a cash machine
- when you send messages over the internet or a mobile phone
- to protect business and military secrets
- in banking
- for data storage
- for data transmission
- for on-line shopping etc

A lot has been written about the use of encryption during the Second World War. In particular, the use of the enigma machine. Read the books. Watch the films. Visit Bletchley Park.

SOLUTION 1

THE MONEY IS IN THE SHED

SOLUTION 2

FRED IS A SPY

footnote

### Vigenere square

To find P+U, find the intersection of the P row and the U column. P+U=J

+	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

$e$

Here are some nice formulas for  $e$  – there are lots more:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots$$

$$\frac{1}{e} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \dots$$

If  $n \rightarrow \infty$  then  $\left(1 + \frac{1}{n}\right)^n \rightarrow e$

If  $n \rightarrow \infty$  then  $\left(1 - \frac{1}{n}\right)^n \rightarrow \frac{1}{e}$

If  $n \rightarrow \infty$  then  $\frac{n}{(n!)^{1/n}} \rightarrow e$

### Example 1

$e$  and compound interest

I invest £1 for one year. How much is my investment worth if ...

a) the interest rate is 100% per year

answer £ $(1+1)^1$

b) the interest rate is 50% per  $1/2$  year

answer £ $\left(1 + \frac{1}{2}\right)^2$

c) the interest rate is 10% per  $1/10$  year

answer £ $\left(1 + \frac{1}{10}\right)^{10}$

d) the interest rate is 5% per  $1/20$  year

answer £ $\left(1 + \frac{1}{20}\right)^{20}$

e) the interest rate is  $(100/n)\%$  per  $1/n$  year

answer £ $\left(1 + \frac{1}{n}\right)^n$

Note:

as  $n \rightarrow \infty$  so answer  $\rightarrow £e$

## Example 2

$e$  and arranging ornaments

I have 3 ornaments. In how many ways can I arrange some (or none) ornaments in a line on my mantelpiece? see chapter: Arrangements and Selections

There are  $(3P0)$  arrangements with no ornaments.

There are  $(3P1)$  arrangements with one ornament.

There are  $(3P2)$  arrangements with two ornaments.

There are  $(3P3)$  arrangements with three ornaments.

The total number of arrangements is:

$$(3P0)+(3P1)+(3P2)+(3P3)=\frac{3!}{3!}+\frac{3!}{2!}+\frac{3!}{1!}+3!=3!\left(\frac{1}{3!}+\frac{1}{2!}+\frac{1}{1!}+1\right)=3!\left(1+\frac{1}{1!}+\frac{1}{2!}+\frac{1}{3!}\right)$$

In general:

If I have  $n$  ornaments then the number of arrangements is:

$$n!\left(1+\frac{1}{1!}+\frac{1}{2!}+\dots+\frac{1}{n!}\right)$$

If  $n$  is large then the number of arrangements is about  $n!e$

## Example 3

Theorem

$$e < 3$$

Proof:

$$e = 1 + \left(1 + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} + \dots\right) < 1 + \left(1 + \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \dots\right) = 1 + \frac{1}{1 - 1/2} = 3$$

## Example 4

Theorem

$e$  is irrational

Note:

$$\frac{7!}{8!} + \frac{7!}{9!} + \frac{7!}{10!} + \dots = \left(\frac{1}{8}\right) + \left(\frac{1}{8 \times 9}\right) + \left(\frac{1}{8 \times 9 \times 10}\right) + \dots < \frac{1}{8^1} + \frac{1}{8^2} + \frac{1}{8^3} + \dots = \frac{\frac{1}{8}}{1 - \frac{1}{8}} = \frac{1}{7}$$

So:

$$\frac{7!}{8!} + \frac{7!}{9!} + \frac{7!}{10!} + \dots < \frac{1}{7}$$

Proof (by contradiction)

Assume  $e$  is rational, say  $e = \frac{19}{7}$

Now:

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots$$

So:

$$\frac{19}{7} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots$$

So:

$$\frac{19}{7} \times 7! = \left( 7! + \frac{7!}{1!} + \frac{7!}{2!} + \frac{7!}{3!} + \dots + \frac{7!}{7!} \right) + \left( \frac{7!}{8!} + \frac{7!}{9!} + \frac{7!}{10!} + \dots \right)$$

The LHS is an integer and the first bracket on the RHS is an integer but the second bracket isn't – see above.

Contradiction.

If we assume:

$e = \frac{p}{q}$  where  $p$  and  $q$  are any positive integers, then we can repeat the above argument and

again get a contradiction. So  $e$  must be irrational.

It has been proved that  $e$ ,  $\pi$  and  $e^\pi$  are irrational

We do not know about  $\pi + e$ ,  $\pi e$ ,  $\pi^\pi$ ,  $e^e$ ,  $\pi^e$

Example 5 if you know about differentiation ...

Investigation

$2^4 = 4^2$  Can you think of another pair of positive integers with this property?

Hint:

If:

$$p^q = q^p$$

show that:

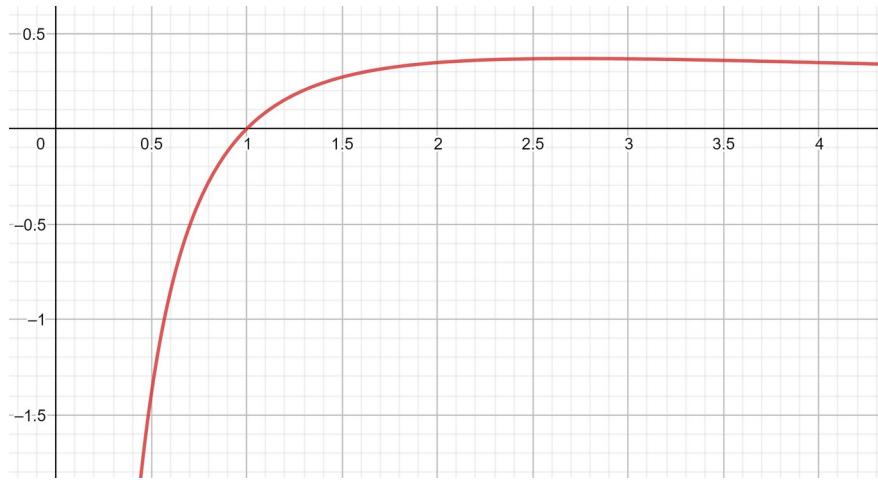
$$q \ln p = p \ln q$$

so:

$$\frac{\ln p}{p} = \frac{\ln q}{q}$$

Here is the graph:

$$y = \frac{\ln x}{x}$$



We want two different  $x$  values, call them  $p$  and  $q$  with the same  $y$  value.

So we want to be able to draw a horizontal line that cuts the graph twice.

Use differentiation to show that the maximum point on the graph occurs at  $x=e$

Hence show that  $2^4=4^2$  is the only solution of  $p^q=q^p$  if  $p$  and  $q$  are positive integers.

Also

The maximum on the graph occurs at  $x=e$

So:

$$\frac{\ln e}{e} > \frac{\ln x}{x} \text{ for any } x \text{ value, in particular } \frac{\ln e}{e} > \frac{\ln \pi}{\pi}$$

Show:

$$\pi \ln e > e \ln \pi$$

Show:

$$e^\pi > \pi^e$$

## Grid Puzzles

### EXERCISE

1)

There are 3 people, Alice, Bill and Jane. One lives in Redland, one lives in Knowle and one lives in Easton. Alice does not live in Easton. Bill lives in Redland. Who lives where?

We put this information onto a grid:

	Redland	Knowle	Easton
Alice			X
Bill	✓		
Jane			

Each row and each column has one ✓ and two X. Can you complete the grid?

2)

There are 3 people, Alice, Bill and Jane. One lives in Redland, one lives in Knowle and one lives in Easton. Alice does not live in Redland. Jane lives in Knowle. Who lives where?

3)

There are 3 people, Alice, Bill and Jane. One lives in Redland, one lives in Knowle and one lives in Easton. One drives a Volvo, one drives a Ford and one drives a Honda. Alice does not live in Easton. The Honda driver does not live in Easton. The Ford driver lives in Redland. Bill drives the Honda. Who lives where and who drives what?

We put this information onto a more complicated grid:

	Redland	Knowle	Easton	Volvo	Ford	Honda
Alice			X			
Bill						✓
Jane						
Volvo				*	*	*
Ford	✓			*	*	*
Honda			X	*	*	*

Can you complete the grid? It's not so easy. Think of it as three  $3 \times 3$  grids where each row and each column has one ✓ and two X. Ignore the \* squares.

4)

There are 3 people, Alice, Bill and Jane. One lives in Redland, one lives in Knowle and one lives in Easton. One drives a Volvo, one drives a Ford and one drives a Honda. Alice drives the Volvo. The Honda driver does not live in Knowle. Jane does not live in Easton. Bill lives in Redland. Who lives where and who drives what?

## SOLUTIONS

1)

	Redland	Knowle	Easton
Alice	X	✓	X
Bill	✓	X	X
Jane	X	X	✓

2)

	Redland	Knowle	Easton
Alice	X	X	✓
Bill	✓	X	X
Jane	X	✓	X

3)

	Redland	Knowle	Easton	Volvo	Ford	Honda
Alice			X			X
Bill				X	X	✓
Jane						X
Volvo	X	X	✓	*	*	*
Ford	✓	X	X	*	*	*
Honda	X	✓	X	*	*	*

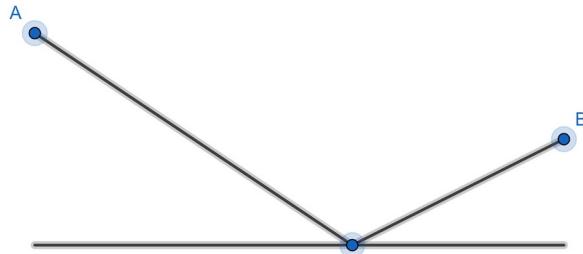
You might be stuck at this point. But, Bill drives the Honda and the Honda lives in Knowle so Bill lives in Knowle. Now can you complete the grid?

4)

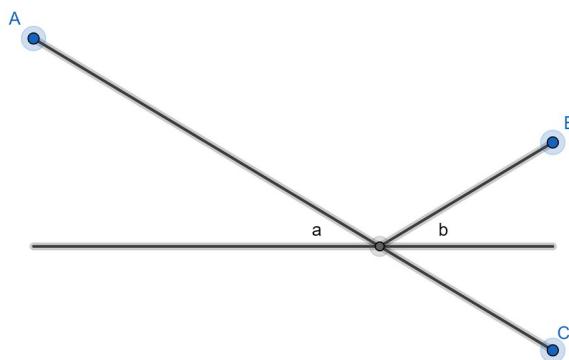
	Redland	Knowle	Easton	Volvo	Ford	Honda
Alice	X	X	✓	✓	X	X
Bill	✓	X	X	X	X	✓
Jane	X	✓	X	X	✓	X
Volvo	X	X	✓	*	*	*
Ford	X	✓	X	*	*	*
Honda	✓	X	X	*	*	*

## Heron's Theorem

We want to find the shortest path from point A to the line and back to point B.



Reflect point B in the line to get point C



The distance from point A to the line and back to point B, is the same as the distance from point A to the line and on to point C. The shortest path from point A to the line and on to point C is a straight line. So the shortest path from point A to the line and back to point B is where angle  $a$  is equal to angle  $b$ . This is Heron's theorem.

Incidentally, if light travelled from point A to the line (which acts as a mirror) and back to point B then it would take this path (remember, angle of incidence equals angle of reflection)

## How To Tune A Piano

When you press a key on a piano, a hammer hits a string and the string vibrates. The frequency of this vibration determines the pitch of the note. For example, a string vibrating 261.6 times per second will produce the note middle C. We write 261.6 times per second as 261.6 Hz

The interval between two notes is the ratio of their frequencies.

The interval between 800 Hz and 600 Hz is  $800/600 = 4/3$

Look at this sequence of notes:

200 Hz, 300 Hz, 450 Hz, 675 Hz, ...

Now

$$\frac{300}{200} = \frac{450}{300} = \frac{675}{450} = \dots = \frac{3}{2}$$

So the intervals between consecutive notes are the same. The frequencies of the notes form a geometric sequence with common ratio  $3/2$  (see Appendix 2: Geometric Sequence)

If one note has twice the frequency of another note then the interval between these notes is called an octave. In western European music, the octave is divided into 12 intervals. So if one note on the piano has frequency 440 Hz then the note, one octave above, has frequency 880 Hz and we need to put another eleven notes in-between. What are the frequencies of these other notes?

If we want equal intervals between consecutive notes then the frequencies must form a geometric sequence:

$$440 \quad 440r^1 \quad 440r^2 \quad 440r^3 \quad \dots \quad 440r^{11} \quad 440r^{12}$$

We want:

$$440r^{12} = 880 \text{ so } r^{12} = 2 \text{ so } r = 2^{1/12}$$

This gives the following frequencies:

440	466.2	493.9	523.3	554.4	587.3	622.3	659.3	698.5	740.0	784.0	830.6	880
A	A#	B	C	C#	D	D#	E	F	F#	G	G#	A

The names of the notes are given below the frequencies.

Notes one octave apart are given the same name.

Once we know the frequencies of all the notes in one octave we can calculate the frequencies of all the notes on the piano.

To find the frequencies of the notes in the octave above we just double these frequencies.

To find the frequencies of the notes in the octave below we just halve these frequencies.

etc

This method for tuning a piano is called equal-tempered tuning because there are equal intervals between the consecutive notes.

Why do we want equal intervals between consecutive notes on the piano?

Here are the first seven notes of “Twinkle Twinkle Little Star”:

523.3 Hz 523.3 Hz 784.0 Hz 784.0 Hz 880 Hz 880 Hz 784.0 Hz

We can play this on the piano. But what if someone says they can't sing notes that low. Can we play the same tune only higher?

If we multiply the frequencies of all these notes by say  $r^3$  then we get:

622.3 Hz 622.3 Hz 932.3 Hz 932.3 Hz 1046.5 Hz 1046.5 Hz 932.3 Hz

All these notes are on the piano. This version of the song has all the same intervals as the first version. It will sound just the same. Only higher.

Musicologists (including Pythagoras) have claimed that two notes sound nice when played together if the interval between them is a simple ratio. So 600 Hz and 400 Hz sound nice when played together because  $600/400=3/2$  is a simple ratio.

Unfortunately, if we use equal-tempered tuning then the interval between any two notes (apart from octaves) is not a simple ratio. It is irrational.

Fortunately, some interval are nearly simple ratios.

The interval between say C and G is  $2^{7/12}$  which is nearly  $3/2$

The interval between say C and F is  $2^{5/12}$  which is nearly  $4/3$

The interval between say C and E is  $2^{4/12}$  which is nearly  $5/4$

Musicologists (including Pythagoras) have devised tuning schemes with lots of simple ratios. But these do not have equal intervals between consecutive notes. So we have a problem.

We want equal intervals. We want simple ratios. We can't have both.

A piano creates a sound with a vibrating string. A bugle creates a sound with a vibrating column of air. A skilled player can produce different notes on a bugle by altering the way their lips vibrate.

Physics tells us that if the lowest note you can get on a bugle is 110Hz then the other notes you can get are: 220 Hz, 330 Hz, 440 Hz, 550 Hz, 660 Hz, ...

110 Hz is an A

220 Hz is an A

330 Hz is nearly an E (329.6Hz)

440 Hz is an A

550 Hz is nearly a C# (554.4Hz)

660 Hz is nearly an E (659.3Hz)

So the bugle notes don't quite match up with the piano notes.

"The Last Post" is played on a bugle with the notes:

220 Hz, 330 Hz, 440 Hz, 550 Hz, 660 Hz

It will sound slightly different if you play it on a piano.

J.S.Bach wrote a piece of music called The Well-Tempered Clavier to demonstrate the advantages of equal-tempered tuning. Check it out.

## Infinite Numbers

I walk into a classroom and see that every student is sitting on a chair and every chair has a student sitting on it. We can pair-up the students with the chairs, so there must be the same number of each.

### Example 1

We can pair-up the positive integers with the even positive integers:

1	2	3	4	...
2	4	6	8	...

So there are the same number of positive integers and even positive integers.

### Example 2

We can pair-up the positive integers with the squares:

1	2	3	4	...
1	4	9	16	...

So there are the same number of positive integers and squares.

### Example 3

We can pair-up the positive integers with all the integers:

1	2	3	4	5	6	7	8	...
0	1	-1	2	-2	3	-3	4	...

So there are the same number of positive integers and integers.

### Example 4

Can we pair-up the positive integers with the positive rational numbers?

We cannot write a list of all the positive rational numbers in numerical order, because between any two positive rational numbers we can always find another positive rational number.

for example: half way between  $\frac{a}{b}$  and  $\frac{c}{d}$  is  $\frac{ad+bc}{2bd}$

However, we can write a list of all the positive rational numbers. Look at this table:

1/1					
1/2	2/1				
1/3	2/2	3/1			
1/4	2/3	3/2	4/1		

1/5	2/4	3/3	4/2	5/1	
...	...	...	...	...	...

We can read-off the positive rational numbers along the rows of the table:

1/1    1/2    2/1    1/3    3/1    1/4    2/3    3/2    4/1 ...

This is a list of all the positive rational numbers.

note: we omitted 2/2 because we have already had 1/1 etc

We can now pair-up the positive integers with the positive rational numbers:

1	2	3	4	5	6	7	8	...
1/1	1/2	2/1	1/3	3/1	1/4	2/3	3/2	...

So there are the same number of positive integers and positive rational numbers. Even though, between any two consecutive integers there are an infinite number of rational numbers.

### Example 5

Can we pair-up the positive integers with the real numbers, between 0 and 1?

We cannot write a list of all the real numbers between 0 and 1, in numerical order, because between any two real numbers we can always find another real number.

for example: half way between  $x$  and  $y$  is  $\frac{x+y}{2}$

We thought of a clever trick so we could write a list of all the positive rational numbers, so perhaps we can think of another clever trick so we could write a list of all the real numbers between 0 and 1.

Say, here is our list of all the real numbers, between 0 and 1

0.475922... , 0.887885... , 0.490035... , 0.186792... , 0.676764... , ...

We can now pair-up the positive integers with the real numbers between 0 and 1:

1	2	3	4	5	...
0.475922...	0.887885...	0.490035...	0.186792...	0.676764...	...

Now this won't do. I can always find a real number between 0 and 1, that is not on the list.

For example 0.59187... is not on the list. How do we know this?

It is not the first number on the list because it has a different first decimal place. It is not the second number on the list because it has a different second decimal place. It is not the third number on the list because it has a different third decimal place, etc

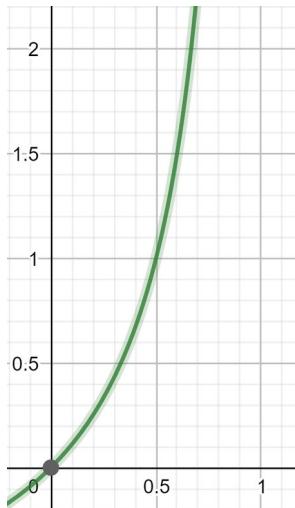
We cannot pair-up the positive integers with the real numbers between 0 and 1.

There are more real numbers between 0 and 1, than positive integers.

### Example 6

We can pair-up the real numbers between 0 and 1 with the positive real numbers.

Look at the graph  $y = \frac{x}{1-x}$  for  $0 \leq x < 1$  and  $0 \leq y < \infty$



We can pair-up each  $x$  value with each  $y$  value.

There are the same number of real numbers between 0 and 1, and positive real numbers.

Subsets:

The finite set  $F$  has 3 members:  $\{p, q, r\}$

A subset of  $F$  is a selection of none, some or all of the members of  $F$

To form a subset, we have 2 choices, include or exclude  $p$ . For each of these choices we have 2 choices, include or exclude  $q$ . For each of these choices we have 2 choices, include or exclude  $r$ . So there are  $2 \times 2 \times 2 = 8$  choices and therefore 8 possible subsets.

The subsets of  $F$  are:  $(\emptyset), (p), (q), (r), (p, q), (p, r), (q, r), (p, q, r)$

In general:

A set with  $n$  members has  $2^n$  subsets

### Example 7

$A = \{1, 2, 3, \dots\}$  is the set of positive integers.

Can we pair-up the members of  $A$  with the subsets of  $A$ ?

Let's say we have thought of a clever trick and we can pair-up the members of  $A$  with the subsets of  $A$  like this:

1	2	3	4	5	...
$\{3, 19, 47\}$	$\{3, 4, 6, \dots\}$	$\{1, 3\}$	$\{2, 5, \dots\}$	$\{3, 5, 7, \dots\}$	...
$X$	$X$	$\checkmark$	$X$	$\checkmark$	...

$1 \leftrightarrow (3, 19, 47)$  we put a  $X$  below because 1 is not a member of this subset.

$2 \leftrightarrow (3, 4, 6, \dots)$  we put a  $X$  below because 2 is not a member of this subset.

$3 \leftrightarrow (1, 3)$  we put a  $\checkmark$  below because 3 is a member of this subset.

etc

One of the subsets of  $A$  is  $C = (1, 2, 4, \dots)$  The set of all the integers with a  $X$

As  $C$  is a subset of  $A$  it must be paired-up with a member of  $A$

Let's say  $N$  is the positive integer that we pair-up with  $C$

Is  $N$  a  $\checkmark$  or a  $X$  integer?

If  $N$  is a  $\checkmark$  integer then  $N$  is a member of  $C$  so  $N$  is a  $X$  integer

If  $N$  is a  $X$  integer then  $N$  is a member of  $C$  so  $N$  is a  $\checkmark$  integer

Contradiction.

We cannot pair-up the members of  $A$  with the subsets of  $A$

There are more subsets of  $A$  than members of  $A$

One of the subsets of  $A$  is  $(1, 4, 5, 7, \dots)$

We could use an alternative notation to denote this subset.

We could write it as  $[1, 0, 0, 1, 1, 0, 1, \dots]$

The 1 in the 1<sup>st</sup> position denotes: include the integer 1

The 0 in the 2<sup>nd</sup> position denotes: exclude the integer 2

The 0 in the 3<sup>rd</sup> position denotes: exclude the integer 3

The 1 in the 4<sup>th</sup> position denotes: include the integer 4

etc

We can think of  $[1, 0, 0, 1, 1, 0, 1, \dots]$  as representing 0.1001101...

We can think of 0.1001101... as a real number (written in binary) between 0 and 1

So we can pair-up any subset of  $A$  with a real number between 0 and 1

There are the same number of subsets of  $A$  and real numbers between 0 and 1

Let  $\infty_1$  be the number of positive integers.

Let  $\infty_2$  be the number of positive real numbers between 0 and 1.

We know that  $\infty_2 = 2^{\infty_1}$  and  $\infty_2 > \infty_1$

### Cantor's Theorem

A set with  $\infty$  members will have  $2^\infty$  subsets and  $2^\infty > \infty$

So we can generate an unending sequence of bigger and bigger infinite numbers:

$$\infty_1 \quad \infty_2 = 2^{\infty_1} \quad \infty_3 = 2^{\infty_2} \quad \infty_4 = 2^{\infty_3} \quad \dots$$

### EXERCISE

The rooms in Hilbert's Hotel hotel are numbered 1, 2, 3, 4, 5 ... (this hotel has an infinite number of rooms). All the rooms are taken. A new guest arrives and asks for a room.

"No problem" says the owner "we can fit you in"

a) how can this be done?

Later that day, an infinite number of new guests arrive and each one asks for a room.

"No problem" says the owner "we can fit you all in"

b) how can this be done?

### SOLUTION

a) The owner moves:

- the person in room 1, to room 2
- the person in room 2, to room 3
- the person in room 3, to room 4 etc

The new guest is given room 1.

b) The owner moves:

- the person in room 1, to room 2
- the person in room 2, to room 4
- the person in room 3, to room 6 etc

The new guests are given rooms 1, 3, 5, ...

## Infinite series

### Example 1

We say the infinite series  $\frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \dots$  converges. What does this mean?

As we add up more and more terms ...

$$\frac{1}{2^1} = \frac{1}{2} \quad \frac{1}{2^1} + \frac{1}{2^2} = \frac{3}{4} \quad \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} = \frac{7}{8} \quad \frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} = \frac{15}{16} \quad \dots$$

the total gets bigger and bigger but never exceeds a certain number (in this case, 1)

### Example 2

We say the infinite series  $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$  diverges. What does this mean?

As we add up more and more terms ...

$$\frac{1}{1} = 1 \quad \frac{1}{1} + \frac{1}{2} = \frac{3}{2} \quad \frac{1}{1} + \frac{1}{2} + \frac{1}{3} = \frac{11}{6} \quad \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12} \quad \dots$$

the total gets bigger and bigger and will eventually exceed any number.

### Proof

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots = \left( \frac{1}{1} \right) + \left( \frac{1}{2} \right) + \left( \frac{1}{3} + \frac{1}{4} \right) + \left( \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} \right) + \dots$$

The value of each bracket on the RHS is greater than  $1/2$

So:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots > \left( \frac{1}{2} \right) + \left( \frac{1}{2} \right) + \left( \frac{1}{2} \right) + \left( \frac{1}{2} \right) + \dots$$

So the series will eventually exceed any number.

Here is another proof (by contradiction)

Assume the series converges to some finite number  $S$

$$\text{So: } S = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \dots$$

$$\text{So: } S > \frac{1}{2} + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{6} + \frac{1}{6} + \dots$$

$$\text{So: } S > \left( \frac{1}{2} + \frac{1}{2} \right) + \left( \frac{1}{4} + \frac{1}{4} \right) + \left( \frac{1}{6} + \frac{1}{6} \right) + \dots$$

$$\text{So: } S > \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots$$

$$\text{So: } S > S$$

Contradiction.

The series:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots$$

is called the harmonic series. It diverges but very slowly. The sum of the first billion terms is only about 21.3

Example 3

Compare the series:  $\frac{1}{2^1} + \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{2^4} + \dots$  with the series:  $\frac{1}{2^1} + \frac{1}{3^2} + \frac{1}{4^3} + \frac{1}{5^4} + \dots$

The terms in the second series are equal to or smaller than the corresponding terms in the first series. We know the first series converges so the second series must converge.

Example 4

Compare the series:  $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \dots$  with the series:  $\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \frac{1}{\sqrt{4}} + \frac{1}{\sqrt{5}} + \dots$

The terms in the second series are equal to or larger than the corresponding terms in the first series. We know the first series diverges so the second series must diverge.

Example 5

Look at this series:  $\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots$

Show that:  $\frac{1}{k^2} < \frac{2}{k(k+1)}$  for any  $k > 1$

Show that:  $\frac{2}{k} - \frac{2}{k+1} = \frac{2}{k(k+1)}$

Show that:  $\sum_{k=1}^{\infty} \frac{1}{k^2} < \sum_{k=1}^{\infty} \left( \frac{2}{k} - \frac{2}{k+1} \right) = \left( \frac{2}{1} - \frac{2}{2} \right) + \left( \frac{2}{2} - \frac{2}{3} \right) + \left( \frac{2}{3} - \frac{2}{4} \right) + \dots$

Show that:  $\sum_{k=1}^{\infty} \frac{1}{k^2} < 2$

So the series converges.

If you study maths at a higher level you will learn how to manage infinite series properly.

In the meantime we can have some fun ...

Example 6

Evaluate:  $S = \frac{1}{1} - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \dots$

Now:  $S = \left( 1 - \frac{1}{2} \right) + \left( \frac{1}{3} - \frac{1}{4} \right) + \left( \frac{1}{5} - \frac{1}{6} \right) + \dots$

So:  $S > 0$

$$\text{But: } S = \left( \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \dots \right) - 2 \left( \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \dots \right) = \left( \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots \right) - \left( \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots \right)$$

So:  $S=0$

Example 7

Evaluate:  $S=1-1+1-1+1-1+\dots$

1<sup>st</sup> attempt:  $S=(1-1)+(1-1)+(1-1)+\dots$   $S=0$

2<sup>nd</sup> attempt:  $S=1-(1-1)-(1-1)-(1-1)-\dots$   $S=1$

3<sup>rd</sup> attempt:  $S=1-(1-1+1-1+1-1+\dots)=1-S$   $S=1/2$

Example 8

Evaluate:  $S=1+2+4+8+\dots$

Now:  $2S=2+4+8+16+\dots$

So:  $2S-S=(2+4+8+16+\dots)-(1+2+4+8+16+\dots)$

So:  $S=-1$

Example 9

Evaluate:  $S=1-2+4-8+\dots$

1<sup>st</sup> attempt:  $S=1+(-2+4)+(-8+16)+\dots$   $S \rightarrow \infty$

2<sup>nd</sup> attempt:  $S=(1-2)+(4-8)+\dots$   $S \rightarrow -\infty$

3<sup>rd</sup> attempt:  $S=1-2(1-2+4-8+\dots)=1-2S$   $S=1/3$

Example 10

$$U = \frac{1}{1} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \dots \quad \text{and} \quad V = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} + \dots$$

$$\text{So: } U+V = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots = 2V$$

So:  $U=V$

$$\text{But: } U-V = \left( \frac{1}{1} - \frac{1}{2} \right) + \left( \frac{1}{3} - \frac{1}{4} \right) + \left( \frac{1}{5} - \frac{1}{6} \right) + \dots$$

So:  $U>V$

Example 11

Now:  $(1+x)^{-1}=1-x+x^2-x^3+x^4-\dots$  it's a geometric series

So if we sub in  $x=2$  we get:  $1-2+4-8+16-\dots=\frac{1}{3}$

And if we sub in  $x=-2$  we get:  $1+2+4+8+16+\dots=-1$

Example 12

Now:  $(1+x)^{-1}=1-x+x^2-x^3+x^4-\dots$  it's a geometric series

If we differentiate we get:  $(1-x)^{-2}=1+2x+3x^2+4x^3+\dots$

So if we sub in  $x=-1$  we get:  $1-2+3-4+\dots=\frac{1}{4}$

Example 13

Now:  $\frac{1}{1+x^2}=1-x^2+x^4-x^6+\dots$  it's a geometric series

So if we sub in  $x=1$  we get:  $1-1+1-1+\dots=\frac{1}{2}$

Example 14

We know:  $a=1-1+1-1+1-1+\dots=\frac{1}{2}$  see example 14

We know:  $b=1-2+3-4+5-6+\dots=\frac{1}{4}$  see example 13

Let:  $c=1+2+3+4+5+6+\dots$

So:  $b-c=(1-2+3-4+5-6+\dots)-(1+2+3+4+5+6+\dots)$

So:  $b-c=(1-1)+(-2-2)+(3-3)+(-4-4)+(5-5)+(-6-6)+\dots$

So:  $b-c=0-4+0-8+0-12+\dots=-4-8-12-\dots=-4(1+2+3+\dots)=-4c$

So:  $b=-3c$  but  $b=\frac{1}{4}$  so  $c=-\frac{1}{12}$

Hence:  $1+2+3+4+5+6+\dots=-\frac{1}{12}$

Example 15

Consider the series:  $a_1+a_2+a_3+a_4+\dots$

$$a_1=a_1$$

$$a_2=(a_1+a_2)-a_1$$

$$a_3=(a_1+a_2+a_3)-(a_1+a_2)$$

$$a_4=(a_1+a_2+a_3+a_4)-(a_1+a_2+a_3) \text{ etc}$$

The terms on the LHS sum to:

$$a_1+a_2+a_3+a_4+\dots$$

The terms on the RHS all cancel.

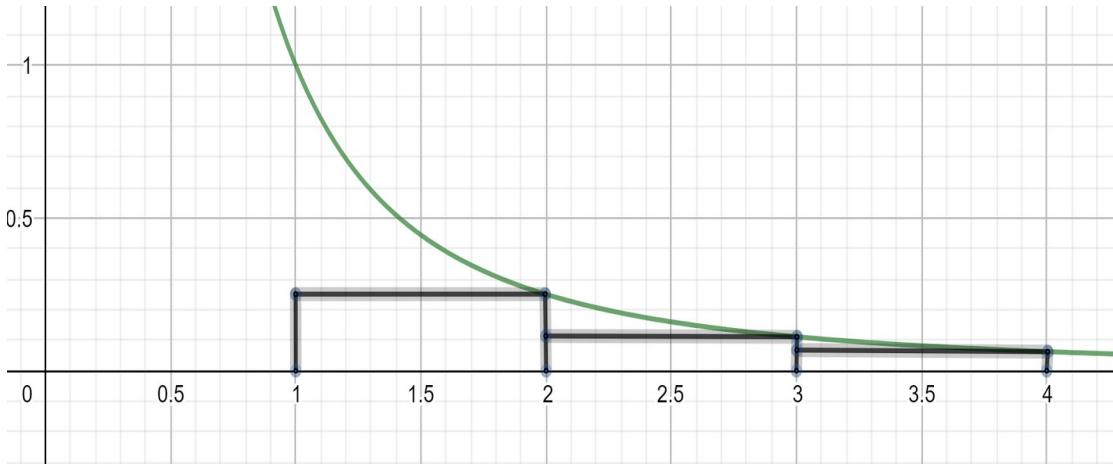
$$\text{So } a_1+a_2+a_3+a_4+\dots=0$$

Every infinite series sums to zero. We should have done this example first!

If you know about integration ...

Example

Here is the graph  $y=\frac{1}{x^2}$



The diagram shows blocks between  $x=1$  and  $x=4$

The area of the blocks is:  $\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \dots$

The area under the graph is:  $\int_1^\infty \frac{1}{x^2} dx = 1$

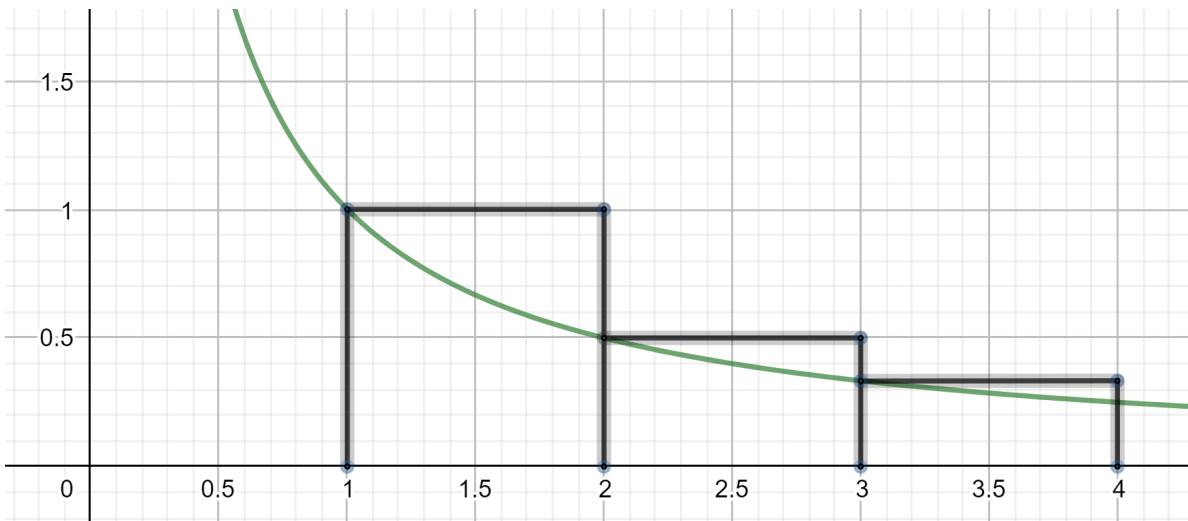
The area of the blocks is less than the area under the graph.

So:  $\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \dots < 1$

So:  $\frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \dots$  converges.

Example

Here is the graph  $y = \frac{1}{x}$



The area of the blocks is:  $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$

The area under the graph is:  $\int_1^{\infty} \frac{1}{x} dx \rightarrow \infty$

The area of the blocks is greater than the area under the graph.

So:  $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$  diverges.

## Knight Tours

### Example 1

Here is a knight tour on a  $6 \times 6$  board:

1	28	15	12	3	34
16	11	2	35	22	13
27	36	29	14	33	4
10	17	8	23	30	21
7	26	19	32	5	24
18	9	6	25	20	31

The knight must visit each square once (and only once). The squares are numbered in the order they are visited by the knight. The knight starts on square 1, moves to square 2, moves to square 3, ... and ends on square 36.

This is a closed tour because the end square (36) is a knight move from the start square (1)

Any tour can be reversed. The knight could move: 36, 35, 34, ... 3, 2, 1

We can think of a closed tour as starting on any square. We can think of the above tour as starting on square 17. The knight could move: 17, 18, 19, ... 36, 1, 2, 3, ... 16

### Example 2

Here is another knight tour:

1	20	25	8	3	18
26	9	2	19	32	7
21	24	33	6	17	4
10	27	22	35	14	31
23	34	29	12	5	16
28	11	36	15	30	13

This is an open tour because the end square (36) is not a knight move from the start square (1)

This tour could be reversed. This tour could not start on any square.

## Theorem

There is no closed tour on any  $N \times N$  board where  $N$  is odd.

### Proof

We can colour the squares on a board, black and white. Like a chess board. A knight on a black square can only move to a white square. A knight on a white square can only move to a black square. If the start square of a closed tour is black then the end square must be white, because the end square is a knight move from the start square. So there must be the same number of black and white squares. This won't happen on an  $N \times N$  board if  $N$  is odd.

### Theorem

There are no closed tours on a  $2 \times 2$  board.

### Proof

Just think about it.

### Theorem

There are no closed tours on a  $4 \times 4$  board.

### Proof

We can colour the board, black and white.

W	B	W	B
B	W	B	W
W	B	W	B
B	W	B	W

The knight must alternate between black and white squares.

We can colour the board, red and green.

R	R	R	R
G	G	G	G
G	G	G	G
R	R	R	R

A knight on a red square can only move to a green square. We can think of a closed tour as starting on any square. If the start square is red then the end square must be green, because the end square is a knight move from the start square. The knight must visit the same number of red and green squares. So the knight must alternate between red and green squares.

If the knight starts on the bottom left hand corner square, which is a black/red square then it can only move to a white/green square then to a black/red square etc. It isn't ever going to visit the black/green squares or the white/red squares. So there is no closed tour on a  $4 \times 4$  board.

### Schwenk's Closed Tour Theorem

- a) There is no closed tour on any  $N \times N$  board where  $N$  is odd.
- b) There is a closed tour on every  $N \times N$  board where  $N$  is even and greater than 4.

Have we proved Schwenk's theorem?

We have proven part (a)

What about part (b)?

Schwenk says: if  $N$  is even and greater than 4 then there is a closed tour

We have proved: if  $N$  is even and isn't greater than 4 then there isn't a closed tour

Not the same thing at all.

### Example 3

Here is a tour on a  $5 \times 5$  board:

3	10	21	16	5
20	15	4	11	22
9	2		6	17
14	19	8	23	12
1	24	13	18	7

We can finish by going into the middle square.

### Example 4

Here is a tour on a  $9 \times 9$  board: CHECK THIS

5	20	47	34	7	22	49	36	9
46	33	6	21	48	35	8	23	50
19	4						10	37
32	45						51	24
3	18						38	11
44	31						25	52
17	2						12	39
30	42	16	55	28	41	14	53	26

1	56	29	42	15	54	27	40	13
---	----	----	----	----	----	----	----	----

We can finish by going into the middle  $5 \times 5$  square.

Try this method on a  $13 \times 13$  board.

See EXERCISE 1

Example 5

Here is a tour on a chess-board:

1	48	31	50	33	16	63	18
30	51	46	3	62	19	14	35
47	2	49	32	15	34	17	64
52	29	4	45	20	61	36	13
5	44	25	56	9	40	21	60
28	53	8	41	24	57	12	37
43	6	55	26	39	10	59	22
54	27	42	7	58	23	38	11

Amusingly, the numbers in each column and each row add up to the same total.

We call this a semi-magic square.

There are many methods to find knight tours. Look them up.

See Exercise

EXERCISE

1)

I am looking for a tour on this board:


		A			

Why will I fail if I start at square A?

2)

Look at this  $6 \times 6$  board:

B	D	A	C	B	D
A	C	B	D	A	C
D	B			D	B
C	A			C	A
B	D	A	C	B	D
A	C	B	D	A	C

The knight can tour all the A squares. The knight can tour all the B squares, etc.

Can you find a tour by linking up these cycles, using the middle squares?

3)

Look at this  $8 \times 8$  board:

D	B	C	A	D	B	C	A
C	A	D	B	C	A	D	B
B	D	A	C	B	D	A	C
A	C	B	D	A	C	B	D
D	B	C	A	D	B	C	A
C	A	D	B	C	A	D	B
B	D	A	C	B	D	A	C
A	C	B	D	A	C	B	D

The knight can tour all the A squares. The knight can tour all the B squares, etc.

Can you find a tour by linking up these cycles?

4)

Divide and conquer methods involve dividing the board into parts and touring each part separately.

Here is a  $10 \times 10$  board:

5	16	21	12	7					
22	11	6	15	20					

17	4	13	8	25				
10	23	2	19	14				
3	18	9	24	1				

We divide the board into four  $5 \times 5$  quarter boards and tour each quarter board separately.

A tour of the top left hand corner quarter board is shown.

Rotate this  $90^\circ$  clockwise and place in the top right hand corner. Rotate again for the bottom right hand corner. Rotate again for the bottom left hand corner. Now join up these four quarter board tours. Unfortunately, we cannot use this method on an  $8 \times 8$  board because there are no tours of a  $4 \times 4$  board.

## SOLUTIONS

1)

Let's colour the board black and white, with the bottom left-hand corner black. There are 13 black squares and 12 white squares. The knight must alternate between black and white squares. So this will only work if the tour goes B, W, B, W, ... B. Unfortunately, the start square is white.

2)

16	23	4	31	10	25			
3	30	17	24	5	32			
22	15	36	9	26	11			
29	2	27	18	33	6			
14	21	8	35	12	19			
1	28	13	20	7	34			

3)

38	55	22	13	36	51	18	11
23	14	37	54	17	12	35	50
56	39	16	21	52	33	10	19
15	24	53	40	9	20	49	34
42	57	28	1	48	61	32	7

25	2	41	60	29	8	47	62
58	43	4	27	64	45	6	31
3	26	59	44	5	30	63	46

4)

5	16	21	12	7	28	35	42	47	30
22	11	6	15	20	43	49	29	36	41
17	4	13	8	25	34	27	38	31	46
10	23	2	19	14	49	44	33	40	37
3	18	9	24	1	26	39	50	45	32
82	95	100	89	76	51	74	59	67	53
87	90	83	94	99	64	69	52	73	60
96	81	88	77	84	75	58	63	54	67
91	86	79	98	93	70	65	56	61	72
80	97	92	85	78	57	62	71	66	55

Lanchester model

if you know about differential equations ...

In a tank battle, one army has  $x$  tanks and the other army has  $y$  tanks. We are going to assume that the rate at which one army's tanks are destroyed is proportional to the number of tanks in the opposing army.

So:

$$\frac{dx}{dt} = -k_1 y \quad \text{and} \quad \frac{dy}{dt} = -k_2 x$$

Let's also assume that each army is equally good at aiming so that:

$$k_1 = k_2$$

Dividing these equations gives:

$$\frac{dy}{dx} = \frac{x}{y}$$

$$\text{So } \int y dy \int x dx \quad \text{So} \quad \frac{1}{2} y^2 = \frac{1}{2} x^2 + c \quad \text{So} \quad y^2 = x^2 + 2c$$

So as the battle proceeds  $y^2 - x^2$  will remain constant.

Example

At the start of the battle:

$$x=24 \quad \text{and} \quad y=25$$

Throughout the battle:

$$y^2 - x^2 = 49$$

At the end of the battle:

$$x=0 \quad \text{and} \quad y=7$$

The strength of a tank army is not proportional to the number of tanks but to the square of the number of tanks. This means weird stuff can happen.

Example

I start with 30 tanks and you start with 42 tanks. In one big battle with all the tanks, I am going to lose. But what if I could arrange some small skirmishes.

If 5 of my tanks engage with 3 of your tanks, then at the end of this skirmish, I'll have 4 tanks and you will have no tanks. If I keep doing this, then I'll soon have more tanks than you!

## Lewis Carroll

Charles Dodgson (1832 – 1898) was a mathematics lecturer at Oxford University. He was also the author of several books for children, which he wrote under the pen-name, Lewis Carroll. His two most famous books are:

Alice's Adventures In Wonderland and Through The Looking Glass.

These books have always been popular with mathematicians and you should read them. It might be best to read The Annotated Alice by Martin Gardner as this book explains the jokes and the logic which are easy to miss. Here are some quotes from these books:

Alice laughed, "There's no use trying" she said, "one can't believe impossible things."

"I daresay you haven't had much practice," said the Queen. "When I was younger, I always did it for half an hour a day. Why, sometimes I've believed as many as six impossible things before breakfast."

"Take some more tea" the March Hare said to Alice very earnestly.

"I've had nothing yet" Alice replied in an offended tone "so I can't take more."

"You mean you can't take less" said the Hatter "it's very easy to take more than nothing"

"Then you should say what you mean," the March Hare went on.

"I do, " Alice hastily replied, "at least I mean what I say, that's the same thing, you know."

"Not the same thing a bit!" said the Hatter. "Why, you might just as well say that "I see what I eat" is the same thing as "I eat what I see!"

"It's very good jam," said the Queen.

"Well, I don't want any to-day, at any rate."

"You couldn't have it if you did want it," the Queen said. "The rule is jam tomorrow and jam yesterday but never jam to-day."

"It must come sometimes to "jam to-day," Alice objected.

"No it can't," said the Queen. "It's jam every other day; to-day isn't any other day, you know."

"When I use a word," Humpty Dumpty said, in a rather scornful tone, "it means just what I choose it to mean, neither more nor less."

"The question is," said Alice, "whether you can make words mean so many different things."

"The question is," said Humpty Dumpty, "which is to be master, that's all."

Maclaurin Series

if you know about differentiation and integration ...

Sometimes we can write a function  $f(x)$  as a power series:

$$f(x) = a + bx + cx^2 + dx^3 + ex^4 + \dots$$

Put  $x=0$

$$f(0) = a$$

Differentiate

$$f'(x) = b + 2cx + 3dx^2 + 4ex^3 + \dots$$

Put  $x=0$

$$f'(0) = b$$

Differentiate

$$f''(x) = 2c + (3 \times 2)dx + (4 \times 3)ex^2 + \dots$$

Put  $x=0$

$$f''(0) = 2c$$

Differentiate

$$f'''(x) = (3 \times 2)d + (4 \times 3 \times 2)ex + \dots$$

Put  $x=0$

$$f'''(0) = (3 \times 2)d$$

etc

$$\text{So } f(x) = f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \frac{f''''(0)}{4!}x^4 + \dots$$

Example 1

Lets try this out with  $f(x) = \sin x$

$$f(x) = \sin x \quad f(0) = 0$$

$$f'(x) = \cos x \quad f'(0) = 1$$

$$f''(x) = -\sin x \quad f''(0) = 0$$

$$f'''(x) = -\cos x \quad f'''(0) = -1$$

$$f''''(x) = \sin x \quad f''''(0) = 0$$

etc

$$\text{So } \sin x = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 + \dots$$

Find a graph plotter online and plot the following graphs:

$$y=x$$

$$y = x - \frac{1}{3!}x^3$$

$$\sin x = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5$$

etc

And see how these graphs get more and more like  $y = \sin x$

### Example 2

Show that:

$$\cos x = 1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^4 + \dots$$

### Example 3

Show that:

$$e^x = 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \frac{1}{4!}x^4 + \dots$$

### Example 4

There is a sneaky way to find the Maclaurin series for  $\ln(1+x)$

We start with:

$$1 - x + x^2 - x^3 + \dots = \frac{1}{1+x} \quad \text{it is a geometric series}$$

So:

$$\int \frac{1}{1+x} dx = \int (1 - x + x^2 - x^3 + \dots) dx$$

So:

$$\ln(1+x) = x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \frac{1}{4}x^4 + \dots \quad \text{this is only valid for } -1 < x \leq 1$$

### Example 5

There is also a sneaky way to find the Maclaurin series for  $\tan^{-1} x$

We start with:

$$1 - x^2 + x^4 - x^6 + \dots = \frac{1}{1+x^2} \quad \text{it is a geometric series}$$

So:

$$\int \frac{1}{1+x^2} dx = \int (1 - x^2 + x^4 - x^6 + \dots) dx$$

So:

$$\tan^{-1}x = x - \frac{1}{3}x^3 + \frac{1}{5}x^5 - \frac{1}{7}x^7 + \dots \quad \text{this is only valid for } -1 \leq x \leq 1$$

As a bonus:

show that:

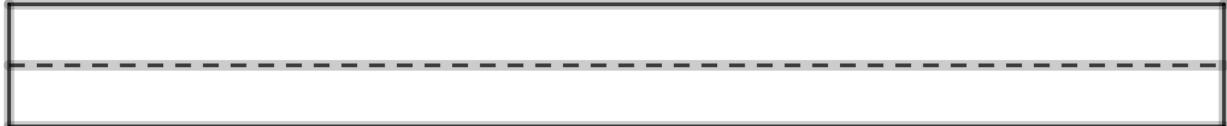
$$\frac{\pi}{4} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$$

## Möbius Strip

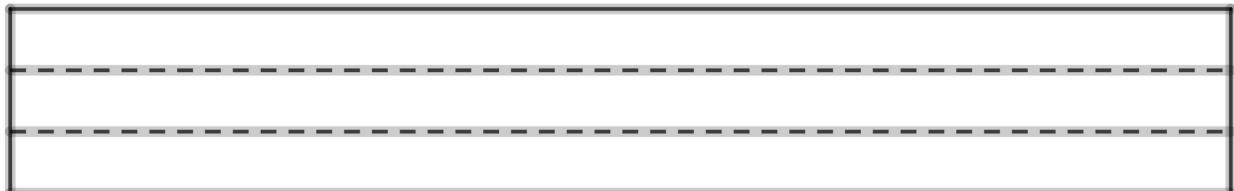
## DIAGRAMS ???

1) Take a long, thin strip of paper. Put one twist in it. Glue the two ends together. This is a Möbius strip. Try painting one side of the Möbius strip red and the other side blue.

2) Take a long, thin strip of paper and draw a dotted line along the length. Put one twist in it. Glue the two ends together. Now cut along the dotted line.



3) Take a long, thin strip of paper and draw two dotted lines along the length. Put one twist in it. Glue the two ends together. Now cut along the dotted line.



4) Play around. Try putting two twists in the strip of paper. Try drawing three dotted lines. etc

Multiples:

rule of 2: 36478 is a multiple of 2 because 8 (the last digit) is a multiple of 2

$$36478 = 36470 + 8 \text{ and } 36470 \text{ is a multiple of 2}$$

rule of 3: 264 is a multiple of 3 because  $2+6+4$  is a multiple of 3

$$264 = 2(100) + 6(10) + 4 = 2(99) + 6(9) + (2+6+4) \text{ and } 2(99) + 6(9) \text{ is a multiple of 3}$$

rule of 4: 94524 is a multiple of 4 because 24 (last two digits) is a multiple of 4

$$94524 = 94500 + 24 \text{ and } 94500 \text{ is a multiple of 4}$$

rule of 5: 743665 is a multiple of 5 because 5 (last digit) is a multiple of 5

$$74365 = 74360 + 5 \text{ and } 74360 \text{ is a multiple of 5}$$

rule of 6: 29622 is a multiple of 6 because 29622 is a multiple of 2 and a multiple of 3

rule of 8: 59136 is a multiple of 8 because 136 (last three digits) is a multiple of 8

$$59136 = 59000 + 136 \text{ and } 59000 \text{ is a multiple of 8}$$

rule of 9: 648 is a multiple of 9 because  $6+4+8$  is a multiple of 9

$$648 = 6(100) + 4(10) + 8 = 6(99) + 4(9) + (6+4+8) \text{ and } 6(99) + 4(9) \text{ is a multiple of 9}$$

rule of 10: 89210 is a multiple of 10 because the last digit is 0

rule of 11: 836 is a multiple of 11 because  $8-3+6$  is a multiple of 11

$$836 = 8(100) + 3(10) + 6 = 8(99) + 3(11) + (8-3+6) \text{ and } 8(99) + 3(11) \text{ is a multiple of 11}$$

## EXERCISE

1)

Is 36470587624275 a multiple of 3?

2)

Is 47385900738828 a multiple of 8?

3)

Is 49775883661205 a multiple of 11?

4)

Show that every palindrome with an even number of digits (like 637736) is a multiple of 11

5)

Show that any 3-digit-repeater (like 726726) is a multiple of 7 and 11 and 13

6)

If  $n$  and  $x$  are positive integers, prove the following using the factor theorem:

- a)  $x^n+1$  is a multiple of  $x+1$  if  $n$  is odd
- b)  $x^n-1$  is a multiple of  $x+1$  if  $n$  is even
- c)  $x^n-1$  is a multiple of  $x-1$

## SOLUTIONS

1)

Yes. Because  $3+6+4+7+0+5+8+7+6+2+4+2+7+5=66$  a multiple of 3

2)

No. Because 828 is not multiple of 8

3)

No. Because  $4-9+7-7+5-8+8-3+6-6+1-2+0-5=-9$  not a multiple of 11

4)

$$6-3+7-7+3-6=0 \text{ and } 0 \text{ is a multiple of 11}$$

5)

$$7 \times 11 \times 13 = 1001 \text{ and } 726726 = 726 \times 1001$$

6)

a) if  $n$  is odd:

$$f(x)=x^n+1 \text{ so } f(-1)=0 \text{ so } (x+1) \text{ is a factor of } f(x)$$

b) if  $n$  is even:

$$f(x)=x^n-1 \text{ so } f(-1)=0 \text{ so } (x+1) \text{ is a factor of } f(x)$$

c)  $f(x)=x^n-1$  so  $f(1)=0$  so  $(x-1)$  is a factor of  $f(x)$

Paint Pot

if you know about integration ...

Take the curve  $y = \frac{1}{x}$  between  $x=1$  and  $x=\infty$  and rotate it  $360^\circ$  around the x axis to form a long, funnel shaped paint pot.

DIAGRAM???

The volume of the paint pot is:

$$\int_1^{\infty} \pi y^2 dx = \int_1^{\infty} \pi \frac{1}{x^2} dx = \dots = \pi$$

The surface area of the paint pot is:

$$\int_1^{\infty} 2\pi y \sqrt{1 + \left(\frac{dy}{dx}\right)^2} dx = \int_1^{\infty} 2\pi \frac{1}{x} \sqrt{1 + \left(\frac{1}{x^4}\right)} dx$$

Now this integral is too difficult for me but ...

$$2\pi \frac{1}{x} \sqrt{1 + \left(\frac{1}{x^4}\right)} > 2\pi \frac{1}{x}$$

So the surface area of the paint pot is greater than:

$$\int_1^{\infty} 2\pi \frac{1}{x} dx = \dots = \infty$$

So the paint pot has a finite volume but an infinite surface area.

If you fill the pot with paint then you won't have enough paint to cover the surface of the pot!

## Paradoxes

### Example 1

Achilles and the tortoise decide to run a race. Because Achilles can run 10 times as fast as the tortoise, the tortoise is given a head start of 100m. The tortoise starts at point A.

By the time Achilles reaches point A, the tortoise has moved on by 10m, to point B.

By the time Achilles reaches point B, the tortoise has moved on by 1m, to point C.

By the time Achilles reaches point C, the tortoise has moved on by 0.1m, to point D.

Each time Achilles reaches the point where the tortoise was, the tortoise has moved on.

So Achilles can never catch up with the tortoise.

### Example 2

In the first half of the cricket season:

Fred faced 475 deliveries and scored 170 runs. John faced 717 deliveries and scored 250 runs.

So Fred had the better batting average.

In the second half of the cricket season:

Fred faced 725 deliveries and scored 185 runs. John faced 483 deliveries and scored 112 runs.

So Fred had the better batting average.

Over the whole season:

Fred faced 1200 deliveries and scored 355 runs. John faced 1200 deliveries and scored 362 runs.

So John had the better batting average.

### Example 3

I claim that all ravens are black. You wish to investigate my claim, so you look at lots of ravens.

Every time you see a raven and it turns out to be black, your confidence in my claim increases.

All ravens are black, means the same as, all non-black things are non-ravens.

So every time you see a non-black thing and it turns out to be a non-raven, your confidence in my claim increases. Suppose you see a yellow thing and it turns out to be a banana. This should increase your confidence in my claim.

### Example 4

There are two envelopes on the table. One envelope contains twice as much money as the other envelope. You can keep one of these envelopes and the money inside. But you are only allowed to look inside one envelope before making your decision. What should you do?

You look inside one envelope. It contains £100. So the other envelope must contain £50 or £200. If you choose to keep the other envelope, you could lose £50 but you are just as likely to gain £100.

So the best plan is to keep the other envelope. You come to this conclusion however much money is in the first envelope. So to save time, choose an envelope, don't bother to look inside it, and keep the other one.

#### Example 5

Teacher Alice sets her pupils a test and their mean score is 60%. Teacher Bill sets his pupils the same test and their mean score is 50%. Susan is in Alice's class. Susan scored 54%. If Susan is moved from Alice's class to Bill's class then the mean score for both classes would increase.

#### Example 6

A naughty girl did not complete her maths homework, so she is to be punished. She is allowed to make one statement. If the statement is true, she will have to clean the board. If the statement is false, she will have to pick-up litter. The girl makes the statement: "I shall have to pick-up litter". So what happens?

#### Example 7

I teach my maths class every Monday, Tuesday, Wednesday, Thursday and Friday. I tell them that they are going to have a test next week. But to add to their misery, they will not know, at the start of each day, if they are getting the test that day. Then one of my brighter students says:

"We can't have the test on Friday, because if we haven't had the test by then, we will know at the start of Friday that we are getting the test that day"

So the test has to take place on Monday, Tuesday, Wednesday or Thursday.

The student then argues that the test can't take place on Thursday or Wednesday or Tuesday or Monday.

The student therefore concludes that I can't give them an unexpected test.

Imagine their surprise when they get the test on Tuesday!

## Pascal's Triangle

The triangle is usually set out like an isosceles triangle but I have set it out slightly differently:

	Col 0	Col 1	Col 2	Col 3	Col 4	Col 5	Col 6	Col 7	Col 8	Col 9
Row 0	1									
Row 1	1	1								
Row 2	1	2	1							
Row 3	1	3	3	1						
Row 4	1	4	6	4	1					
Row 5	1	5	10	10	5	1				
Row 6	1	6	15	20	15	6	1			
Row 7	1	7	21	35	35	21	7	1		
Row 8	1	8	28	56	70	56	28	8	1	
Row 9	1	9	36	84	126	126	84	36	9	1

1) The numbers in the triangle are selection numbers. (see chapter: Arrangements and Selections)

For example, the number in row 9 and column 3 is  $(9C3)$

2) We can generate each row of the triangle from the row above. To generate row 10:

$$(10C0)=1$$

$$(10C1)=(9C0)+(9C1)=1+9=10$$

$$(10C2)=(9C1)+(9C2)=9+36=45$$

$$(10C3)=(9C2)+(9C3)=36+84=120 \text{ etc}$$

3) Look at the numbers in row 7 of Pascal's triangle: 1, 7, 21, 35, 35, 21, 7, 1

$$\text{A typical number in this row is } (7C3)=\frac{7\times 6\times 5\times 4\times 3\times 2\times 1}{(3\times 2\times 1)(4\times 3\times 2\times 1)}$$

After lots of cancelling, we are left with a positive integer. The 7 on the top of the fraction can't be cancelled out by numbers on the bottom of the fraction because 7 is prime. So  $(7C3)$  must be a multiple of 7

In general:

If  $p$  is prime then all the numbers in line  $p$  of Pascal's triangle will be a multiple of  $p$  (apart from the 1 at each end)

#### 4) Binomial theorem for multiplying out brackets

$$(1+x)^1 = 1+x$$

$$(1+x)^2 = 1+2x+x^2$$

$$(1+x)^3 = 1+3x+3x^2+x^3$$

$$(1+x)^4 = 1+4x+6x^2+4x^3+x^4$$

In general: if  $n$  is a positive integer

$$(1+x)^n = (nC0) + (nC1)x + (nC2)x^2 + (nC3)x^3 + \dots + (nCn)x^n$$

sub in  $x=1$   $(nC0) + (nC1) + (nC2) + \dots + (nCn) = 2^n$

sub in  $x=-1$   $(nC0) - (nC1) + (nC2) - (nC3) + \dots = 0$

sub in  $x=2$   $(nC0) + 2(nC1) + 2^2(nC2) + \dots + 2^n(nCn) = 3^n$

etc

By adding or subtracting the first two results we get:

$$(nC0) + (nC2) + (nC4) + \dots = 2^{n-1}$$

$$(nC1) + (nC3) + (nC5) + \dots = 2^{n-1}$$

#### EXERCISE

Write down row 10 of Pascal's triangle.

#### SOLUTION

$$1, 1+9=10, 9+36=45, 36+84=120, 84+126=210, 126+126=252, 126+84=210, 84+36=120,$$

$$36+9=45, 9+1=10, 1$$

## Pigeon-hole Principle

I have 10 boxes and 14 pigeons. I put each pigeon in a box. Obviously one (or more) box must end up with two (or more) pigeons.

How can something so trivial be of any use? Let's find out.

### EXERCISE

1) There are 10 people in a room. Everyone shouts out an integer between 1 and 9

Why must two (or more) people shout out the same integer?

2) There are 40 people at a party. Everyone shakes hands with at least one other person. At the end of the party, everyone is asked: "How many people did you shake hands with?"

Why must two (or more) people give the same reply?

3) Pick 11 different positive integers.

Why must two (or more) of these integers have a difference that is a multiple of ten.

4) Pick 6 different integers from 1, 2, 3, ... 10

Why must two (or more) of these integers add up to 11?

### SOLUTIONS

1) I have 9 boxes, labelled 1, 2, ... 9. I put each person in a box.

If a person shouts out 8 then I put them in the box with 8 on the label. etc

There are 9 boxes and 10 people. One (or more) box must contain two (or more) people.

2) I have 39 boxes, labelled 1, 2, ... 39. I put each person in a box.

If a person shakes hands with 17 people, then I put them in the box with 17 on the label. etc

There are 39 boxes and 40 people. One (or more) box must contain two (or more) people.

Note: each person shakes hands with 1 or 2 or 3 ... or 39 people.

Note: this argument will apply however many people are at the party.

3) I have 10 boxes, labelled 0, 1, 2, ... 9. I put each integer in a box.

If an integer is 3768 then I put it in the box with 8 on the label because 8 is its last digit. etc

There are 10 boxes and 11 integers. One (or more) box must contain two (or more) integers.

Note: integers in the same box have the same last digit so their difference is a multiple of 10

4) I have 5 boxes, labelled A, B, C, D, E. I put each integer in a box.

1 and 10 go in box A.

2 and 9 go in box B.

3 and 8 go in box C.

4 and 7 go in box D.

5 and 6 go in box E.

There are 5 boxes and 6 integers. One (or more) box must contain two (or more) integers.

Note: integers in the same box add up to 11

Pi

Here are some nice formulas for  $\pi$  – there are lots more.

$$\frac{\pi}{4} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$$

$$\frac{\pi}{2} = \frac{2}{1} \times \frac{2}{3} \times \frac{4}{3} \times \frac{4}{5} \times \frac{6}{5} \times \frac{6}{7} \times \dots$$

$$\frac{\pi^2}{6} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots$$

$$\frac{\pi^2}{6} = \left( \frac{1}{1-1/2^2} \right) \left( \frac{1}{1-1/3^2} \right) \left( \frac{1}{1-1/5^2} \right) \left( \frac{1}{1-1/7^2} \right) \left( \frac{1}{1-1/11^2} \right) \dots$$

$\frac{\pi}{4} = \frac{3}{4} \times \frac{5}{4} \times \frac{7}{8} \times \frac{11}{12} \times \frac{13}{12} \dots$  where the numerators are the primes (not including 2) and each denominator is the multiple of 4 nearest to the corresponding numerator.

$$\frac{\pi}{4} = 4 \arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{239}\right)$$

$$\frac{\pi\sqrt{2}}{4} = 1 + \frac{1}{3} - \frac{1}{5} - \frac{1}{7} + \frac{1}{9} + \frac{1}{11} - \dots$$

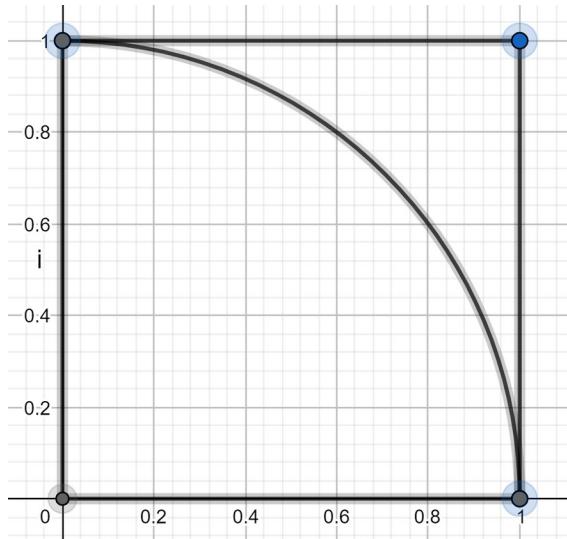
$$\frac{\pi-3}{4} = \frac{1}{2 \times 3 \times 4} - \frac{1}{4 \times 5 \times 6} + \frac{1}{6 \times 7 \times 8} - \dots$$

$$\frac{\pi}{2} = 1 + \frac{1}{3} + \frac{1 \times 2}{3 \times 5} + \frac{1 \times 2 \times 3}{3 \times 5 \times 7} + \dots$$

$\pi = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} - \frac{1}{5} + \frac{1}{6} + \dots$  where  $1/n$  is preceded by a  $-$  sign if and only if  $n$  has an odd number of prime factors of the form  $4k+1$

$$\frac{\pi}{2} - 1 = \frac{(2^1)(1!)^2}{3!} + \frac{(2^2)(2!)^2}{5!} + \frac{(2^3)(3!)^2}{7!} + \frac{(2^4)(4!)^2}{9!} + \dots$$

We can estimate  $\pi$  using random numbers



Get two random numbers  $x$  and  $y$  where  $0 \leq x \leq 1$  and  $0 \leq y \leq 1$

We can think of  $(x, y)$  as the co-ordinates of a point inside the unit square. This point will be inside the quarter circle if  $x^2 + y^2 < 1$ . Now get lots of points.

The number of points inside the quarter circle divided by the total number of points will be approximately equal to the area of the quarter circle divided by the area of the unit square.

Show that this is  $\pi/4$

So if we pick 1000 points and 763 of these points are inside the quarter circle then:

$$\frac{763}{1000} \approx \frac{\pi}{4} \text{ giving } \pi \approx 3.05$$

To get a better approximation we need to take more points. See Appendix 1 for a computer program to estimate  $\pi$

Viete's formula for  $\pi$

if you know about trigonometry ... (all angles in radians)

a) We know:

$$\cos 2\theta = 2\cos^2\theta - 1$$

the double angle formula

Show that:

$$\cos\theta = \sqrt{\left(\frac{1+\cos 2\theta}{2}\right)}$$

the half angle formula

We know:

$$\cos \frac{\pi}{4} = \frac{\sqrt{2}}{2}$$

Use the half angle formula to show that:

$$\cos \frac{\pi}{8} = \sqrt{\left( \frac{1+\cos \pi/4}{2} \right)} = \sqrt{\left( \frac{1+\sqrt{2}/2}{2} \right)} = \dots = \frac{\sqrt{2+\sqrt{2}}}{2}$$

Use the half angle formula to show that:

$$\cos \frac{\pi}{16} = \sqrt{\left( \frac{1+\cos \pi/8}{2} \right)} = \dots = \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2}$$

etc

b) We know:

$$\sin 2\theta = 2 \cos \theta \sin \theta \quad \text{the double angle formula}$$

If we repeatedly use the double angle formula we get:

$$\sin \theta = 2 \cos \frac{\theta}{2} \sin \frac{\theta}{2} = 2 \cos \frac{\theta}{2} \left( 2 \cos \frac{\theta}{4} \sin \frac{\theta}{4} \right) = 2 \cos \frac{\theta}{2} 2 \cos \frac{\theta}{4} \left( 2 \cos \frac{\theta}{8} \sin \frac{\theta}{8} \right) \quad \text{etc}$$

So:

$$\sin \theta = 2^n \cos \frac{\theta}{2} \cos \frac{\theta}{4} \cos \frac{\theta}{8} \cos \frac{\theta}{16} \dots \cos \frac{\theta}{2^n} \sin \frac{\theta}{2^n}$$

So:

$$\frac{\sin \theta}{\theta} = 2^n \cos \frac{\theta}{2} \cos \frac{\theta}{4} \cos \frac{\theta}{8} \dots \cos \frac{\theta}{2^n} \left( \frac{\sin \frac{\theta}{2^n}}{\left( \frac{\theta}{2^n} \right)} \right)$$

So:

$$\frac{\sin \theta}{\theta} = \cos \frac{\theta}{2} \cos \frac{\theta}{4} \cos \frac{\theta}{8} \dots \cos \frac{\theta}{2^n} \left( \frac{\sin \frac{\theta}{2^n}}{\left( \frac{\theta}{2^n} \right)} \right)$$

We know:

$$\text{if } x \rightarrow 0 \text{ then } \frac{\sin x}{x} \rightarrow 1$$

So:

$$\text{if } n \rightarrow \infty \text{ then } \left( \frac{\sin \frac{\theta}{2^n}}{\left( \frac{\theta}{2^n} \right)} \right) \rightarrow 1$$

So:

$$\frac{\sin \theta}{\theta} = \cos \frac{\theta}{2} \cos \frac{\theta}{4} \cos \frac{\theta}{8} \dots$$

Put:

$$\theta = \frac{\pi}{2}$$

and show that:

$$\frac{2}{\pi} = \cos \frac{\pi}{4} \cos \frac{\pi}{8} \cos \frac{\pi}{16} \dots$$

c) Use part (a) and part (b) to obtain Viete's formula:

$$\frac{2}{\pi} = \frac{\sqrt{2}}{2} \frac{\sqrt{2+\sqrt{2}}}{2} \frac{\sqrt{2+\sqrt{2+\sqrt{2}}}}{2} \dots$$

## Quotes

You can easily find lots of mathematics quotes on the internet. Here are a few:

1)

To call in the statistician after the experiment is done may be no more than asking him to perform a post-mortem examination. He may be able to say what the experiment died of.

R. A. Fisher

2)

Everything should be made as simple as possible, but not simpler.

A. Einstein

3)

A mathematician is a machine for turning coffee into theorems.

P. Erdos

4)

The mathematician's patterns, like the painter's or the poet's must be beautiful; the ideas, like the colours or the words must fit together in a harmonious way. Beauty is the first test: there is no permanent place in this world for ugly mathematics.

G. H. Hardy

5)

Mathematics is a game played according to certain simple rules with meaningless marks on paper.

D. Hilbert

6)

Logic is the art of going wrong with confidence.

M. Kline

7

In mathematics you don't understand things, you just get used to them.

J. von Neumann

8)

In the fall of 1972 President Nixon announced that the rate of increase of inflation was decreasing.

This was the first time a sitting president used the third derivative to advance his case for re-election.

H. Rossi

9)

I remember once going to see Ramanujan when he was lying ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavourable omen. "No," he replied, "it is a very interesting number; it is the smallest

number expressible as the sum of two cubes in two different ways."

G. H. Hardy

10)

It is more important to have beauty in one's equations than to have them fit experiment.

P. A. M. Dirac

11)

Mathematicians do not study objects, but relations between objects. Thus, they are free to replace some objects by others so long as the relations remain unchanged. Content to them is irrelevant: they are interested in form only.

H. Poincaré

12)

Ordinary language is totally unsuited for expressing what Physics really asserts, since the words of everyday life are not sufficiently abstract. Only mathematics and mathematical logic can say as little as the physicist means to say.

B. Russell

13)

The propositions of mathematics have, therefore, the same unquestionable certainty which is typical of such propositions as "All bachelors are unmarried," but they also share the complete lack of empirical content which is associated with that certainty. The propositions of mathematics are devoid of all factual content; they convey no information whatever on any empirical subject matter.

C. Hempel

14)

The universe cannot be read until we have learnt the language and become familiar with the characters in which it is written. It is written in mathematical language, and the letters are triangles, circles and other geometrical figures, without which means it is humanly impossible to comprehend a single word.

G. Galileo

15)

[Criticized for using formal mathematical manipulations, without understanding how they worked]

Should I refuse a good dinner simply because I do not understand the process of digestion?

O. Heaviside

16)

If triangles invented a god, they would make him three-sided.

Montesquieu

17)

If I have seen further than others, it is by standing upon the shoulders of giants.

I. Newton

18)

Mathematics is the art of giving the same name to different things.

H. Poincare

19)

Thus Mathematics may be defined as the subject in which we never know what we are talking about, nor whether what we are saying is true.

B. Russell

20)

In science, you want to say something that nobody knew before, in words which everyone can understand. In poetry you want to say something that everyone knows already in words that nobody can understand.

P. A. M. Dirac

21)

One cannot escape the feeling that these mathematical formulas have an independent existence and an intelligence of their own, that they are wiser than we are, wiser even than their discoverers, that we get more out of them than was originally put into them.

H. Hertz

22)

Reductio ad absurdum, which Euclid loved so much, is one of a mathematician's finest weapons. It is a far finer gambit than any chess play: a chess player may offer the sacrifice of a pawn or even a piece, but a mathematician offers the game.

G. H. Hardy

23)

Mathematics, rightly viewed, possesses not only truth, but supreme beauty – a beauty cold and austere, like that of sculpture, without appeal to any part of our weaker nature, without the gorgeous trappings of painting or music, yet sublimely pure and capable of a stern perfection such as only the greatest art can show.

B. Russell

24)

Read Euler, read Euler, he is the master of us all.

P. S. Laplace

25)

There is no branch of mathematics, however abstract, which may not some day be applied to the phenomena of the real world

N. Lobatchevsky

26)

He uses statistics as a drunken man uses lamp-posts. For support rather than illumination.

A. Lang

## Rationals and Irrationals

$\frac{13}{7}$  is a rational number because it is an integer divided by another integer.

### Theorem

$x$  is a rational number if and only if  $x$  is a terminating or recurring decimal.

This is really two theorems:

#### Theorem 1

If  $x$  is a rational number then  $x$  is a terminating or recurring decimal.

##### Proof

Say  $x = \frac{13}{7}$

$$\frac{13}{7} = 1 + \frac{6}{7} \quad \frac{13}{7} \text{ equals } 1 \text{ remainder } 6$$

$$\frac{6}{7} = \frac{1}{10} \left( \frac{60}{7} \right) = \frac{1}{10} \left( 8 + \frac{4}{7} \right) \quad \frac{60}{7} \text{ equals } 8 \text{ remainder } 4$$

$$\frac{4}{7} = \frac{1}{10} \left( \frac{40}{7} \right) = \frac{1}{10} \left( 5 + \frac{5}{7} \right) \quad \frac{40}{7} \text{ equals } 5 \text{ remainder } 5$$

$$\frac{5}{7} = \frac{1}{10} \left( \frac{50}{7} \right) = \frac{1}{10} \left( 7 + \frac{1}{7} \right) \quad \frac{50}{7} \text{ equals } 7 \text{ remainder } 1$$

etc

$$\text{So } \frac{13}{7} = 1 + \frac{8}{10} + \frac{5}{100} + \frac{7}{1000} + \dots = 1.857\dots$$

The remainders can only be 0, 1, 2, 3, 4, 5, 6

Either we will get a remainder of 0, in which case the decimal terminates.

Or we will get a remainder we have had before, in which case the decimal recurs.

Either way  $x$  is a terminating decimal or a recurring decimal

#### Theorem 2

If  $x$  is a terminating or recurring decimal then  $x$  is a rational number.

##### Proof

If:

$x$  is a terminating decimal, say  $x = 0.123$

then:

$x = \frac{123}{1000}$  so  $x$  is a rational number.

If:

$x$  is a recurring decimal, say  $x = 0.\overline{123123123\dots}$

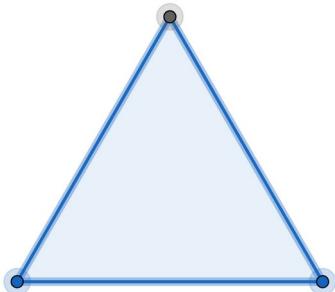
then:

$1000x = 123.\overline{123123123\dots}$  so  $999x = 123$  so  $x = \frac{123}{999}$  so  $x$  is a rational number.

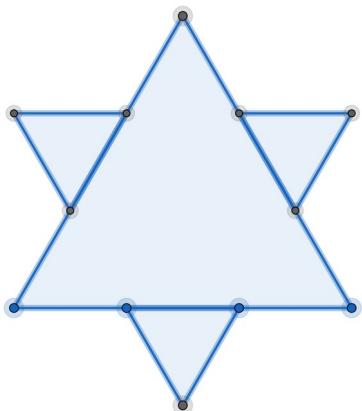
Either way  $x$  is a rational number.

## Snow-flake Curve

We start with an equilateral triangle:



Then we add a smaller equilateral triangle to each of the three sides:



Then we add an even smaller equilateral triangle to each of the twelve sides.

We repeat this an infinite number of times to get the snowflake curve. We want to find the perimeter and area of this curve.

### Perimeter

At the start, we have 3 sides of length  $L$  so the perimeter is  $3L$

The first iteration replaces each side by 4 sides of length  $\frac{L}{3}$  so the perimeter is  $\frac{4L}{3}$

Each iteration increases the perimeter by a factor of  $\frac{4}{3}$

So after an infinite number of iterations, the perimeter is infinite.

### Area

At the start, we have a triangle with area 1

The first iteration adds 3 triangles, each of area  $\frac{1}{9}$

The second iteration adds  $3 \times 4$  triangles, each of area  $\left(\frac{1}{9}\right)^2$

The third iteration adds  $3 \times 4 \times 4$  triangles, each of area  $\left(\frac{1}{9}\right)^3$

etc

So after an infinite number of iterations, the area is:

$$1 + \left(3 \times \frac{1}{9}\right) + \left(3 \times 4 \times \frac{1}{9^2}\right) + \left(3 \times 4^2 \times \frac{1}{9^3}\right) + \dots$$

Now:

$$\left(3 \times \frac{1}{9}\right) + \left(3 \times 4 \times \frac{1}{9^2}\right) + \left(3 \times 4^2 \times \frac{1}{9^3}\right) + \dots = \frac{3/9}{1 - 4/9} = \frac{3}{5} \quad (\text{see Appendix 2: Geometric Sequence})$$

So the final area is:

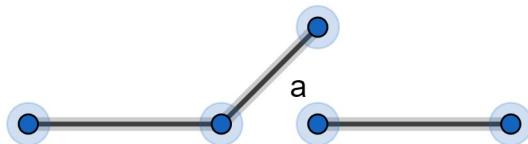
$$1 + \frac{3}{5} = \frac{8}{5}$$

So the snow-flake curve has a finite area but an infinite perimeter.

## Switching Circuits

### Example 1

Here is a switch called  $a$ . It can be closed or open.



If  $a$  is closed then electric current can flow. We say  $a=1$

If  $a$  is open then electric current cannot flow. We say  $a=0$

### Example 2

Here are two switches in series:



$a.b$  denotes switches  $a$  and  $b$  in series (this is not multiplication!)

If  $a$  is closed and  $b$  is closed then electric current can flow.

So if  $a=1$  and  $b=1$  then  $a.b=1$  So  $1.1=1$

If  $a$  is open or  $b$  is open (or both) then electric current cannot flow.

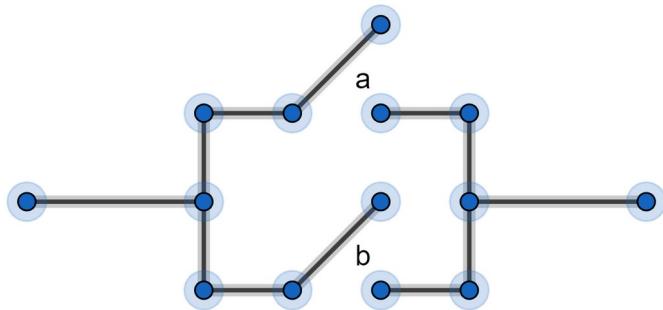
So if  $a=0$  or  $b=0$  (or both) then  $a.b=0$  So  $0.1=0$   $1.0=0$   $0.0=0$

We can set this out in a table:

$a$	$b$	$a.b$
0	0	0
0	1	0
1	0	0
1	1	1

### Example 3

Here are two switches in parallel:



$a+b$  denotes switches  $a$  and  $b$  in parallel (this is not addition!)

$a$  is closed or  $b$  is closed (or both) then electric current can flow.

So if  $a=1$  or  $b=1$  (or both) then  $a+b=1$  So  $1+0=1$   $0+1=1$   $1+1=1$

If  $a$  is open and  $b$  is open then electric current cannot flow.

So if  $a=0$  and  $b=0$  then  $a+b=0$  So  $0+0=0$

We can set this out in a table:

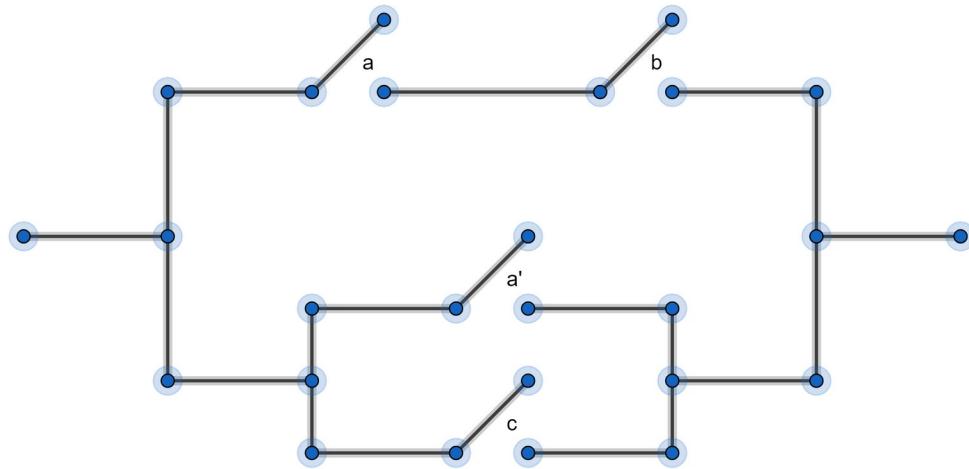
$a$	$b$	$a+b$
0	0	0
0	1	1
1	0	1
1	1	1

We can have switches that are linked to each other. If two switches are both called  $a$  then they are always in the same state, either both open or both closed. If one switch is called  $a$  and another switch is called  $a'$  then they are always in opposite states, one open and the other one closed.

If  $a=1$  then  $a'=0$  If  $a=0$  then  $a'=1$

#### Example 4

Here is a circuit:



The mathematical expression for this circuit is:  $(a \cdot b) + (a' + c)$  Think about it.

The table for this circuit is:

$a$	$b$	$c$	$a \cdot b$	$a'$	$a' + c$	$(a \cdot b) + (a' + c)$
0	0	0	0	1	1	1
0	0	1	0	1	1	1
0	1	0	0	1	1	1
0	1	1	0	1	1	1
1	0	0	0	0	0	0
1	0	1	0	0	1	1
1	1	0	1	0	0	1
1	1	1	1	0	1	1

see EXERCISE 1

Look at Exercise 1 questions (4) and (5)

You should have found that the columns for  $(a \cdot b) + (a \cdot c)$  and  $a \cdot (b + c)$  are the same.

We say  $(a \cdot b) + (a \cdot c) = a \cdot (b + c)$

The circuit in (5) does the same thing as the circuit in (4) but uses fewer switches.

$a \cdot 1$  denotes switch  $a$  in series with a closed switch  
 electric current can flow if  $a$  is closed, so  $a \cdot 1 = 1$  if  $a = 1$   
 electric current cannot flow if  $a$  is open, so  $a \cdot 1 = 0$  if  $a = 0$   
 So  $a \cdot 1 = a$

$a+1$  denotes switch  $a$  in parallel with a closed switch. Electric current can always flow.  
 So  $a+1 = 1$

$a \cdot 0$  denotes switch  $a$  in series with an open switch. Electric current can never flow.  
 So  $a \cdot 0 = 0$

$a+0$  denotes switch  $a$  in parallel with an open switch  
 electric current can flow if  $a$  is closed, so  $a+0 = 1$  if  $a = 1$   
 electric current cannot flow if  $a$  is open, so  $a+0 = 0$  if  $a = 0$   
 So  $a+0 = a$

Use tables to prove the following rules: (no need to do them all)

$$\begin{array}{ll}
 (a')' = a & \\
 a \cdot a = a & a + a = a \\
 a \cdot a' = 0 & a + a' = 1 \\
 a \cdot b = b \cdot a & a + b = b + a \\
 (a \cdot b) \cdot c = a \cdot (b \cdot c) & (a + b) + c = a + (b + c) \\
 a \cdot (b + c) = (a \cdot b) + (a \cdot c) & a + (b \cdot c) = (a + b) \cdot (a + c) \\
 (a \cdot b)' = a' + b' & (a + b)' = a' \cdot b' \\
 a \cdot (a + b) = a & a + (a \cdot b) = a
 \end{array}$$

## EXERCISE

1) Draw the circuit and fill in the table for  $(a+b)+(a \cdot b)$

a	b	$a+b$	$a \cdot b$	$(a+b)+(a \cdot b)$
0	0			
0	1			
1	0			
1	1			

2) Draw the circuit and fill in the table for  $a.(a' + b)$

a	b	$a'$	$a' + b$	$a.(a' + b)$
0	0			
0	1			
1	0			
1	1			

3) Draw the circuit and fill in the table for  $(a.b) + c$

a	b	c	$a.b$	$(a.b) + c$
0	0	0		
0	0	1		
0	1	0		
0	1	1		
1	0	0		
1	0	1		
1	1	0		
1	1	1		

4) Draw the circuit and fill in the table for  $(a.b) + (a.c)$

a	b	c	$a.b$	$a.c$	$(a.b) + (a.c)$
0	0	0			
0	0	1			
0	1	0			
0	1	1			
1	0	0			
1	0	1			
1	1	0			
1	1	1			

5) Draw the circuit and fill in the table for  $a.(b+c)$

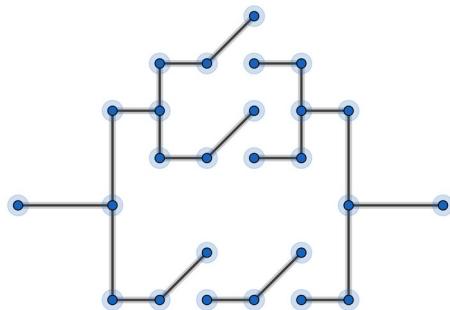
a	b	c	$b+c$	$a.(b+c)$
0	0	0		
0	0	1		
0	1	0		
0	1	1		
1	0	0		
1	0	1		
1	1	0		
1	1	1		

## SOLUTIONS

1)

a	b	$a+b$	$a \cdot b$	$(a+b)+(a \cdot b)$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	1

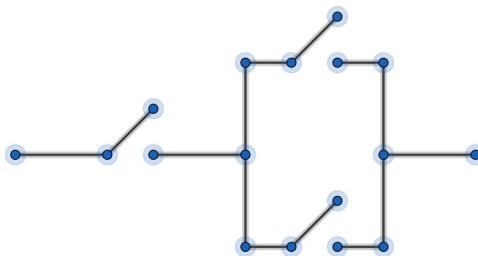
Here is the circuit. Can you label the switches?



2)

a	b	$a'$	$a'+b$	$a \cdot (a'+b)$
0	0	1	1	0
0	1	1	1	0
1	0	0	0	0
1	1	0	1	1

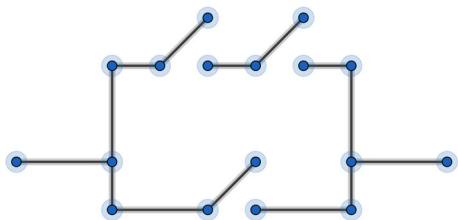
Here is the circuit. Can you label the switches?



3)

a	b	c	$a \cdot b$	$(a \cdot b) + c$
0	0	0	0	0
0	0	1	0	1
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	1

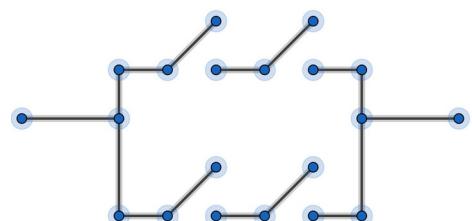
Here is the circuit. Can you label the switches?



4)

a	b	c	$a \cdot b$	$a \cdot c$	$(a \cdot b) + (a \cdot c)$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
0	1	1	0	0	0
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	1	0	1
1	1	1	1	1	1

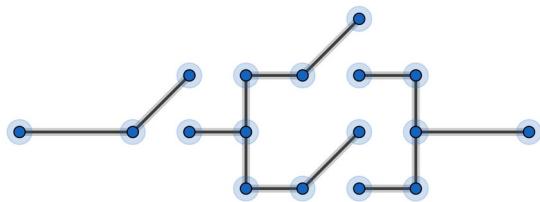
Here is the circuit. Can you label the switches?



5)

a	b	c	$b+c$	$a.(b+c)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Here is the circuit. Can you label the switches?



## Three Games

1)

Nim – a game for two players

There is a pile of 18 counters on the table. Players take turns to remove counters. Each player can remove 1, 2, 3 or 4 counters on each turn. The player who removes the last counter is the winner.  
For example:

Eric takes 4 counters, Bill takes 2, Eric takes 3, Bill takes 4, Eric takes 3, Bill takes 2. Bill wins.

Jane has a good strategy to play this game. If Eric takes  $n$  counters then Jane next takes  $5 - n$  counters so they have taken 5 counters between them.

We start with 18 counters. Jane goes first and takes 3 counters, leaving 15 counters.

15 is a multiple of 5. Now it is Eric's go. Can you see why Jane will win?

Note: You can play this game with any number of counters at the start.

We start with 97 counters. Jane goes first and takes 2 counters, leaving 95 counters.

95 is a multiple of 5. Now it is Eric's go. Can you see why Jane will win?

We start with 30 counters. Jane lets Eric go first. How nice of her. Can you see why Jane will win?

2)

Fifteen – a game for two players

We have nine cards numbered 1, 2, ... 9. Players take turns to take a card. The first player who has taken three cards that add up to fifteen is the winner.

For example:

Eric takes the 4, Bill takes the 9, Eric takes the 6, Bill takes the 5, Eric takes the 3, Bill takes the 8, Eric takes the 2, Bill takes the 1. Bill holds the 9, 5 and 1. So Bill wins.

Jane has a good strategy to play this game. She has a magic square:

8	3	4
1	5	9
6	7	2

How will this help?

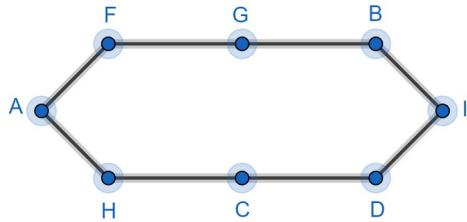
3)

A game for one player

A	B	C
D	E	F
G	H	I

Place white knights on squares A and C. Place black knights on squares G and I. Move the knights (in any order) so that the white knights end up on the squares G and I and the black knights end up on the squares A and C.

The diagram below shows which squares are connected by knight moves. So, for example, a knight can move from square F to square A or to square G. We could play the game on this diagram. It would be much easier. Can you see why?



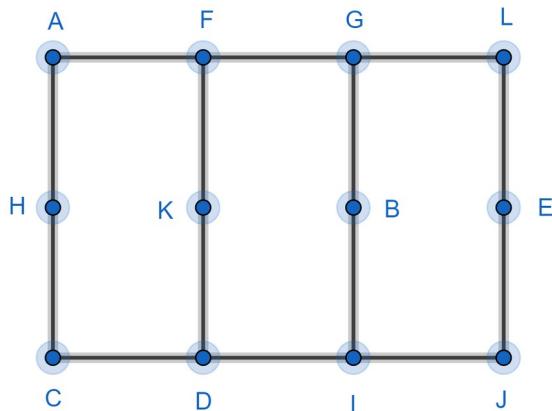
4)

A game for one player

A	B	C
D	E	F
G	H	I
J	K	L

Place white knights on squares A, B and C. Place black knights on squares J, K and L. Move the knights (in any order) so that the white knights end up on the squares J, K and L and the black knights end up on the squares A, B and C.

The diagram below shows which squares are connected by knight moves ...



## Tiling

### Example 1

I want to cover my  $8 \times 8$  chess-board with thirty-two  $2 \times 1$  tiles. Try it. It's easy.

### Example 2

Someone has removed two squares from my chess-board. The bottom left-hand corner square and the top right-hand corner square. Can I cover my mutilated chess-board with thirty-one  $2 \times 1$  tiles?

Each  $2 \times 1$  tile covers one black square and one white square. So however I arrange the tiles, I will always cover the same number of black squares and white squares. The bottom left-hand corner square and the top right-hand corner are both black. So the mutilated chess-board has 30 black squares and 32 white squares. So I cannot cover my mutilated chess-board with thirty-one  $2 \times 1$  tiles.

### Example 3

Someone has removed two squares from my chess-board. Can I cover my mutilated chess-board with thirty-one  $2 \times 1$  tiles?

The answer will depend on which squares have been removed. We know, from the previous example that if two black squares have been removed or if two white squares have been removed then the answer is: No!

### Gomory's Theorem

I can cover my mutilated chess-board with thirty-one  $2 \times 1$  tiles if any black square and any white square have been removed.

### Proof

Here is a chess-board:

1	64	63	62	61	60	59	58
2	51	52	53	54	55	56	57
3	50	49	48	47	46	45	44
4	37	38	39	40	41	42	43
5	36	35	34	33	32	31	30
6	23	24	25	26	27	28	29
7	22	21	20	19	18	17	16
8	9	10	11	12	13	14	15

Look at the way I have numbered the squares. I can go for a walk around the board, visiting every square in the order 1, 2, 3, ... 64

Say, the black square 24 and the white square 41 have been removed on my mutilated chess-board. I can cover the board as follows:

Put the first tile on squares 25 and 26, the next tile on squares 27 and 28, ... on squares 39 and 40, the next tile on squares 42 and 43, the next tile on squares 44 and 45, ... on squares 22 and 23.

This method will work whichever black square and whichever white square have been removed.

### Investigation

Someone has removed two black squares and two white squares from my chess-board. Can I cover my mutilated chess-board with thirty  $2 \times 1$  tiles?

### Example 4

Can I cover a chess-board with  $3 \times 1$  tiles?

Each tile covers 3 squares. There are 64 squares on the board. So the answer is: No!

### Example 5

Someone has removed one square from my chess-board. Can I cover my mutilated chess-board with twenty-one  $3 \times 1$  tiles?

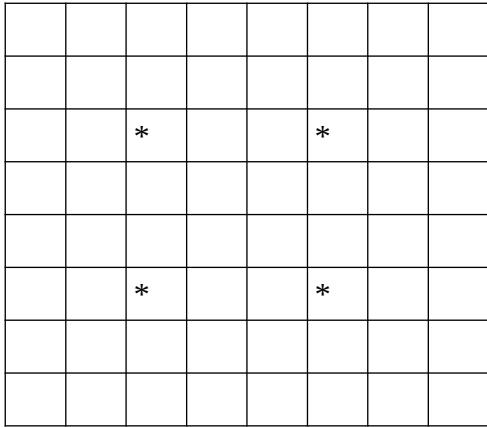
The answer will depend on which square has been removed. Let's colour the squares white, red and black:

W	R	B	W	R	B	W	R
B	W	R	B	W	R	B	W
R	B	W	R	B	W	R	B
W	R	B	W	R	B	W	R
B	W	R	B	W	R	B	W
R	B	W	R	B	W	R	B
W	R	B	W	R	B	W	R
B	W	R	B	W	R	B	W

Each  $3 \times 1$  tile covers one white square, one red square and one black square. So however I arrange the tiles, I will always cover the same number of white squares, red squares and black squares. The chess-board (before the square has been removed) has 22 white squares, 21 red squares and 21 black squares. So the removed square must be white. But can it be any white square?

If I could cover the mutilated chess-board with the bottom right-hand corner square removed then I could rotate the board  $90^\circ$  clockwise and I would have covered the mutilated chess-board with the bottom left-hand corner removed. But we know that this is not possible.

To have any hope of covering my mutilated chess-board, the removed square must be one of the \* squares:



Can I can cover my mutilated chess-board if the removed square is one of the \* squares?

I don't know. Try it.

### Example 6

This final example is a bit different and involves no mutilation.

I have a  $100 \times 101$  board.

I have lots of  $2 \times 2$  tiles  $4 \times 4$  tiles  $6 \times 6$  tiles and  $13 \times 13$  tiles available.

Can I cover my board with tiles?

We are going to colour the squares black and white, but in an unusual way:

B	B	B	B	B	B	...
W	W	W	W	W	W	...
B	B	B	B	B	B	...
W	W	W	W	W	W	...
B	B	B	B	B	B	...
W	W	W	W	W	W	...
...	...	...	...	...	...	...

Each  $2 \times 2$  tile covers 2 black squares and 2 white squares.

Each  $4 \times 4$  tile covers 8 black squares and 8 white squares.

Each  $6 \times 6$  tile covers 18 black squares and 18 white squares.

Each  $13 \times 13$  tile covers 91 black squares and 78 white squares or 78 black squares and 91 white squares. So the difference between the number of black squares I can cover and the number of white squares I can cover must be a multiple of 13. But the board has 5100 black squares and 5000 white squares. So the answer is: No!

## Triangle Problem.

### Theorem

Mark six points (A, B, C, D, E, F) on a piece of paper so that no three points are in a straight line.

Join each pair of points with a straight line. Colour each line red or green.

However you choose to colour the lines, there will always be a triangle with 3 red lines or a triangle with 3 green lines.

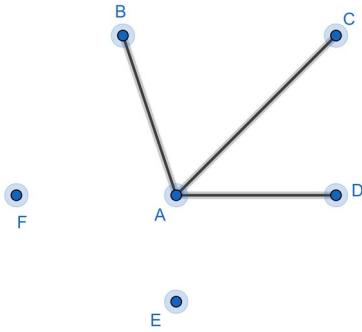
### Proof

A is connected to 5 lines and each line is either red or green.

either: A is connected to 3 (or more) red lines

or: A is connected to 3 (or more) green lines

Consider the case where A is connected to 3 (or more) red lines, say AB, AC and AD.



If line BC is red then triangle ABC has 3 red lines

If line CD is red then triangle ACD has 3 red lines

If line BD is red then triangle ABD has 3 red lines

If lines BC, CD, BD are all green then triangle BCD has 3 green lines

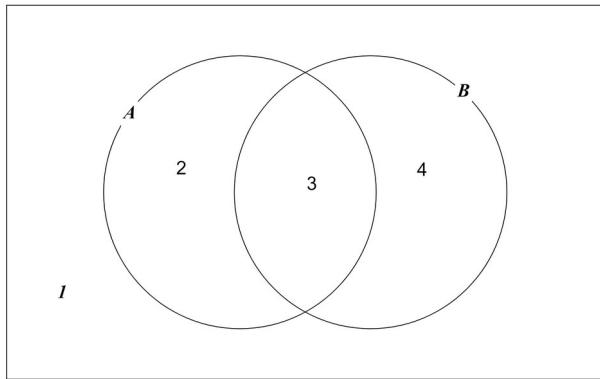
We can repeat this argument if A connected to 3 (or more) green lines.

Either way, we have the required triangle.

## Venn Diagrams and Tables

### Venn Diagrams

Two circle diagrams:



Let's talk about regions inside this rectangle.

- |            |  |                    |
|------------|--|--------------------|
| $a$        | is the region inside the A circle                                  | regions 2 and 3    |
| $a'$       | is the region not inside the A circle                              | regions 1 and 4    |
| $a \cap b$ | is the region inside both the A circle and the B circle            | region 3           |
| $a \cup b$ | is the region inside either the A circle or the B circle (or both) | regions 2, 3 and 4 |

etc

Example 1

- |             |                 |
|-------------|-----------------|
| $a$         | regions 2 and 3 |
| $b'$        | regions 1 and 2 |
| $a \cap b'$ | region 2        |

Example 2

- |             |                   |
|-------------|-------------------|
| $a'$        | regions 1 and 4   |
| $b$         | regions 3 and 4   |
| $a' \cup b$ | regions 1,3 and 4 |

Example 3

- |               |                    |
|---------------|--------------------|
| $a \cap b$    | region 3           |
| $(a \cap b)'$ | regions 1, 2 and 4 |

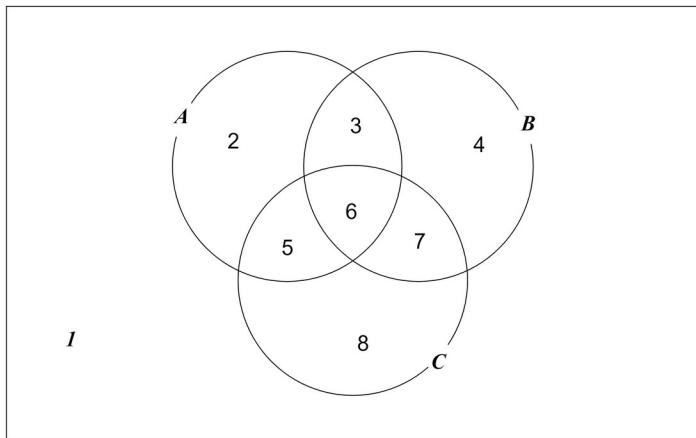
Example 4

- |              |                   |
|--------------|-------------------|
| $a'$         | regions 1 and 4   |
| $b'$         | regions 1 and 2   |
| $a' \cup b'$ | regions 1,2 and 4 |

Now  $(a \cap b)'$  and  $a' \cup b'$  are both regions 1,2 and 4

We say  $(a \cap b)' = a' \cup b'$

Three circle diagrams:



Let's talk about regions inside this rectangle.

Example 5

$$a \cap b \quad \text{regions 3 and 6}$$

$$c \quad \text{regions 5, 6, 7, 8}$$

$$(a \cap b) \cap c \quad \text{region 6}$$

Example 6

$$a \cup b \quad \text{regions 2, 3, 4, 5, 6, 7}$$

$$a \cup c \quad \text{regions 2, 3, 5, 6, 7, 8}$$

$$(a \cup b) \cap (a \cup c) \quad \text{regions 2,3,5,6, 7}$$

Example 7

$$a \cap b \quad \text{regions 3, 6}$$

$$a \cap c \quad \text{regions 5, 6}$$

$$(a \cap b) \cup (a \cap c) \quad \text{regions 3, 5, 6}$$

Example 8

$$b \cup c \quad \text{regions 3, 4, 5, 6, 7, 8}$$

$$a \quad \text{regions 2, 3, 5, 6}$$

$$a \cap (b \cup c) \quad \text{regions 3, 5, 6}$$

Now

$(a \cap b) \cup (a \cap c)$  and  $a \cap (b \cup c)$  are both regions 3, 5, 6

We say  $(a \cap b) \cup (a \cap c) = a \cap (b \cup c)$

Let 1 denote the whole region inside the rectangle, that is regions 1, 2, 3, 4, 5, 6, 7, 8

Let 0 denote no region. So:

$a \cap 1$	regions 2, 3, 5, 6	so $a \cap 1 = a$
$a \cup 1$	regions 1, 2, 3, 4, 5, 6, 7, 8	so $a \cup 1 = 1$
$a \cap 0$	no region	so $a \cap 0 = 0$
$a \cup 0$	regions 2, 3, 5, 6	so $a \cup 0 = a$

Use Venn diagrams to prove the following rules: (no need to do them all)

$(a')' = a$	
$a \cap a = a$	$a \cup a = a$
$a \cap a' = 0$	$a \cup a' = 1$
$a \cap b = b \cap a$	$a \cup b = b \cup a$
$(a \cap b) \cap c = a \cap (b \cap c)$	$(a \cup b) \cup c = a \cup (b \cup c)$
$a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$	$a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$
$(a \cap b)' = a' \cup b'$	$(a \cup b)' = a' \cap b'$
$a \cap (a \cup b) = a$	$a \cup (a \cap b) = a$

You will have noticed that we have the same rules for Propositions, Switching Circuits and Venn Diagrams (with slightly different notation). This means that we can use Venn diagrams to simplify expressions arising from propositions or switching circuits.

### Propositions

We can use a Venn diagram to show that:  $(a \cap b) \cup (a \cap c) = a \cap (b \cup c)$

And this shows that:  $(a \wedge b) \vee (a \wedge c) = a \wedge (b \vee c)$

### Switching circuits

We can use a Venn diagram to show that:  $(a \cap b) \cup (a \cap c) = a \cap (b \cup c)$

And this shows that:  $(a \cdot b) + (a \cdot c) = a \cdot (b + c)$

see EXERCISE 1

### Tables

We can also use tables to simplify expressions arising from propositions or switching circuits.

Let's use the notation we had for switching circuits. (We could equally well use the notation we had for propositions)

Here is a table for two variables. The cell marked \* represents  $a' \cdot b$

	$a$	$a'$
$b$		*
$b'$		

Here is another table. The cells marked \* together represent  $(a \cdot b) + (a \cdot b')$

	$a$	$a'$
$b$	*	
$b'$	*	

But:

$$(a \cdot b) + (a \cdot b') = a \cdot (b + b') = a \cdot 1 = a$$

So the cells marked \* together represent  $a$

etc

### Example 1

Simplify:  $(a \cdot b) + (a' \cdot b)$

We mark the cells

	$a$	$a'$
$b$	*	*
$b'$		

The \* occupy all the  $b$  cells.

So:

$$(a \cdot b) + (a' \cdot b) = b$$

We could do this using the rules:

$$(a \cdot b) + (a' \cdot b) = (a + a') \cdot b = 1 \cdot b = b$$

## Example 2

Simplify:  $(a'.b)+(a'.b')+(a.b')$

We mark the cells

	$a$	$a'$
$b$		*
$b'$	*	*

The \* occupy all the  $a'$  cells and all the  $b'$  cells.

So:

$$(a'.b)+(a'.b')+(a.b')=a'+b'$$

Wait a minute. Haven't we counted the  $a'.b'$  cell twice?

Yes we have and it's OK.

You will recall that:

$$a+a=a \text{ so } a'.b'=(a'.b')+(a'.b')$$

So:

$$\begin{aligned} (a'.b)+(a'.b')+(a.b') &= (a'.b)+(a'.b')+(a.b')+(a'.b') \\ &= a'.(b+b')+(a+a').b' \\ &= (a'.1)+(1.b') \\ &= a'+b' \end{aligned}$$

Here is a table for three variables. The cell marked \* represents  $a.b'.c'$

	$a$	$a$	$a'$	$a'$
$b$				
$b'$	*			
	$c'$	$c$	$c$	$c'$

etc

## Example 3

Simplify  $(a'.b.c)+(a'.b'.c)$

We mark the cells

	$a$	$a$	$a'$	$a'$
$b$			*	
$b'$			*	
	$c'$	$c$	$c$	$c'$

The \* occupy all the  $a'.c$  cells

So:

$$(a'.b.c) + (a'.b'.c) = a'.c$$

Example 4

Simplify  $(a.b.c) + (a'.b.c) + (a'.b'.c)$

We mark the cells

	$a$	$a$	$a'$	$a'$
$b$		*	*	
$b'$			*	
	$c'$	$c$	$c$	$c'$

The \* occupy all the  $a'.c$  cells and all the  $b.c$  cells

So:

$$(a.b.c) + (a'.b.c) + (a'.b'.c) = (a'.c) + (b.c)$$

We can further simplify this to:

$$(a' + b).c$$

Example 5

Simplify  $(a.b.c) + (a'.b.c) + (a.b.c') + (a'.b.c')$

We mark the cells

	$a$	$a$	$a'$	$a'$
$b$	*	*	*	*
$b'$				
	$c'$	$c$	$c$	$c'$

The \* occupy all the  $b$  cells

So:

$$(a.b.c) + (a'.b.c) + (a.b.c') + (a'.b.c') = b$$

Example 6

Simplify  $(a.b.c) + (a.b'.c) + (a'.b.c) + (a'.b'.c) + (a.b.c') + (a'.b.c')$

We mark the cells

	$a$	$a$	$a'$	$a'$
$b$	*	*	*	*
$b'$		*	*	
	$c'$	$c$	$c$	$c'$

The \* occupy all the  $b$  cells and all the  $c$  cells.

So:

$$(a.b.c) + (a.b'.c) + (a'.b.c) + (a'.b'.c) + (a.b.c') + (a'.b.c') = b + c$$

Example 7

$$\text{Simplify } (a.b.c) + (a.b'.c) + (a'.b.c) + (a'.b'.c) + (a.b.c') + (a.b'.c')$$

We mark the cells

	$a$	$a$	$a'$	$a'$
$b$	*	*	*	
$b'$	*	*	*	
	$c'$	$c$	$c$	$c'$

The \* occupy all the  $a$  cells and all the  $c$  cells.

So:

$$(a.b.c) + (a.b'.c) + (a'.b.c) + (a'.b'.c) + (a.b.c') + (a.b'.c') = a + c$$

Example 8

$$\text{Simplify } (a.b.c.d) + (a.b'.c.d) + (a.b'.c.d') + (a'.b.c.d) + (a'.b'.c.d) + (a'.b'.c.d')$$

We mark the cells

	$a$	$a$	$a'$	$a'$	
$b$					$d'$
$b$	*	*			$d$
$b'$	*	*			$d$
$b'$	*	*			$d'$
	$c'$	$c$	$c$	$c'$	

The \* occupy all the  $b'.c$  cells and all the  $c.d$  cells

So:

$$(a.b.c.d) + (a.b'.c.d) + (a.b'.c.d') + (a'.b.c.d) + (a'.b'.c.d) + (a'.b'.c.d') = (b'.c) + (c.d)$$

We can further simplify this to:

$$c \cdot (b' + d)$$

We have used Venn diagrams and tables to simplify expressions. Instead we could bash through the algebra.

Example

$$\begin{aligned} (a \cdot b \cdot c) + (a' \cdot b \cdot c) + (a \cdot b' \cdot c) + (a' \cdot b' \cdot c) &= ((a \cdot b) + (a' \cdot b) + (a \cdot b') + (a' \cdot b')).c \\ &= ((a \cdot b) + (a \cdot b') + (a' \cdot b) + (a' \cdot b')).c \\ &= (a \cdot (b + b') + a' \cdot (b + b')).c \\ &= ((a \cdot 1) + (a' \cdot 1)).c \\ &= (a + a').c \\ &= 1.c \\ &= c \end{aligned}$$

I think I prefer to use Venn diagrams and tables.

## EXERCISE 1

1)

Use a Venn diagram to show:

$$(a \cap b) \cup (a \cap b') \cup (a' \cap b') = a \cup b'$$

So the circuit:

$$(a \cdot b) + (a \cdot b') + (a' \cdot b')$$

is equivalent to circuit:

$$a + b'$$

We have a circuit. We write down a mathematical expression to describe this circuit. We simplify this expression using a Venn diagram. We redesign our circuit using fewer switches.

How cool is that?

2)

Use a Venn diagram to show:

$$(a \cap b \cap c) + (a \cap b \cap c') + (a \cap b' \cap c) + (a \cap b' \cap c') = a$$

So circuit:

$$(a \cdot b \cdot c) + (a \cdot b \cdot c') + (a \cdot b' \cdot c) + (a \cdot b' \cdot c')$$

is equivalent to a single switch

3)

Re-do question (1) using a table.

4)

Re-do question (2) using a table.

## EXERCISE 2

Simplify the following, using tables.

1)  $(a \cdot b') + (a' \cdot b')$

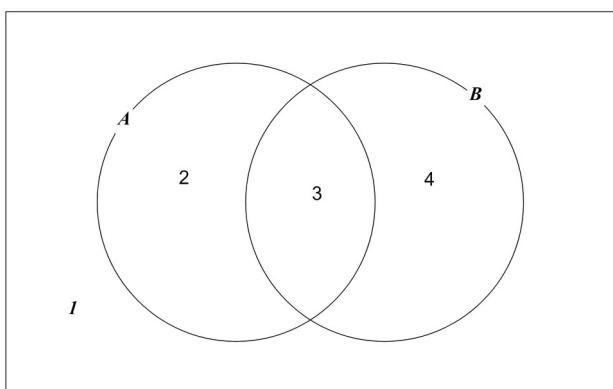
2)  $(a \cdot b) + (a \cdot b') + (a' \cdot b')$

3)  $(a \cdot b \cdot c) + (a \cdot b' \cdot c) + (a' \cdot b \cdot c) + (a' \cdot b' \cdot c)$

4)  $(a' \cdot b \cdot c) + (a' \cdot b' \cdot c) + (a \cdot b \cdot c') + (a \cdot b' \cdot c') + (a' \cdot b \cdot c')$

## SOLUTIONS 1

1)



$$a \cap b$$

region 3

$$a \cap b'$$

region 2

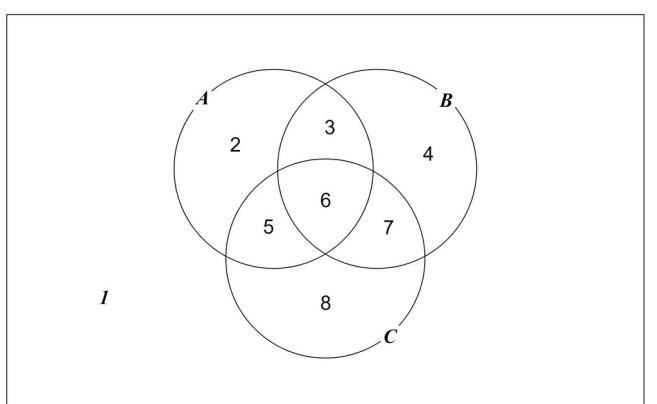
$$a' \cap b'$$

region 1

$$(a \cap b) + (a \cap b') + (a' \cap b')$$

regions 1, 2, 3

and



$$a \cup b'$$

regions 1,

2, 3

2)

$a \cap b \cap c$	region 6
$a \cap b \cap c'$	region 3
$a \cap b' \cap c$	region 5
$a \cap b' \cap c'$	region 2
$(a \cap b \cap c) + (a \cap b \cap c') + (a \cap b' \cap c) + (a \cap b' \cap c')$	regions 2, 3, 5, 6

and

$$a \quad \text{regions } 2, 3, 5, 6$$

3)  $(a.b) + (a.b') + (a'.b') = a + b'$

	$a$	$a'$
$b$	*	
$b'$	*	*

$$(a.b) + (a.b') + (a'.b') = a + b'$$

4)  $(a.b.c) + (a.b.c') + (a.b'.c) + (a.b'.c') = a$

	$a$	$a$	$a'$	$a'$
$b$	*	*		
$b'$	*	*		
	$c'$	$c$	$c$	$c'$

$$(a.b.c) + (a.b.c') + (a.b'.c) + (a.b'.c') = a$$

SOLUTIONS 2

1)

	$a$	$a'$
$b$		
$b'$	*	*

Simplifies to  $b'$

2)

	$a$	$a'$
$b$	*	
$b'$	*	*

Simplifies to  $a+b'$

3)

	$a$	$a$	$a'$	$a'$
$b$		*	*	
$b'$		*	*	
	$c'$	$c$	$c$	$c'$

Simplifies to  $c$

4)

	$a$	$a$	$a'$	$a'$
$b$	*		*	*
$b'$	*		*	
	$c'$	$c$	$c$	$c'$

Simplifies to

$$(a' \cdot c) + (a \cdot c') + (a' \cdot b)$$

Which further simplifies to:

$$a' \cdot (b+c) + (a \cdot c')$$

## Voting Systems

### Example 1

There are 3 candidates A, B and C. We need to elect one of them. There are 62 voters and each voter has put the candidates in order of preference:

Order of preference	Number of voters
ABC	18
ACB	15
BAC	5
BCA	14
CAB	8
CBA	2

This means:

18 voters put A as their first choice, B as their second choice and C as their third choice, etc.

Let's look at three different voting systems:

#### a) First-Past-The-Post

If a voter puts a candidate first choice, then that candidate gets 1 point.

A gets  $18+15=33$  points, B gets  $5+14=19$  points and C gets  $8+2=10$  points.

The winner is the candidate with the most points.

So A is the winner.

#### b) Alternative-Vote

If a voter puts a candidate first choice, then that candidate gets 1 point.

A gets  $18+15=33$  points, B gets  $5+14=19$  points and C gets  $8+2=10$  points.

The candidate with the fewest points is eliminated. So C is eliminated.

The 8 voters whose order of preference was CAB now put A as their first choice and B as their second choice.

The 2 voters whose order of preference was CBA now put B as their first choice and A as their second choice.

A now gets  $18+15+8=41$  points and B now gets  $5+14+2=21$  points.

So A is the winner.

#### c) Most-Popular

In an election between just A and B:

$18+15=33$  voters prefer A to B and  $5+14=19$  voters prefer B to A

So A is more popular than B.

In an election between just A and C:

$18+15=33$  voters prefer A to C and  $8+2=10$  voters prefer C to A

So A is more popular than C.

In an election between just B and C:

$5+14+18=37$  voters prefer B to C and  $8+2+15=25$  voters prefer C to B

So B is more popular than C.

A is more popular than B and A is more popular than C.

So A is the winner.

See EXERCISE

This all seems straight forward, but ...

Example 2

Order of preference	Number of voters
ABC	40
ACB	10
BAC	5
BCA	30
CAB	8
CBA	40

B is more popular than A and C is more popular than A.

But with First-Past-The-Post, A is the winner.

Example 3

Order of preference	Number of voters
ABC	6
ACB	15
BAC	5
BCA	15
CAB	8
CBA	10

C is more popular than A and C is more popular than B.

But with Alternative-Vote, C is eliminated.

#### Example 4

Order of preference	Number of voters
ABC	14
ACB	7
BAC	8
BCA	12
CAB	12
CBA	6

A is more popular than B and B is more popular than C and C is more popular than A.

So with Most-Popular, there is no winner.

#### Example 5

Order of preference	Number of voters
ABC	20
ACB	20
BAC	5
BCA	24
CAB	17
CBA	14

With Alternative-Vote:

A gets 40 points, B gets 29 points and C gets 31 points. So B is eliminated.

A now gets 45 points and C now gets 55 points. So C is the winner.

If 3 of the voters whose order of preference was ABC, had voted tactically and voted BAC then:

Order of preference	Number of voters
ABC	17
ACB	20
BAC	8
BCA	24
CAB	17
CBA	14

A gets 37 points, B gets 32 points and C gets 31 points. So C is eliminated.

A now gets 54 points and B now gets 46 points. So A is the winner.

So tactical voting paid off. But you need to be careful ...

If 10 of the voters whose order of preference was ABC, had voted tactically and voted BAC then:

Order of preference	Number of voters
ABC	10
ACB	20
BAC	15
BCA	24
CAB	17
CBA	14

A gets 30 points, B gets 39 points and C gets 31 points. A is eliminated. Whoops!

### Example 6

Order of preference	Number of governors
ABC	5
ACB	4
BAC	5
BCA	3
CAB	1
CBA	3

There are 3 candidates for a job at a school. Each of the governors has put the candidates in order of preference.

With First-Past-The-Post:

A gets 9 points, B gets 8 points, C gets 4 points. So the governors decide to appoint A.

However, just before the Principal announces the result, C gets a call on her phone, offering her a job at a different school, which she accepts. “Never mind” says the Principal “we were not going to give her the job anyway”. Not so fast! If C is no longer available:

A gets 10 points, B gets 11 points.

There are many other voting systems for electing one candidate. However ...

Arrow’s Theorem:

There is no perfect voting system. Arrow wrote a list of the features you would certainly want in any voting system. Arrow’s theorem proves that no voting system can have all these features.

Gibbard–Satterthwaite theorem:

We would like a voting system where there is no benefit in tactical voting. The Gibbard–Satterthwaite theorem proves that this is not possible.

## EXERCISE

1)

Order of preference	Number of voters
ABC	5
ACB	7
BAC	1
BCA	9
CAB	2
CBA	7

a) Who wins with First-Past-The-Post?

b) Who wins with Alternative-Vote?

c) Who wins with Most-Popular?

2)

Another voting system is Borda score.

If a voter puts a candidate first choice, then the candidate gets 3 points.

If a voter puts a candidate second choice, then the candidate gets 2 points.

If a voter puts a candidate third choice, then the candidate gets 1 point.

The winner is the candidate with the most points.

Look at Example 1 at the start of this chapter. Who is the winner with Borda score?

## SOLUTIONS

1)

a) A gets  $5+7=12$  B gets  $1+9=10$  C gets  $2+7=9$

A is the winner.

b) A gets  $5+7=12$  B gets  $1+9=10$  C gets  $2+7=9$  C is eliminated.

A now gets  $5+7+2=14$  B now gets  $1+9+7=17$

B is the winner.

c) A against B                    A gets  $5+7+2=14$  B gets  $1+9+7=17$

A against C                    A gets  $5+7+1=13$  C gets  $2+7+9=18$

B against C                    B gets  $1+9+5=15$  C gets  $2+7+7=16$

C is the winner.

2)

A gets  $(18+15)\times 3 + (5+8)\times 2 + (14+2)\times 1 = 141$

B gets  $(5+14)\times 3 + (18+2)\times 2 + (15+8)\times 1 = 120$

C gets  $(8+2)\times 3 + (15+14)\times 2 + (18+5)\times 1 = 111$

A is the winner.

## Wason Test

### EXERCISE

1) I have four cards. Each card has a letter on one side and an integer on the other side.

I put the cards down on a table, so you can only see one side of each card.

You can see: A, M, 4, 7

Which cards do you have to turn over to test the rule:

If the letter is a vowel then the integer is even?

2) I have four cards. Each card has a town on one side and a mode of transport on the other side.

I put the cards down on a table, so you can only see one side of each card.

You can see: Leeds, Manchester, Car, Train

Which cards do you have to turn over to test the rule:

If the town is Manchester then the mode of transport is Train?

3) I have four cards. Each card has a person's age on one side and a drink on the other side.

I put the cards down on a table, so you can only see one side of each card.

You can see: 16 years old, 24 years old, Beer, Lemonade

Which cards do you have to turn over to test the rule:

If the drink is Beer then the person's age must be over 18 years old?

### SOLUTIONS

We need to look for potential rule breakers.

1) A rule-breaker has got a vowel on one side and an odd integer on the other side.

We need to turn over A in case the other side is an odd integer.

We need to turn over 7 in case the other side is a vowel.

2) A rule-breaker has got Manchester on one side and not Train on the other side.

We need to turn over Manchester in case the other side is not Train.

We need to turn over Car in case the other side is Manchester.

3) A rule breaker has got Beer on one side and not over 18 years old on the other side.

We need to turn over Beer in case the other side is not over 18 years old.

We need to turn over 16 years old in case the other side is Beer.

Note: These three questions are logically equivalent. However research has shown that nearly every-one gets example (1) incorrect but nearly every-one gets example (3) correct.

There is no research available on example (2) because I just made it up.

## Euler's Sine Formula

Reminder of the factor theorem

Example

$$p(x) = x^4 - 17x^3 + 99x^2 - 223x + 140$$

Now:

$p(1)=0$  so  $(x-1)$  is a factor of  $p(x)$  - this is the factor theorem - see Appendix 2

$p(4)=0$  so  $(x-4)$  is a factor

$p(5)=0$  so  $(x-5)$  is a factor

$p(7)=0$  so  $(x-7)$  is a factor

So:

$$p(x) = c(x-1)(x-4)(x-5)(x-7) \text{ where } c \text{ is some constant}$$

Now:

$$p(0)=140 \text{ so } c=1$$

Rearranging gives:

$$p(x) = (1-x)(4-x)(5-x)(7-x) = 140 \left(1 - \frac{x}{1}\right) \left(1 - \frac{x}{4}\right) \left(1 - \frac{x}{5}\right) \left(1 - \frac{x}{7}\right)$$

Now:

$\sin(0)=0$  so  $(x-0)$  is a factor of  $\sin x$

$\sin(\pi)=0$  so  $(x-\pi)$  is a factor

$\sin(-\pi)=0$  so  $(x+\pi)$  is a factor

$\sin(2\pi)=0$  so  $(x-2\pi)$  is a factor

$\sin(-2\pi)=0$  so  $(x+2\pi)$  is a factor

$\sin(3\pi)=0$  so  $(x-3\pi)$  is a factor

$\sin(-3\pi)=0$  so  $(x+3\pi)$  is a factor etc

So:

$$\sin x = cx(x-\pi)(x+\pi)(x-2\pi)(x+2\pi)(x-3\pi)(x+3\pi)\dots \text{ where } c \text{ is some constant}$$

So:

$$\frac{\sin x}{x} = c(x-\pi)(x+\pi)(x-2\pi)(x+2\pi)(x-3\pi)(x+3\pi)\dots$$

Sub in  $x=0$  see Footnote

$$1 = c(-\pi)(+\pi)(-2\pi)(+2\pi)(-3\pi)(+3\pi)\dots$$

So:

$$c = \frac{1}{(-\pi)(+\pi)(-2\pi)(+2\pi)(-3\pi)(+3\pi)\dots}$$

So:

$$\sin x = \frac{x(x-\pi)(x+\pi)(x-2\pi)(x+2\pi)(x-3\pi)(x+3\pi)\dots}{(-\pi)(+\pi)(-2\pi)(+2\pi)(-3\pi)(+3\pi)\dots}$$

Fool around with this and show that:

$$\sin x = x \left(1 - \frac{x}{\pi}\right) \left(1 + \frac{x}{\pi}\right) \left(1 - \frac{x}{2\pi}\right) \left(1 + \frac{x}{2\pi}\right) \left(1 - \frac{x}{3\pi}\right) \left(1 + \frac{x}{3\pi}\right) \dots$$

Or if you prefer:

$$\sin(x) = x \left(1 - \frac{x^2}{\pi^2}\right) \left(1 - \frac{x^2}{2^2 \pi^2}\right) \left(1 - \frac{x^2}{3^2 \pi^2}\right) \dots \text{ this is Euler's sine formula}$$

We can have some fun with this.

1) We recall that:

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots \text{ this is the Maclaurin series}$$

Equating Maclaurin's formula and Euler's formula we have:

$$x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots = x \left(1 - \frac{x^2}{\pi^2}\right) \left(1 - \frac{x^2}{2^2 \pi^2}\right) \left(1 - \frac{x^2}{3^2 \pi^2}\right) \dots$$

Equating coefficients of  $x^3$  we (eventually) get:

$$-\frac{1}{3!} = -\frac{1}{\pi^2} - \frac{1}{2^2 \pi^2} - \frac{1}{3^2 \pi^2} - \dots$$

Rearranging gives:

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \dots = \frac{\pi^2}{6}$$

What a surprising answer. Why is  $\pi$  doing here?

As a bonus:

Equating coefficients of  $x^5$  we (eventually) get:

$$\frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \dots = \frac{\pi^4}{90}$$

We can also find formulas for:

$$\frac{1}{1^6} + \frac{1}{2^6} + \frac{1}{3^6} + \dots \text{ and } \frac{1}{1^8} + \frac{1}{2^8} + \frac{1}{3^8} + \dots \text{ etc}$$

What about?

$$\frac{1}{1^3} + \frac{1}{2^3} + \frac{1}{3^3} + \dots \text{ and } \frac{1}{1^5} + \frac{1}{2^5} + \frac{1}{3^5} + \dots \text{ etc}$$

Well Euler failed to find a formula for these series.

2) If we put  $x = \frac{\pi}{2}$  into Euler's sine formula we get:

$$1 - \frac{1}{2^2} \left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{2^2 \cdot 2^2}\right) \left(1 - \frac{1}{2^2 \cdot 3^2}\right) \dots$$

Now:

$$1 - \frac{1}{2^2 n^2} = \frac{(2n-1)(2n+1)}{2^2 n^2}$$

So:

$$1 = \frac{\pi}{2} \left( \frac{1 \times 3}{2^2} \right) \left( \frac{3 \times 5}{2^2 \cdot 2^2} \right) \left( \frac{5 \times 7}{2^2 \cdot 3^2} \right) \dots = \frac{\pi}{2} \left( \frac{1 \times 3}{2 \times 2} \right) \left( \frac{3 \times 5}{4 \times 4} \right) \left( \frac{5 \times 7}{6 \times 6} \right) \dots$$

Which gives us Wallis's formula:

$$\frac{\pi}{2} = \frac{2}{1} \times \frac{2}{3} \times \frac{4}{3} \times \frac{4}{5} \times \frac{6}{5} \times \frac{6}{7} \times \dots$$

3)

$$\sin x = x \left(1 - \frac{x}{\pi}\right) \left(1 + \frac{x}{\pi}\right) \left(1 - \frac{x}{2\pi}\right) \left(1 + \frac{x}{2\pi}\right) \left(1 - \frac{x}{3\pi}\right) \left(1 + \frac{x}{3\pi}\right) \dots$$

So:

$$\ln \sin x = \ln x + \ln \left(1 - \frac{x}{\pi}\right) + \ln \left(1 + \frac{x}{\pi}\right) + \ln \left(1 - \frac{x}{2\pi}\right) + \ln \left(1 + \frac{x}{2\pi}\right) + \ln \left(1 - \frac{x}{3\pi}\right) + \ln \left(1 + \frac{x}{3\pi}\right) \dots$$

Differentiate both sides and show that:

$$\frac{\cos x}{\sin x} = \frac{1}{x} - \frac{1}{\pi - x} + \frac{1}{\pi + x} - \frac{1}{2\pi - x} + \frac{1}{2\pi + x} - \frac{1}{3\pi - x} + \frac{1}{3\pi + x} - \dots$$

Sub in  $x = \frac{\pi}{4}$  and show that:

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \frac{1}{13} - \dots$$

Footnote:

Am I really saying?

$$\frac{\sin 0}{0} = 1$$

Look at the Maclaurin series:

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots$$

$$\frac{\sin x}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \dots$$

$$x \rightarrow 0 \quad \frac{\sin x}{x} \rightarrow 1$$

## Euler's Zeta Function

Euler introduced the zeta function:

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \dots$$

where  $x$  is a real number and  $x > 1$  which guarantees the series converges.

Look at this infinite product of infinite series:

$$\left(1 + \frac{1}{2^1} + \frac{1}{2^2} + \dots\right) \left(1 + \frac{1}{3^1} + \frac{1}{3^2} + \dots\right) \left(1 + \frac{1}{5^1} + \frac{1}{5^2} + \dots\right) \left(1 + \frac{1}{7^1} + \frac{1}{7^2} + \dots\right) \left(1 + \frac{1}{11^1} + \frac{1}{11^2} + \dots\right) \dots$$

where the denominators of the fractions are powers of the prime numbers.

First attempt:

Each bracket is a geometric series. So this infinite product is equal to:

$$\left(\frac{1}{1 - \frac{1}{2}}\right) \left(\frac{1}{1 - \frac{1}{3}}\right) \left(\frac{1}{1 - \frac{1}{5}}\right) \left(\frac{1}{1 - \frac{1}{7}}\right) \left(\frac{1}{1 - \frac{1}{11}}\right) \dots$$

Second attempt:

If we multiply out the brackets, we get a lot of fractions. All these fractions will have 1 as the numerator. No two fractions will have the same denominator. The denominator of each fraction will be a product of powers of primes. Every possible product of powers of primes will appear as a denominator. So this infinite product is equal to:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots$$

Equating:

$$\left(\frac{1}{1 - \frac{1}{2}}\right) \left(\frac{1}{1 - \frac{1}{3}}\right) \left(\frac{1}{1 - \frac{1}{5}}\right) \left(\frac{1}{1 - \frac{1}{7}}\right) \left(\frac{1}{1 - \frac{1}{11}}\right) \dots = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \dots$$

Now look at this infinite product of infinite series:

$$\left(1 + \frac{1}{2^x} + \frac{1}{2^{2x}} + \dots\right) \left(1 + \frac{1}{3^x} + \frac{1}{3^{2x}} + \dots\right) \left(1 + \frac{1}{5^x} + \frac{1}{5^{2x}} + \dots\right) \left(1 + \frac{1}{7^x} + \frac{1}{7^{2x}} + \dots\right) \left(1 + \frac{1}{11^x} + \frac{1}{11^{2x}} + \dots\right) \dots$$

By repeating what we did above we (eventually) get:

$$\left(\frac{1}{1 - \frac{1}{2^x}}\right) \left(\frac{1}{1 - \frac{1}{3^x}}\right) \left(\frac{1}{1 - \frac{1}{5^x}}\right) \left(\frac{1}{1 - \frac{1}{7^x}}\right) \left(\frac{1}{1 - \frac{1}{11^x}}\right) \dots = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \dots \quad ***$$

Notice, the right-hand side is  $\zeta(x)$

So we can write the zeta function in terms of primes:

$$\zeta(x) = \left( \frac{1}{1 - \frac{1}{2^x}} \right) \left( \frac{1}{1 - \frac{1}{3^x}} \right) \left( \frac{1}{1 - \frac{1}{5^x}} \right) \left( \frac{1}{1 - \frac{1}{7^x}} \right) \left( \frac{1}{1 - \frac{1}{11^x}} \right) \dots$$

Note:

In the chapter, Euler's Sine Formula, we got the result:

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \frac{\pi^2}{6}$$

So:

$$\frac{\pi^2}{6} = \left( \frac{1}{1 - \frac{1}{2^2}} \right) \left( \frac{1}{1 - \frac{1}{3^2}} \right) \left( \frac{1}{1 - \frac{1}{5^2}} \right) \left( \frac{1}{1 - \frac{1}{7^2}} \right) \left( \frac{1}{1 - \frac{1}{11^2}} \right) \dots$$

And we have a formula for  $\pi$  in terms of primes.

Note:

If we sub  $x=1$  into \*\*\*

We know the RHS diverges, so the LHS diverges, so there must be an infinite number of primes!

## Euler's Prime Sum

In the chapter, Euler's Zeta Function, we got the result:

$$\left( \frac{1}{1-\frac{1}{2}} \right) \left( \frac{1}{1-\frac{1}{3}} \right) \left( \frac{1}{1-\frac{1}{5}} \right) \left( \frac{1}{1-\frac{1}{7}} \right) \cdots = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \cdots$$

Taking logs of both sides:

$$\ln\left(\frac{1}{1-\frac{1}{2}}\right) + \ln\left(\frac{1}{1-\frac{1}{3}}\right) + \ln\left(\frac{1}{1-\frac{1}{5}}\right) + \ln\left(\frac{1}{1-\frac{1}{7}}\right) + \cdots = \ln\left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \cdots\right)$$

So:

$$\sum_{\text{primes}} \ln\left(\frac{1}{1-\frac{1}{p}}\right) = \ln \sum_1^{\infty} \frac{1}{n} \quad *$$

Now:

$$\left( \frac{1}{1-\frac{1}{p}} \right) = \left( 1 - \frac{1}{p} \right)^{-1} \quad \text{So} \quad \ln\left(\frac{1}{1-\frac{1}{p}}\right) = -\ln\left(1 - \frac{1}{p}\right)$$

So we can write \* as:

$$\sum_{\text{primes}} -\ln\left(1 - \frac{1}{p}\right) = \ln \sum_1^{\infty} \frac{1}{n} \quad **$$

Now:

$$\ln(1+x) = x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \frac{1}{4}x^4 + \cdots \quad \text{this is the Maclaurin series}$$

$$\text{Put } x = -\frac{1}{p}$$

We get:

$$\ln\left(1 - \frac{1}{p}\right) = -\frac{1}{p} - \frac{1}{2p^2} - \frac{1}{3p^3} - \frac{1}{4p^4} - \cdots \quad \text{So} \quad -\ln\left(1 - \frac{1}{p}\right) = \frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \frac{1}{4p^4} + \cdots$$

So we can write \*\* as:

$$\sum_{\text{primes}} \left( \frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \frac{1}{4p^4} + \cdots \right) = \ln \sum_1^{\infty} \frac{1}{n}$$

So:

$$\sum_{\text{primes}} \frac{1}{p} + \sum_{\text{primes}} \left( \frac{1}{2p^2} + \frac{1}{3p^3} + \frac{1}{4p^4} + \cdots \right) = \ln \sum_1^{\infty} \frac{1}{n} \quad ***$$

Consider:

$$\sum_{\text{primes}} \left( \frac{1}{2 p^2} + \frac{1}{3 p^3} + \frac{1}{4 p^4} + \dots \right)$$

Now:

$$\frac{1}{2 p^2} + \frac{1}{3 p^3} + \frac{1}{4 p^4} + \dots < \frac{1}{p^2} + \frac{1}{p^3} + \frac{1}{p^4} + \dots = \frac{\left( \frac{1}{p^2} \right)}{\left( 1 - \frac{1}{p} \right)} = \dots = \frac{1}{p-1} - \frac{1}{p}$$

So:

$$\sum_{\text{primes}} \left( \frac{1}{2 p^2} + \frac{1}{3 p^3} + \frac{1}{4 p^4} + \dots \right) < \sum_{\text{primes}} \left( \frac{1}{p-1} - \frac{1}{p} \right) < \sum_2^\infty \left( \frac{1}{p-1} - \frac{1}{p} \right) = \left( \frac{1}{1} - \frac{1}{2} \right) + \left( \frac{1}{2} - \frac{1}{3} \right) + \left( \frac{1}{3} - \frac{1}{4} \right) + \dots = 1$$

Look at \*\*\* again:

$$\sum_{\text{primes}} \frac{1}{p} + \sum_{\text{primes}} \left( \frac{1}{2 p^2} + \frac{1}{3 p^3} + \frac{1}{4 p^4} + \dots \right) = \ln \sum_1^\infty \frac{1}{n}$$

We know:

$$\ln \sum_1^\infty \frac{1}{n} \text{ diverges.}$$

We have just shown that:

$$\sum_{\text{primes}} \left( \frac{1}{2 p^2} + \frac{1}{3 p^3} + \frac{1}{4 p^4} + \dots \right) \text{ converges.}$$

So we can deduce that:

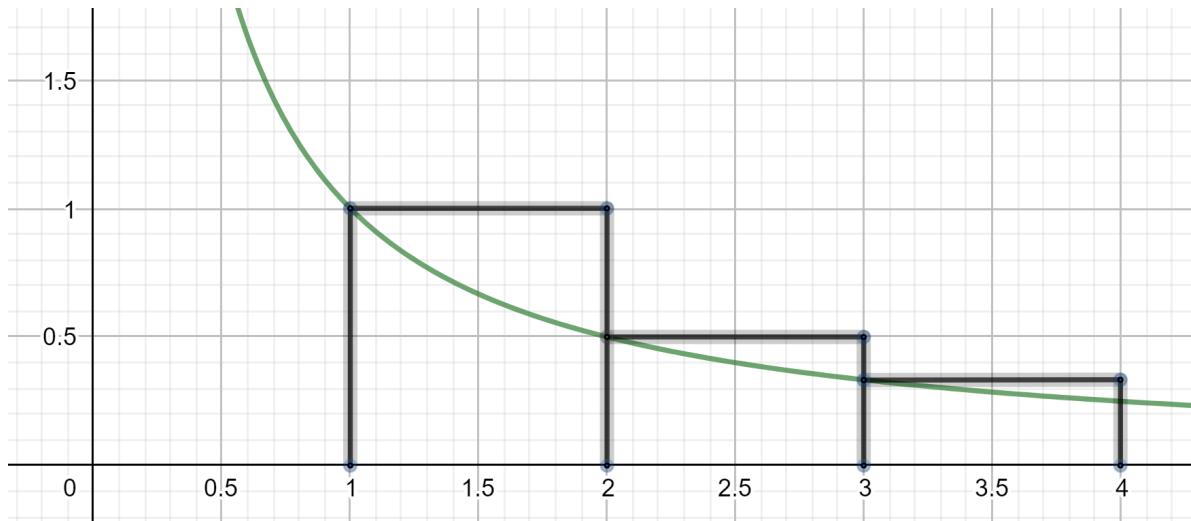
$$\sum_{\text{primes}} \frac{1}{p} \text{ diverges.}$$

So:

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{23} + \dots \text{ diverges. Astonishing!}$$

## Euler's Constant

Here is the graph  $y = \frac{1}{x}$  ADD SHADING



Look at the graph from  $x=1$  to  $x=4$

The area of the shaded bits is the area of the blocks minus the area under the graph.

The area of the blocks is:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3}$$

The area under the graph is:

$$\int_1^4 \frac{1}{x} dx = \ln 4$$

So the area of the shaded bits is:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} - \ln 4$$

Imagine the graph went from  $x=1$  to  $x=n+1$

The area of the shaded bits is:

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \ln(n+1)$$

Now let  $n \rightarrow \infty$

The total area of all the shaded bits is called  $\gamma$  This is Euler's constant.

$$\gamma = \lim_{n \rightarrow \infty} \left( \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} - \ln(n+1) \right)$$

Imagine sliding all the shaded bits horizontally to the left. They will all fit inside the first block with room to spare. So  $\gamma < 1$

Incidentally, it is not known if  $\gamma$  is rational or irrational.

# Error Detecting Codes

An online book shop sells books. Each book has a four digit code-number. To order a book you have to type this code-number into an online order form. But you might make an error when you do this.

Say the book you want to buy has code-number 4693.

You might type in 4673 instead of 4693. This is a digit error.

You might type in 4963 instead of 4693. This is a swap error.

If you make an error then you get sent the wrong book. It would be great if the shop could detect these errors. There are many ways to do this. We will look at the check-digit method.

### Example 1

## Sum of digits method:

We add a check-digit at the end of each four digit code-number. So now each book has a five digit code-number. The check-digit is chosen so that the sum of the digits is a multiple of 10.

If a book has code-number 3725, then the check-digit is 3 because  $3+7+2+5+3=20=2 \times 10$

This book now has code-number 37253

The shop will not send you the wrong book because 37283 does not correspond to any book. The shop will know you have made an error and will ask you to re-order.

The shop will send you the wrong book.

## Example 2

**Weighted sum of digits method:**

We add a check-digit at the end of each four digit code-number. So now each book has a five digit code-number. The check-digit is chosen so that the weighted-sum of the digits is a multiple of 10.

If a book has code-number 3725 and if we use the weights: 1, 3, 1, 3, 1,

	3	7	2	5	?
weight	1	3	1	3	1

then the check-digit is 9 because  $(3 \times 1) + (7 \times 3) + (2 \times 1) + (5 \times 3) + (9 \times 1) = 50 = 5 \times 10$

The book now has code-number 37259

If you make a digit error and type in 37659

	3	7	6	5	9
weight	1	3	1	3	1

then this will be detected because  $(3 \times 1) + (7 \times 3) + (6 \times 1) + (5 \times 3) + (9 \times 1) = 54$

If you make a swap error and type in 37529

	3	7	5	2	9
weight	1	3	1	3	1

then this will be detected because  $(3 \times 1) + (7 \times 3) + (5 \times 1) + (2 \times 3) + (9 \times 1) = 44$

### Example 3

If a book has code-number 3521 and we are using the weights: 1, 4, 1, 4, 1

then the check-digit is 1.

The book now has code-number 35211.

If you make a digit error and type in 35261

	3	5	2	6	1
weight	1	4	1	4	1

then this will not be detected.

In the code-number, you replaced 1 by 6. The digit has changed by 5.

In the weighted sum, you replaced  $(1 \times 4)$  by  $(6 \times 4)$ . The difference is  $5 \times 4 = 20$

The weighted sum has changed by a multiple of 10 and so the error will not be detected.

So for digit errors:

If the digit changes by 5 and the weight is a multiple of 2

Or

If the digit changes by a multiple of 2 and the weight is 5

then the error will not be detected.

So we avoid using 2, 4, 5, 6, 8 as weights, and use 1, 3, 7, 9 instead. This means all digit errors will be detected.

We also use different weights on adjacent digits so that most swap errors are detected.

### Example 4

If a book has code-number 4273 and we are using the weights: 1, 9, 1, 9, 1

then the check-digit is 4.

The book now has code-number 42734

If you make a swap error and type in 47234

	4	7	2	3	4
weight	1	9	1	9	1

then this will not be detected.

In the code-number you swapped 2 and 7. The difference between these digits is 5.

In the weighted sum, you replaced  $(2 \times 9) + (7 \times 1)$  by  $(7 \times 9) + (2 \times 1)$ . The difference is 40.

The weighted sum has changed by a multiple of 10 and so the error will not be detected.

So for swap errors:

If the digits that are swapped differ by 5 and their weights differ by a multiple of 2 (which they will if we only use 1, 3, 7, 9 as weights) then the error will not be detected.

There are lots of other check-digit methods. For example, some books have a 10 digit ISBN number. The book, Symmetry by Hermann Weyl has the number 0691023743

The last digit is the check-digit. This is calculated as follows:

ISBN	0	6	9	1	0	2	3	7	4	3
weight	10	9	8	7	6	5	4	3	2	1

The weighted sum is:

$$(0 \times 10) + (6 \times 9) + (9 \times 8) + (1 \times 7) + (0 \times 6) + (2 \times 5) + (3 \times 4) + (7 \times 3) + (4 \times 2) + (3 \times 1) = 187$$

The check-digit is chosen so that this weighted sum is divisible by 11.

If the check-digit is 10 then it is denoted by X in the ISBN code.

## Error Correcting Codes

Your space probe is approaching Pluto. It takes a black and white photo and sends it back to Earth. The photo is made up of pixels. Each pixel can be one of sixteen grey-levels. Each grey-level is represented by a 4-digit binary-string. So 0000 represents a white pixel, 1111 represents a black pixel and all the other binary-strings represent shades of grey in-between.

Here are the sixteen possible binary-strings:

0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111

Back on Earth, you receive a sequence of binary-strings, each binary-string telling you the grey-level of a pixel.

There might be transmission errors. The space probe sends a 0 and you receive a 1 or the space probe sends a 1 and you receive a 0. We want to detect these errors. But if we detect an error, we can't tell the space probe to go back and take the photo again. We need a way to correct the error. We are going to add 3 extra digits at the end of each binary-string. Richard Hamming came up with a clever way to do this. Here are the sixteen binary-strings with their extra digits added on:

0	0	0	0	0	0	0
0	0	0	1	0	1	1
0	0	1	0	1	1	0
0	0	1	1	1	0	1
0	1	0	0	1	0	1
0	1	0	1	1	1	0
0	1	1	0	0	1	1
0	1	1	1	0	0	0
1	0	0	0	1	1	1
1	0	0	1	1	0	0
1	0	1	0	0	0	1
1	0	1	1	0	1	0
1	1	0	0	0	1	0
1	1	1	0	1	0	0
1	1	1	1	1	1	1

We call these our good-strings.

Take any two good-strings, for example, 0010110 and 1011010

To change the first good-string into the second good-string you have to change three of the digits.

The first one, the fourth one and the fifth one.

Hamming chose the extra digits so that to change any good-string into any other good-string you have to change at least three of the digits.

1001100 is a good-string.

If you change just the first digit you get 0001100

If you change just the second digit you get 1101100

...

If you change just the seventh digit you get 1001101

We call these strings the bad-neighbours of 1001100

1001100 has seven bad-neighbours.

1011010 is another good-string.

1011010 has seven bad-neighbours.

good-string	good-string
1001100	1011010
bad-neighbours	bad-neighbours
0001100	0011010
1101100	1111010
1011100	1001010
1000100	1010010
1001000	1011110
1001110	1011000
1001101	1011011

Can a bad-neighbour of 1001100 also be a bad-neighbour of 1011010?

If yes, then we could start with 1001100, change one digit to get a bad-neighbour and then change one more digit to get 1011010. We would have changed a good-string into another good-string by changing just two digits. We know this is not possible.

So a bad-neighbour of one good-string cannot be a bad-neighbour of another good-string.

We have sixteen good-strings and each good-string has seven bad-neighbours making a total of 128 different strings. This accounts for every possible 7-digit binary-string.

So every binary-string is either a good-string or a bad-neighbour.

So every binary-string is either a good-string or one digit change away from a good-string.

Back on Earth you receive the string 1010011

This is not a good-string. An error has occurred. We assume that only one digit has been corrupted.

If errors are very rare then this seems reasonable.

We correct this error by replacing 1010011 by the good-string 1010001 which is only one digit change away.

Error correcting codes are useful whenever we want to store or transmit digital data.

## Complex Numbers

### Example

We can try to solve the quadratic equation

$$x^2 - 4x + 13 = 0$$

using the quadratic formula

$$x = \frac{4 \pm \sqrt{16 - 52}}{2} = \frac{4 \pm \sqrt{-36}}{2}$$

At this point we give up because  $\sqrt{-36}$  does not exist.

Let's introduce a new number  $i$  where  $i^2 = -1$

Now

$$(6i)^2 = 6i \times 6i = 36i^2 = -36$$

So we can now solve our equation

$$x = \frac{4 \pm 6i}{2} = 2 \pm 3i$$

Check:

If

$$x = 2 + 3i$$

then

$$x^2 = (2 + 3i)(2 + 3i) = 4 + 6i + 6i + 9i^2 = 4 + 12i - 9 = -5 + 12i$$

So

$$x^2 - 4x + 13 = (-5 + 12i) - 4(2 + 3i) + 13 = -5 + 12i - 8 - 12i + 13 = 0 \text{ Good.}$$

And if

$$x = 2 - 3i \text{ etc}$$

A number like  $2 + 3i$  is called a complex number. We can add, subtract, multiply and divide complex numbers:

Addition

$$(3 + 7i) + (2 - 5i) = 5 + 2i$$

Subtraction

$$(3 + 7i) - (2 - 5i) = 1 + 12i$$

Multiplication

$$(3 + 7i)(2 - 5i) = 6 - 15i + 14i - 35i^2 = 6 - 15i + 14i + 35 = 41 - i$$

Division

Here we need a trick

$$\frac{(3+7i)}{(2-5i)} = \frac{(3+7i)(2+5i)}{(2-5i)(2+5i)} = \dots = \frac{-29+29i}{29} = -1+i$$

Squaring

$$(3+7i)^2 = 9+42i+49i^2 = 9+42i-49 = -40+42i$$

Powers of  $i$

$$i^3 = (i^2)i = (-1)i = -i$$

$$i^4 = (i^2)(i^2) = (-1)(-1) = 1$$

$$i^5 = (i^2)(i^2)i = (-1)(-1)i = i$$

$$i^{379} = \dots = i^3 = -i$$

Quadratic equations

$$x^2 - 4x + 29 = 0$$

$$x = \frac{4 \pm \sqrt{-100}}{2} = 2 \pm 5i$$

Real and imaginary parts.

We say 2 is the real part of  $2+3i$  and we say 3 is the imaginary part of  $2+3i$

Example

$$2x+y+3i-4iy=10-5i$$

where  $x$  and  $y$  are real numbers

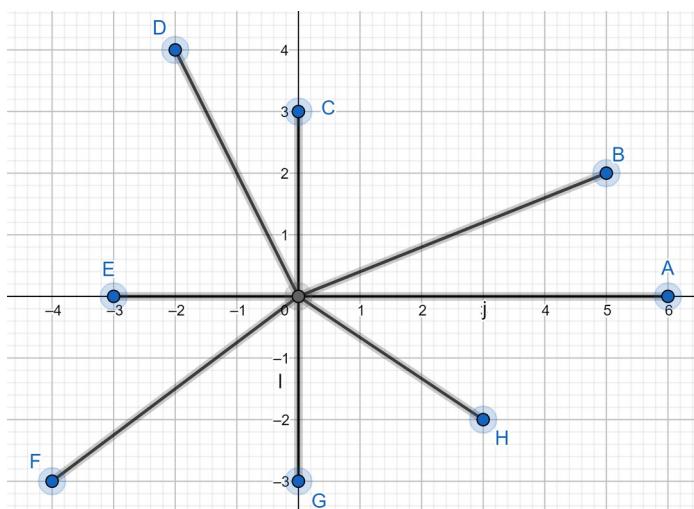
We can rewrite this as:

$$(2x+y)+i(3-4y)=(10)+i(-5)$$

If two complex numbers are equal then their real parts must be equal and their imaginary parts must be equal.

So  $2x+y=10$  and  $3-4y=-5$  so  $x=4$  and  $y=2$

We can think of a complex number as a point on a number plane:



A is the complex number:

6

B is the complex number:

$$5+2i$$

C is the complex number:

$3i$

D is the complex number:

$$-2+4i$$

E is the complex number:

-3

F is the complex number:

$$-4-3i$$

G is the complex number:

$-3i$

H is the complex number:

$$3-2i$$

If  $z=4+2i$  then:

a)  $iz=i(4+2i)=-2+4i$

Draw a line from the origin  $O$  to  $z$  Draw a line from the origin  $O$  to  $iz$

Multiplying  $z$  by  $i$  is the same as rotating  $Oz$  by  $\frac{\pi}{2}$

b)  $-z=-(4+2i)=-4-2i$

Multiplying  $z$  by  $-1$  is the same as rotating  $Oz$  by  $\pi$

c)  $-iz=-i(4+2i)=2-4i$

Multiplying  $z$  by  $-i$  is the same as rotating  $Oz$  by  $-\frac{\pi}{2}$

### Fundamental Theorem of Algebra

Without complex numbers, some polynomials can be factorised:

$$x^2 - 5x + 6 = (x-2)(x-3)$$

but other polynomials cannot be factorised:

$$x^2 - 4x + 13$$

However, with complex numbers we have a nice result:

Every polynomial of degree  $n$  can be factorised into  $n$  brackets.

For example  $x^4 - 4x^3 + 3x^2 + 2x - 6 = (x+1)(x-3)(x-1+i)(x-1-i)$

Footnote:

Did mathematicians invent complex numbers or did they invent them?

## EXERCISE

1)

Evaluate

- a)  $(3+5i)+(-2+7i)$
- b)  $(5-3i)-(8+4i)$
- c)  $(1+3i)(5-2i)$
- d)  $\frac{(8+5i)}{(7+2i)}$  hint multiply top and bottom by  $(7-2i)$
- e)  $(2-5i)^2$

2)

Solve

- a)  $x^2 - 6x + 13 = 0$
- b)  $x^2 - 14x + 58 = 0$

3)

Solve  $3x+iy-6+2i=2ix+3y+8i$  where  $x$  and  $y$  are real numbers

## SOLUTIONS

1)

- a)  $1+12i$
- b)  $-3-7i$
- c)  $11+13i$
- d)  $\frac{66}{53} + \frac{19}{53}i$
- e)  $-21-20i$

2)

$$\begin{aligned} a) \quad x &= \frac{2 \pm \sqrt{4-52}}{2} = \frac{2 \pm \sqrt{-48}}{2} = 1 \pm 12i \\ b) \quad x &= \frac{14 \pm \sqrt{196-232}}{2} = \frac{14 \pm \sqrt{-36}}{2} = 7 \pm 3i \end{aligned}$$

3)

equating real parts:

$$3x - 6 = 3y$$

equating imaginary parts:

$$y + 2 = 2x + 8$$

$$x = -8 \quad y = -10$$

## Euler's Identity

In the chapter, Maclaurin Series we saw that:

$$\cos x = 1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^4 + \dots$$

$$\sin x = x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5$$

$$e^x = 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \frac{1}{4!}x^4 + \dots$$

So

$$e^{(i\theta)} = 1 + (i\theta) + \frac{1}{2!}(i\theta)^2 + \frac{1}{3!}(i\theta)^3 + \frac{1}{4!}(i\theta)^4 + \frac{1}{5!}(i\theta)^5 + \dots$$

$$e^{i\theta} = 1 + i\theta - \frac{1}{2!}\theta^2 - \frac{1}{3!}i\theta^3 + \frac{1}{4!}\theta^4 + \frac{1}{5!}i\theta^5 + \dots$$

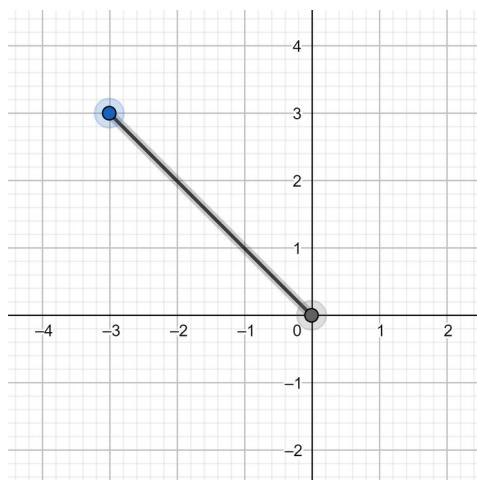
$$e^{(i\theta)} = \left( 1 - \frac{1}{2!}\theta^2 + \frac{1}{4!}\theta^4 + \dots \right) + i \left( \theta - \frac{1}{3!}\theta^3 + \frac{1}{5!}\theta^5 + \dots \right)$$

$$e^{(i\theta)} = \cos \theta + i \sin \theta$$

This is Euler's identity. It is simply astounding.

## Mod-arg form

The point  $(-3, 3)$  represents the complex number  $-3+3i$



The length of the line from the origin to  $-3+3i$  is:

$$r = \sqrt{(-3)^2 + (3)^2} = \sqrt{18} \quad \text{We say } \text{mod}(-3+3i) = \sqrt{18}$$

The angle between the positive  $x$  axis and the line from the origin to  $-3+3i$  is:

$$\theta = \frac{3\pi}{4} \quad \text{We say } \text{arg}(-3+3i) = \frac{3\pi}{4}$$

We know from trigonometry that:

$$\cos\theta = \frac{-3}{\sqrt{18}} \text{ and } \sin\theta = \frac{3}{\sqrt{18}} \text{ so } -3 = \sqrt{18}\cos\theta \text{ and } 3 = \sqrt{18}\sin\theta$$

So:

$$-3 + 3i = \sqrt{18} \cos \frac{3\pi}{4} + i \sqrt{18} \sin \frac{3\pi}{4} = \sqrt{18} \left( \cos \frac{3\pi}{4} + i \sin \frac{3\pi}{4} \right) = \sqrt{18} e^{i3\pi/4}$$

In general

We can write  $x+iy$  in the form  $r e^{i\theta}$  where  $r = \text{mod}(x+iy)$  and  $\theta = \arg(x+iy)$

Where

$$r = \sqrt{x^2 + y^2}$$

and

$$\cos\theta = \frac{x}{r} \text{ and } \sin\theta = \frac{y}{r} \text{ so } \tan\theta = \frac{y}{x} \text{ so } \theta = \tan^{-1}\left(\frac{y}{x}\right) \text{ We usually choose } -\pi < \theta \leq \pi$$

If we want to convert a complex number to mod-arg form then it is a good idea to mark the number on the number plane. Do this and show that:

$$\text{mod}(1+i\sqrt{3})=2 \quad \arg(1+i\sqrt{3})=\frac{\pi}{3} \quad \text{so } 1+i\sqrt{3}=2e^{i\pi/3}$$

$$\text{mod}(4-4i)=\sqrt{32} \quad \arg(4-4i)=-\frac{\pi}{4} \quad \text{so } 4-4i=\sqrt{32}e^{-i\pi/4}$$

$$\text{mod}(-1)=1 \quad \arg(-1)=\pi \quad \text{so } -1=e^{i\pi}$$

$$\text{mod}(i)=1 \quad \arg(i)=\frac{\pi}{2} \quad \text{so } i=e^{i\pi/2}$$

$$\text{mod}(-i)=1 \quad \arg(-i)=-\frac{\pi}{2} \quad \text{so } -i=e^{-i\pi/2}$$

There are advantages in writing complex numbers in mod-arg form, for example:

multiplication

$$(3e^{i\pi/4})(5e^{i\pi/2})=15e^{i3\pi/4}$$

division

$$\frac{12e^{i\pi}}{4e^{i\pi/3}}=3e^{i2\pi/3}$$

powers

$$(2e^{i\pi/7})^5=32e^{i5\pi/7}$$

Note:

If  $w = r e^{i\theta}$  and  $z = t e^{i\phi}$  then  $wz = rt e^{i(\theta+\phi)}$

So

$$\text{mod}(wz) = \text{mod}(w) \times \text{mod}(z)$$

And

$$\arg(wz) = \arg(w) + \arg(z)$$

Note:

If  $z = r e^{i\theta}$  then:

a)  $iz = (e^{i\pi/2})r e^{i\theta} = r e^{i(\theta+\pi/2)}$

Multiplying  $z$  by  $i$  is the same as rotating  $Oz$  by  $\frac{\pi}{2}$

b)  $-z = (e^{i\pi})r e^{i\theta} = r e^{i(\theta+\pi)}$

Multiplying  $z$  by  $-1$  is the same as rotating  $Oz$  by  $\pi$

c)  $-iz = (e^{-i\pi/2})r e^{i\theta} = r e^{i(\theta-\pi/2)}$

Multiplying  $z$  by  $-i$  is the same as rotating  $Oz$  by  $-\frac{\pi}{2}$

Let's fool around with Euler's identity  $e^{i\theta} = \cos\theta + i\sin\theta$

a) Put  $\theta = \pi$  in Euler's identity

$$e^{i\pi} = \cos\pi + i\sin\pi = -1 \text{ so } -1 = e^{i\pi}$$

So:

$$(-1)^i = (e^{i\pi})^i = e^{-\pi} \text{ which is real}$$

And:

$$\ln(-1) = \ln(e^{i\pi}) = i\pi$$

And:

$$e^{i\pi} + 1 = 0 \text{ My five favourite numbers all in one neat formula.}$$

b) Put  $\theta = \pi/2$  in Euler's identity

$$e^{i\pi/2} = \cos\pi/2 + i\sin\pi/2 = i \text{ so } i = e^{i\pi/2}$$

So:

$$(i)^i = e^{-\pi/2} \text{ which is real}$$

And:

$$\ln(i) = i\pi/2$$

c) We have shown that  $e^{i\theta} = \cos\theta + i\sin\theta$  We can also show that  $e^{-i\theta} = \cos\theta - i\sin\theta$

Adding gives:

$$2\cos\theta = e^{i\theta} + e^{-i\theta} \quad \text{So} \quad \cos\theta = \frac{1}{2}(e^{i\theta} + e^{-i\theta})$$

Subtracting gives:

$$2i\sin\theta = e^{i\theta} - e^{-i\theta} \quad \text{So} \quad \sin\theta = \frac{1}{2i}(e^{i\theta} - e^{-i\theta})$$

So:

$$\cos(i) = \frac{1}{2}\left(\frac{1}{e} + e\right) \quad \text{and} \quad \sin(i) = \frac{1}{2i}\left(\frac{1}{e} - e\right)$$

d) Solve  $\cos\theta = 2$

$$\frac{1}{2}(e^{i\theta} + e^{-i\theta}) = 2 \quad \text{so} \quad e^{i\theta} + e^{-i\theta} = 4 \quad \text{so} \quad e^{i2\theta} - 4e^{i\theta} + 1 = 0 \quad \text{so} \quad e^{i\theta} = \frac{4 \pm \sqrt{16-4}}{2} = 2 \pm \sqrt{3}$$

Now:

$$e^{i\theta} = 2 + \sqrt{3} \quad \text{so} \quad \theta = \frac{1}{i} \ln(2 + \sqrt{3})$$

And:

$$e^{i\theta} = 2 - \sqrt{3} \quad \text{so} \quad \theta = \frac{1}{i} \ln(2 - \sqrt{3})$$

Footnote:

We have been rather casual in our approach to complex numbers. For example, we know that

$(e^a)(e^b) = e^{a+b}$  is true if  $a$  and  $b$  are real numbers and we have just assumed it is also true if  $a$  and  $b$  are complex numbers. Which of the rules that apply to real numbers still apply to complex numbers? We need to be careful about this or we can run into problems ...

a)  $1 = \sqrt{-1} = \sqrt{-1 \times -1} = \sqrt{-1} \times \sqrt{-1} = i^2 \quad \text{so} \quad 1 = -1$

b)  $e^{i2\pi} = 1 \quad \text{and} \quad e^{i4\pi} = 1 \quad \text{so} \quad e^{i2\pi} = e^{i4\pi} \quad \text{so} \quad \ln(e^{i2\pi}) = \ln(e^{i4\pi}) \quad \text{so} \quad i2\pi = i4\pi \quad \text{so} \quad 2\pi = 4\pi$

c)  $(-1)^2 = 1 \quad \text{so} \quad \ln((-1)^2) = \ln(1) \quad \text{so} \quad 2\ln(-1) = 0 \quad \text{so} \quad \ln(-1) = 0 \quad \text{so} \quad -1 = e^0$

## EXERCISE

1)

Write in mod-arg form:

a)  $\sqrt{3}+i$       b)  $-1+i$       c)  $-2-2i$       d)  $1-\sqrt{3}i$

2)

If  $w=2e^{i\pi/4}$  and  $z=3e^{i2\pi/3}$  write down:

Write in mod-arg form:

a)  $wz$       b)  $\frac{w}{z}$       c)  $w^7$       d)  $iw$       e)  $-z$       f)  $-iw$

3)

Convert  $(1+i)$  to mod-arg form and hence find  $(1+i)^{16}$

## SOLUTIONS

1)

Mark these numbers on a number plane

a)  $\sqrt{3}+i=2e^{i\pi/6}$       b)  $-1+i=\sqrt{2}e^{i3\pi/4}$       c)  $-2-2i=\sqrt{8}e^{(-3\pi/4)}$       d)  $1-\sqrt{3}i=2e^{-i\pi/3}$

2)

a)  $6e^{i11\pi/12}$       b)  $\frac{2}{3}e^{-i5\pi/12}$       c)  $128e^{i7\pi/4}$  which we can write as  $128e^{-i\pi/4}$

d)  $2e^{i3\pi/4}$       e)  $3e^{i5\pi/3}$  which we can write as  $3e^{-i\pi/3}$       f)  $2e^{-i\pi/4}$

3)

$1+i=\sqrt{2}e^{i\pi/4}$  so  $(1+i)^{16}=(\sqrt{2})^{16}(e^{i\pi/4})^{16}=256e^{i4\pi}=256$

## Using Complex Numbers

Some real problems can be solved using complex numbers. Here are some examples.

### 1. Deriving trig identities

#### a) Pythagoras identity:

We know:

$$\cos\theta = \frac{1}{2}(e^{i\theta} + e^{-i\theta}) \quad \text{and} \quad \sin\theta = \frac{1}{2i}(e^{i\theta} - e^{-i\theta})$$

Show that:

$$\cos^2\theta + \sin^2\theta = 1$$

#### b) Addition identity:

$$(cos\theta + isin\theta)(cos\phi + isin\phi) = e^{i\theta} e^{i\phi} = e^{i(\theta+\phi)} = cos(\theta+\phi) + isin(\theta+\phi)$$

Equating real parts:

$$cos(\theta+\phi) = cos\theta cos\phi - sin\theta sin\phi$$

Equating imaginary parts:

$$sin(\theta+\phi) = cos\theta sin\phi + sin\theta cos\phi$$

#### c) Double angle identity:

$$(cos\theta + isin\theta)^2 = (e^{i\theta})^2 = e^{i2\theta} = cos(2\theta) + isin(2\theta)$$

Equating real parts:

$$cos 2\theta = cos^2\theta - sin^2\theta$$

Equating imaginary parts:

$$sin 2\theta = 2 cos\theta sin\theta$$

Note:

de Moivre's theorem:

$$(cos\theta + isin\theta)^n = cos(n\theta) + isin(n\theta)$$

#### d) Half angle identity:

We know:

$$2 cos\theta = e^{i\theta} + e^{-i\theta}$$

So:

$$(2 cos\theta)^2 = (e^{i\theta} + e^{-i\theta})^2$$

Multiply out the brackets:

$$2^2 \cos^2 \theta = e^{i2\theta} + 2 + e^{-i2\theta}$$

Collect up terms:

$$2^2 \cos^2 \theta = (e^{i2\theta} + e^{-i2\theta}) + 2$$

Write with cosines:

$$2^2 \cos^2 \theta = 2 \cos 2\theta + 2$$

So:

$$\cos^2 \theta = \frac{1}{2} \cos 2\theta + \frac{1}{2}$$

e) Factor identity:

We know:

$$2 \cos \theta = e^{i\theta} + e^{-i\theta} \quad \text{and} \quad 2i \sin \theta = e^{i\theta} - e^{-i\theta}$$

So:

$$\sin \theta \cos \phi = \frac{1}{2i} (e^{i\theta} - e^{-i\theta}) \frac{1}{2} (e^{i\phi} + e^{-i\phi})$$

Show that:

$$\sin \theta \cos \phi = \frac{1}{2} \sin(\theta + \phi) + \frac{1}{2} \sin(\theta - \phi)$$

We could write:

$$\sin \alpha + \sin \beta = 2 \sin \left( \frac{\alpha + \beta}{2} \right) \cos \left( \frac{\alpha - \beta}{2} \right) \quad \text{can you see how?}$$

I could go on ...

## 2. Integration

Example

We want to work out:

$$\int e^{-x} \cos x \, dx \quad \text{and} \quad \int e^{-x} \cos x \, dx$$

Here we go:

$$\int e^{-x} (\cos x + i \sin x) \, dx = \int e^{-x} e^{ix} \, dx = \int e^{(-1+i)x} \, dx = \frac{1}{(-1+i)} e^{(-1+i)x} + C = \frac{1}{(-1+i)} e^{-x} e^{ix} + C$$

But

$$\frac{1}{(-1+i)} = \frac{-1-i}{(-1+i)(-1-i)} = -\frac{1}{2}(1+i)$$

So

$$\int e^{-x}(\cos x + i \sin x) dx = -\frac{1}{2}(1+i)e^{-x}(\cos x + i \sin x) + c$$

Equating real parts:

$$\int e^{-x} \cos x dx = -\frac{1}{2} e^{-x} (\cos x - \sin x) + c' \text{ where } c' \text{ is the real part of } c$$

Equating imaginary parts:

$$\int e^{-x} \sin x dx = -\frac{1}{2} e^{-x} (\cos x + \sin x) + c'' \text{ where } c'' \text{ is the imaginary part of } c$$

3. A formula for  $\ln \sqrt{2}$  and  $\pi$

a)  $1+i = \sqrt{2} e^{i\pi/4}$

So:

$$\ln(1+i) = \ln(\sqrt{2}) + \ln(e^{i\pi/4}) = \ln(\sqrt{2}) + \frac{i\pi}{4}$$

b)  $\ln(1+x) = x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \frac{1}{4}x^4 + \dots$  this is the Maclaurin series

So:

$$\ln(1+i) = i - \frac{1}{2}i^2 + \frac{1}{3}i^3 - \frac{1}{4}i^4 + \dots = i + \frac{1}{2} - \frac{1}{3}i - \frac{1}{4} + \dots$$

c) From (a) and (b) we have:

$$\ln(\sqrt{2}) + \frac{i\pi}{4} = i + \frac{1}{2} - \frac{1}{3}i - \frac{1}{4} + \dots$$

Equating real parts:

$$\ln(\sqrt{2}) = \frac{1}{2} - \frac{1}{4} + \frac{1}{6} - \frac{1}{8} + \dots$$

Equating imaginary parts:

$$\frac{\pi}{4} = \frac{1}{1} - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots$$

4. Van Aubel's Theorem if you know about vectors ...

What do you make of the following proof, where we have recklessly mixed up complex numbers and vectors?

If  $\mathbf{v}$  is a vector then  $i\mathbf{v}$  is the vector you get by rotating  $\mathbf{v}$  anti-clockwise by  $90^\circ$

Draw some diagrams and convince yourself that:

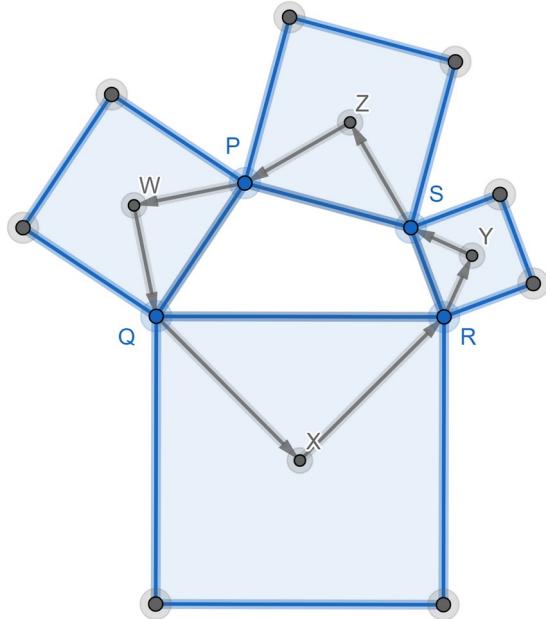
$$i\mathbf{w} + i\mathbf{v} = i(\mathbf{w} + \mathbf{v}) \text{ and } i^2\mathbf{w} = -\mathbf{w} \text{ and if } \mathbf{w} + i\mathbf{w} = \mathbf{0} \text{ then } \mathbf{w} = \mathbf{0}$$

Given any quadrilateral PQRS, draw a square on each side.

W, X, Y and Z are the centres of these squares.

Theorem

ZX and YW will have the same length and are at right-angles.



Proof

$$\text{Let } \mathbf{a} = \vec{PW} \text{ so } i\mathbf{a} = \vec{WQ}$$

$$\text{Let } \mathbf{b} = \vec{QX} \text{ so } i\mathbf{b} = \vec{XR}$$

$$\text{Let } \mathbf{c} = \vec{RY} \text{ so } i\mathbf{c} = \vec{YS}$$

$$\text{Let } \mathbf{d} = \vec{SZ} \text{ so } i\mathbf{d} = \vec{ZP}$$

From the diagram:

$$\mathbf{a} + i\mathbf{a} + \mathbf{b} + i\mathbf{b} + \mathbf{c} + i\mathbf{c} + \mathbf{d} + i\mathbf{d} = \mathbf{0}$$

So:

$$(\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d}) + i(\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d}) = \mathbf{0}$$

So:

$$(\mathbf{a} + \mathbf{b} + \mathbf{c} + \mathbf{d}) = \mathbf{0}$$

Now:

$$\vec{YW} = i\mathbf{c} + \mathbf{d} + i\mathbf{d} + \mathbf{a}$$

So:

$$i\vec{YW} = i^2\mathbf{c} + i\mathbf{d} + i^2\mathbf{d} + i\mathbf{a} = -\mathbf{c} + i\mathbf{d} - \mathbf{d} + i\mathbf{a}$$

Now:

$$\vec{ZX} = i\mathbf{d} + \mathbf{a} + i\mathbf{a} + \mathbf{b} \quad \text{But } \mathbf{b} = -(\mathbf{a} + \mathbf{c} + \mathbf{d})$$

So:

$$\vec{ZX} = i\mathbf{d} + \mathbf{a} + i\mathbf{a} - (\mathbf{a} + \mathbf{c} + \mathbf{d}) = -\mathbf{c} + i\mathbf{d} - \mathbf{d} + i\mathbf{a}$$

So:

$$\vec{ZX} = i \vec{YW} \text{ as required.}$$

## EXERCISE

1)

Derive trig identities for:

$$\cos(\theta - \phi) \text{ and } \sin(\theta - \phi)$$

2)

Derive trig identities for:

$$\cos 3\theta \text{ and } \sin 3\theta$$

3)

Derive the half angle formula for  $\sin^2 \theta$

4)

Use the method of question (3) to write  $\cos^5 \theta$  in terms of  $\cos 5\theta$  and  $\cos 3\theta$  and  $\cos \theta$

5)

Show that:

$$\cos \theta \cos \phi = \frac{1}{2} \cos(\theta + \phi) + \frac{1}{2} \cos(\theta - \phi)$$

or if you prefer:

$$\cos \alpha + \cos \beta = 2 \cos\left(\frac{\alpha + \beta}{2}\right) \cos\left(\frac{\alpha - \beta}{2}\right)$$

6)

We want to evaluate:

$$S = \frac{1}{2} \cos \theta + \frac{1}{4} \cos 2\theta + \frac{1}{8} \cos 3\theta + \dots$$

Now:

$$\cos \theta = \frac{1}{2}(e^{i\theta} + e^{-i\theta}) \text{ so } \cos 2\theta = \frac{1}{2}(e^{i2\theta} + e^{-i2\theta}) \text{ and } \cos 3\theta = \frac{1}{2}(e^{i3\theta} + e^{-i3\theta}) \text{ etc}$$

Show that:

$$S = \left( \frac{1}{4}(e^{i\theta}) + \frac{1}{8}(e^{i2\theta}) + \frac{1}{16}(e^{i3\theta}) + \dots \right) + \left( \frac{1}{4}(e^{-i\theta}) + \frac{1}{8}(e^{-i2\theta}) + \frac{1}{16}(e^{-i3\theta}) + \dots \right)$$

Show that:

$$\frac{1}{4}(e^{i\theta}) + \frac{1}{8}(e^{i2\theta}) + \frac{1}{16}(e^{i3\theta}) + \dots = \frac{\frac{1}{4}(e^{i\theta})}{1 - \frac{1}{2}(e^{i\theta})} \quad \text{hint, geometric series}$$

Show that:

$$\frac{1}{4}(e^{-i\theta}) + \frac{1}{8}(e^{-i2\theta}) + \frac{1}{16}(e^{-i3\theta}) + \dots = \frac{\frac{1}{4}(e^{-i\theta})}{1 - \frac{1}{2}(e^{-i\theta})} \quad \text{hint, geometric series}$$

Show that:

$$S = \frac{\frac{1}{4}(e^{i\theta})}{1 - \frac{1}{2}(e^{i\theta})} + \frac{\frac{1}{4}(e^{-i\theta})}{1 - \frac{1}{2}(e^{-i\theta})}$$

Show that:

$$S = \frac{2\cos\theta - 1}{5 - 4\cos\theta}$$

7)

Another formula for  $\pi$

a)  $\tan^{-1}x = x - \frac{1}{3}x^3 + \frac{1}{5}x^5 - \frac{1}{7}x^7 + \dots$  this is the Maclaurin series

b) Show that:

$$(2+i)(3+i) = 5+5i$$

So:

$$\arg(2+i) + \arg(3+i) = \arg(5+5i)$$

So:

$$\tan^{-1}\left(\frac{1}{2}\right) + \tan^{-1}\left(\frac{1}{3}\right) = \tan^{-1}\left(\frac{5}{5}\right) \quad \text{but } \tan^{-1}\left(\frac{5}{5}\right) = \tan^{-1}(1) = \frac{\pi}{4}$$

So:

$$\tan^{-1}\left(\frac{1}{2}\right) + \tan^{-1}\left(\frac{1}{3}\right) = \frac{\pi}{4}$$

c) Write down the Maclaurin series for:

$$\tan^{-1}\left(\frac{1}{2}\right) \quad \text{and} \quad \tan^{-1}\left(\frac{1}{3}\right)$$

Show that:

$$\frac{\pi}{4} = \left(\frac{1}{2} + \frac{1}{3}\right) - \frac{1}{3}\left(\frac{1}{2^3} + \frac{1}{3^3}\right) + \frac{1}{5}\left(\frac{1}{2^5} + \frac{1}{3^5}\right) + \dots$$

8)

We can make up more formulas for  $\pi$  using the method of question (7)

We need to find  $a, b, c$  where  $(a+i)(b+i) = c+ci$

Show that:

$$ab - 1 = a + b$$

Show that:

$$b = \frac{a+1}{a-1}$$

Now let:

$$a = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers and } p > q > 0$$

Show that:

$$b = \frac{p+q}{p-q}$$

So:

$$\left( \frac{p}{q} + i \right) \left( \frac{p+q}{p-q} + i \right) = c + ci$$

Show that:

$$(p+iq)((p+q)+i(p-q)) = (p^2+q^2)+i(p^2+q^2)$$

So:

$$\arg(p+iq) + \arg((p+q)+i(p-q)) = (p^2+q^2)+i(p^2+q^2)$$

So:

$$\tan^{-1}\left(\frac{q}{p}\right) + \tan^{-1}\left(\frac{p-q}{p+q}\right) = \frac{\pi}{4}$$

Write down the Maclaurin series for:

$$\tan^{-1}\left(\frac{q}{p}\right) \text{ and } \tan^{-1}\left(\frac{p-q}{p+q}\right) \text{ to get a formula for } \pi$$

I chose  $p=17$  and  $q=4$

So:

$$\tan^{-1}\left(\frac{4}{17}\right) + \tan^{-1}\left(\frac{13}{21}\right) = \frac{\pi}{4}$$

and then I got:

$$\frac{\pi}{4} = \left( \frac{4}{17} + \frac{13}{21} \right) - \frac{1}{3} \left( \frac{4^3}{17^3} + \frac{13^3}{21^3} \right) + \frac{1}{5} \left( \frac{4^5}{17^5} + \frac{13^5}{21^5} \right) + \dots$$

## SOLUTIONS

1)

$$(\cos\theta + i\sin\theta)(\cos\phi - i\sin\phi) = e^{i\theta}e^{-i\phi} = e^{i(\theta-\phi)} = \cos(\theta-\phi) + i\sin(\theta-\phi)$$

Equating real parts:

$$\cos\theta\cos\phi + \sin\theta\sin\phi = \cos(\theta-\phi)$$

Equating imaginary parts:

$$-\cos\theta\sin\phi + \sin\theta\cos\phi = \sin(\theta-\phi)$$

2)

$$(\cos\theta + i\sin\theta)^3 = (e^{i\theta})^3 = e^{i3\theta} = \cos(3\theta) + i\sin(3\theta)$$

Equating real parts:

$$\cos^3\theta - 3\cos\theta\sin^2\theta = \cos 3\theta$$

We could replace  $\sin^2\theta$  by  $1 - \cos^2\theta$  and write  $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$

Equating imaginary parts:

$$3\cos^2\theta\sin\theta - \sin^3\theta = \sin 3\theta$$

We could replace  $\cos^2\theta$  by  $1 - \sin^2\theta$  and write  $\sin 3\theta = 3\sin\theta - 4\sin^3\theta$

Dividing:

$$\frac{3\cos^2\theta\sin\theta - \sin^3\theta}{\cos^3\theta - 3\cos\theta\sin^2\theta} = \frac{\sin 3\theta}{\cos 3\theta}$$

Divide top and bottom of the left-hand-side by  $\cos^3\theta$

$$\frac{3\tan\theta - \tan^3\theta}{1 - 3\tan^2\theta} = \tan 3\theta$$

3)

$$(2i\sin\theta)^2 = (e^{i\theta} - e^{-i\theta})^2$$

Multiply out the brackets:

$$2^2 i^2 \sin^4\theta = e^{i2\theta} - 2 + e^{-i2\theta}$$

Collect up terms:

$$-2^2 \sin^2\theta = (e^{i2\theta} + e^{-i2\theta}) - 2$$

Write with cosines:

$$-2^2 \sin^2\theta = 2\cos 2\theta - 2$$

So:

$$\sin^2\theta = \frac{1}{2} - \frac{1}{2}\cos 2\theta$$

4)

$$(2\cos\theta)^5 = (e^{i\theta} + e^{-i\theta})^5$$

Multiply out the brackets:

$$2^5 \cos^5\theta = e^{i5\theta} + 5e^{i3\theta} + 10e^{i\theta} + 10e^{-i\theta} + 5e^{-i3\theta} + e^{-i5\theta}$$

Collect up terms:

$$2^5 \cos^5\theta = (e^{i5\theta} + e^{-i5\theta}) + 5(e^{i3\theta} + e^{-i3\theta}) + 10(e^{i\theta} + e^{-i\theta})$$

Write with cosines:

$$2^5 \cos^5\theta = 2\cos 5\theta + 10\cos 3\theta + 20\cos\theta$$

So:

$$\cos^5 \theta = \frac{1}{16} \cos 5\theta + \frac{5}{16} \cos 3\theta + \frac{5}{8} \cos \theta$$

5)

$$\cos \theta \cos \phi = \frac{1}{2} (e^{i\theta} + e^{-i\theta}) \frac{1}{2} (e^{i\phi} + e^{-i\phi})$$

So:

$$\cos \theta \cos \phi = \frac{1}{4} (e^{i(\theta+\phi)} + e^{i(\theta-\phi)} + e^{i(-\theta+\phi)} + e^{i(-\theta-\phi)})$$

So:

$$\cos \theta \cos \phi = \frac{1}{4} (e^{i(\theta+\phi)} + e^{-i(\theta+\phi)}) + \frac{1}{4} (e^{i(\theta-\phi)} + e^{-i(\theta-\phi)})$$

So:

$$\cos \theta \cos \phi = \frac{1}{2} \cos(\theta + \phi) + \frac{1}{2} \cos(\theta - \phi)$$

Julia Sets

WE NEED DIAGRAMS

Example 1

Choose a complex number  $z_0$  and look at the sequence:

$$z_0 \quad z_1 \quad z_2 \quad z_3 \dots \text{ where } z_{n+1} = z_n^2$$

If we choose:

$$z_0 = 4 e^{i\pi/5}$$

We get:

$$4 e^{i\pi/5} \quad 16 e^{i2\pi/5} \quad 256 e^{i4\pi/5} \quad 65536 e^{i8\pi/5} \dots$$

If we choose:

$$z_0 = \frac{1}{3} e^{i\pi/5}$$

We get:

$$\frac{1}{3} e^{i\pi/5} \quad \frac{1}{9} e^{i2\pi/5} \quad \frac{1}{81} e^{i4\pi/5} \quad \frac{1}{6561} e^{i8\pi/5} \dots$$

If  $\text{mod}(z_0) > 1$  then  $\text{mod}(z_n)$  tends to infinity as  $n$  tends to infinity.

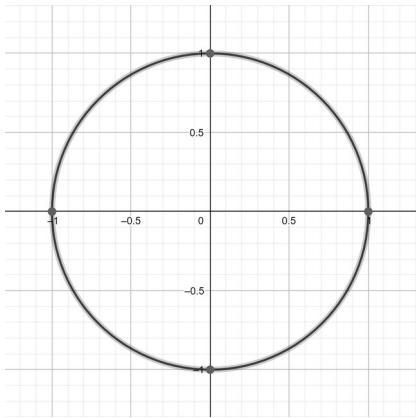
If  $\text{mod}(z_0) < 1$  then  $\text{mod}(z_n)$  does not tend to infinity as  $n$  tends to infinity.

We could colour the number plane.

$z_0$  is in the red region if  $\text{mod}(z_0) > 1$  and  $z_0$  is in the blue region if  $\text{mod}(z_0) < 1$

The Julia set is the boundary between the red region and the blue region.

A circle.



So far, so boring ...

Example 2

Choose a complex number  $z_0$  and look at the sequence:

$z_0 \quad z_1 \quad z_2 \quad z_3 \dots$  where  $z_{n+1} \rightarrow z_n^2 - 0.5 + 0.3i$

For some values of  $z_0$  we find  $\text{mod}(z_n)$  tends to infinity as  $n$  tends to infinity.

For other values of  $z_0$  we find  $\text{mod}(z_n)$  does not tend to infinity as  $n$  tends to infinity.

We could colour the number plane.

$z_0$  is in the red region if  $\text{mod}(z_n)$  tends to infinity as  $n$  tends to infinity.

$z_0$  is in the blue region if  $\text{mod}(z_n)$  does not tend to infinity as  $n$  tends to infinity.

The Julia set is the boundary between the red region and the blue region.

A slightly deformed circle.

## WE NEED A DIAGRAM

So far, so slightly interesting ...

In general:

Choose a complex number  $z_0$  and look at the sequence:

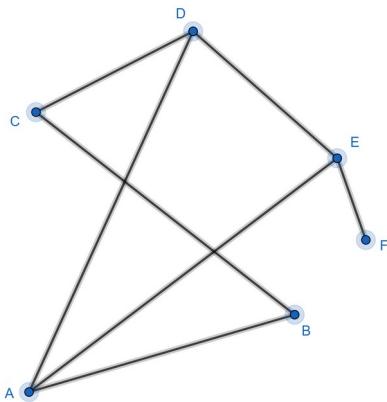
$z_0 \quad z_1 \quad z_2 \quad z_3 \dots$  where  $z_{n+1} \rightarrow z_n^2 + c$

Look at the Julia set for different values of  $c$ . The results are truly amazing.

## WE NEED DIAGRAMS

## Graphs

Here is a graph:



Note: this has nothing to do with graphs that have  $x$  and  $y$  axes.

We have points A, B, C, D, E, F (called vertices) connected by lines (called edges).

The degree of a vertex is the number of edges joined to that vertex.

vertex	A	B	C	D	E	F
degree	3	2	2	3	3	1

The sum of the degrees of the vertices is  $3+2+2+3+3+1=14$

The number of edges is 7

Look at the edge AD. It is counted once when we find the degree of A and counted once again when we find the degree of D. This is true of all the edges. So ...

The handshaking rule:

For any graph, the sum of the degrees of the vertices is twice the number of edges.

We say a vertex is even if its degree is even and a vertex is odd if its degree is odd.

When you add up some positive integers the total will be even if and only if there are an even number of odd integers. The sum of the degrees of the vertices is even. So from the handshaking rule we can deduce:

For any graph, there are an even number of odd vertices.

Why is it called the handshaking rule?

Imagine A, B, C, D, E, F are people who went to a party. During the party, some handshaking took place. We recorded this on the graph.

A and D shook hands so our graph has an edge joining A and D.

B and F did not shake hands so our graph does not have an edge joining B and F.

Vertex D has degree 3, so D shook hands with 3 people.

At the end of the party we ask everyone how many hands they shook. The replies  $(3, 2, 2, 3, 3, 1)$  add up to 14. Each act of handshaking has been counted twice. When A and D shake hands, this contributes to A's total and it contributes to D's total. So the sum of the replies must equal twice the number of handshakes.

## EXERCISE

Both these problems are about people at a party where handshaking took place.

- 1) Everyone shakes hands with 3 people. Why must there be an even number of people at the party?
- 2) Alice and Bill are at a party with 5 other people. Everyone shook hands with at least one other person. Only Alice and Bill shook hands with the same number of people. Why must Alice have shaken hands with an odd number of people?

## SOLUTIONS

1) The sum of the degrees of the vertices is even. If each vertex has degree 3 then there must be an even number of vertices.

2) There are 7 people at the party so everyone must have shaken hands with 1, 2, 3, 4, 5 or 6 people.  
Alice shakes hands with  $A$  people.

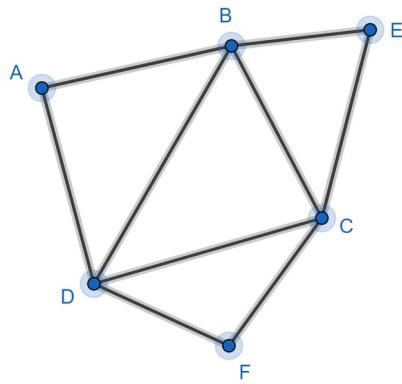
The other 6 people at the party each shook hands with a different number of people.

So the number of people they shook hands with must be 1, 2, 3, 4, 5 and 6

Now  $1+2+3+4+5+6+A$  must be even so  $A$  must be odd.

## Euler Tours

### Example 1

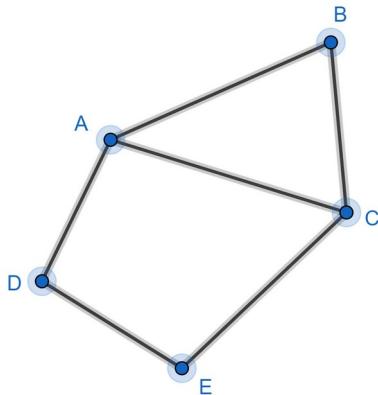


If you walk along the edges of this graph and visit the vertices in the order ABDCBEFCFDA then you have completed an Euler tour because you have walked along each edge once (and only once). This is a closed tour because the end vertex (A) is the same as the start vertex (A).

Any tour can be reversed. You could walk ADFCEBCDBA

A closed tour can start on any vertex. We can think of the above tour as starting on vertex F. You could walk: FDABDCBEFC

### Example 2

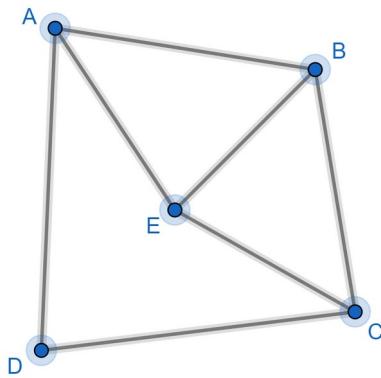


ABCEDAC is an open Euler tour because the end vertex (C) is not the same as the start vertex (A).

Any tour could be reversed. You could walk CADECBA

An open tour cannot start on any vertex.

### Example 3



Does this graph have a closed Euler tour?

Let's think about the start/end vertex of a tour:

If you start on vertex C, you can leave via one edge, return via another edge, leave again via the third edge but there is no edge left for your final return.

So you cannot start/end on vertex C (or vertex A, B or E)

The start/end vertex must be connected to an even number of edges.

Let's think about the vertices that are not at the start/end of a tour:

Each time you go to a vertex via an edge, you have to leave this vertex via a different edge.

So you need an even number of edges connected to this vertex.

For a closed Euler tour, you need an even number of edges connected to every vertex.

So in our example, there is no closed Euler tour.

Does this graph have an open Euler tour?

Let's think about the start/end vertex of a tour:

If you start on vertex C, you can leave via one edge, return via another edge, leave again via the third edge and you don't need to return to vertex C.

The start/end vertex must be connected to an odd number of edges.

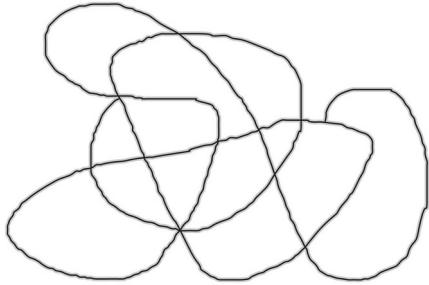
For an open Euler tour, you need an odd number of edges connected to the start and end vertices and an even number of edges connected to all the other vertices.

So in our example, there is no open Euler tour.

When you visit an art gallery, you want to walk along all the corridors, so you don't miss any of the paintings. It would be good if you could return to the entrance without having to walk along any corridor more than once. Think of the corridors as edges and where corridors meet as vertices. A good art gallery lay-out would have no odd vertices.

### Doodle Problem

Here is a doodle:



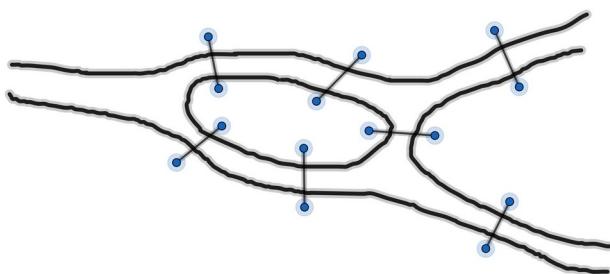
Can you draw this doodle without taking your pencil off the paper and without going over any part of the doodle more than once?

Put a vertex where lines meet and we have a graph. Drawing this doodle without taking your pencil off the paper and without going over any part of the doodle more than once is the same as finding an Euler tour. So we just need to count how many vertices are odd.

In this example there are 2 odd vertices, so you can draw this doodle by starting at one of the odd vertex and finishing at the other odd vertex.

### Konigsberg Bridges Problem

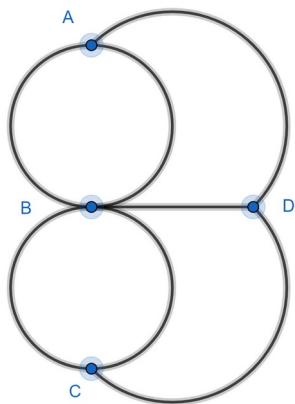
Here is a map of the city of Konigsberg (now known as Kaliningrad):



There is an island in the middle of a river. There are seven bridges connecting the island, the north bank, the south bank and the east area.

The story goes that citizens of Konigsberg wanted to go for a walk and cross each bridge once (and only once). Is this possible?

We can represent this map as a graph showing how the areas are connected by the bridges.



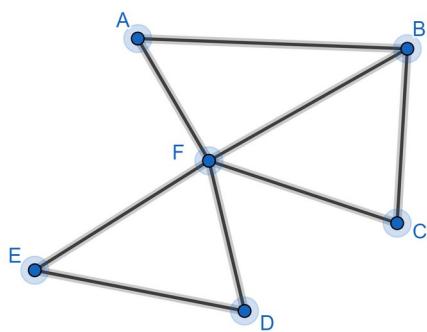
B is the island, A is the north bank, C is the south bank and D is the east area.

The citizens are trying to find an Euler tour. But this is not possible because there are 4 odd vertices.

It was Euler who first solved this problem, thereby starting a whole new branch of mathematics.

### Chinese Postman Problem

Here is a street map of a town (drawn to scale):



The postman starts at A, walks along every street delivering the mail, and then returns to A. The problem is to find the shortest route.

Think of the streets as edges and the street junctions as vertices and we have a graph.

If every vertex was even then the postman could take a closed Euler tour and walk along every edge once (and only once). But as some of the vertices are odd, the postman will have to walk along some edges twice.

B and F are the only odd vertices. The postman could start at B, walk along every edge once (and only once) and end at F. A possible route is BFCBAFEDF. The postman could then find the shortest route from F back to B. This is along edge FB.

We now have the closed non-Euler tour BFCBAFEDFB.

But the postman has to start and finish at A not at B. No problem. We can start a closed tour at any vertex. The tour AFEDFBFCBA will start and finish at A.

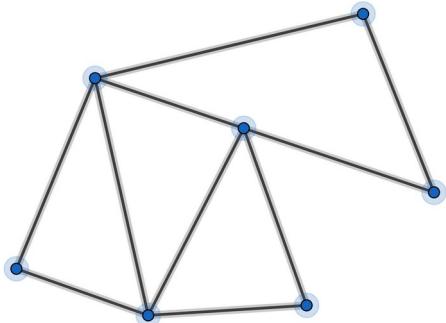
If there are more than 2 odd vertices then this problem is more difficult.

#### EXERCISE

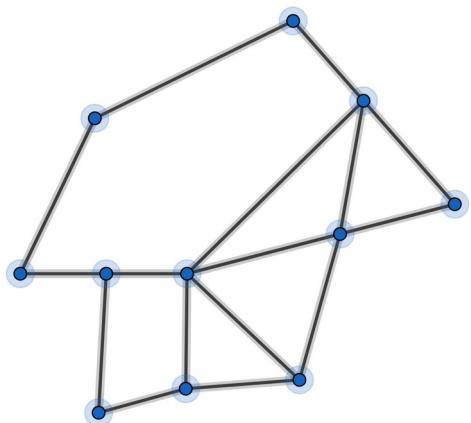
1)

Do these graphs have Euler tours? If so, are they open or closed?

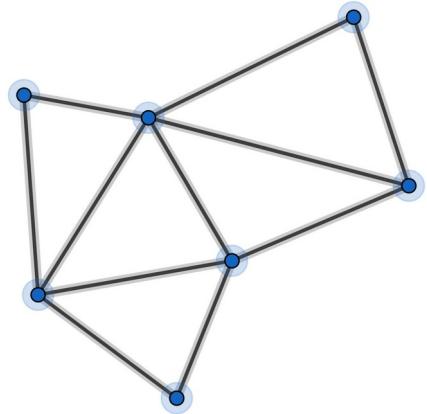
a)



b)



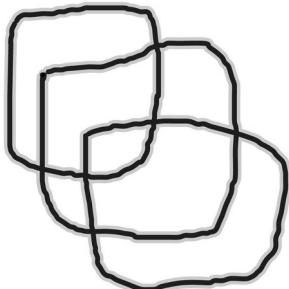
c)



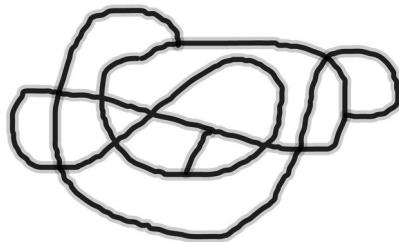
2)

Can you draw these doodles without taking your pencil off the paper and without going over any part of the doodle more than once?

a)



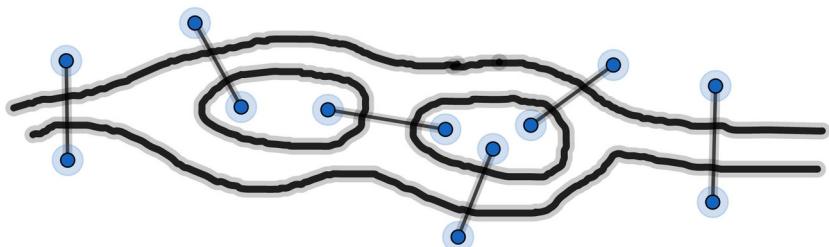
b)



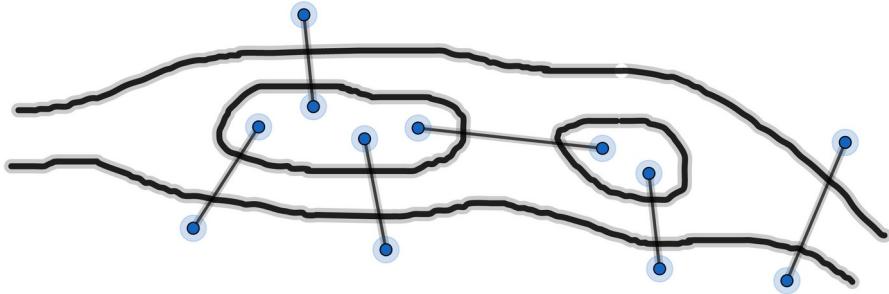
3)

Can you go for a walk and cross each bridge exactly once?

a)



b)

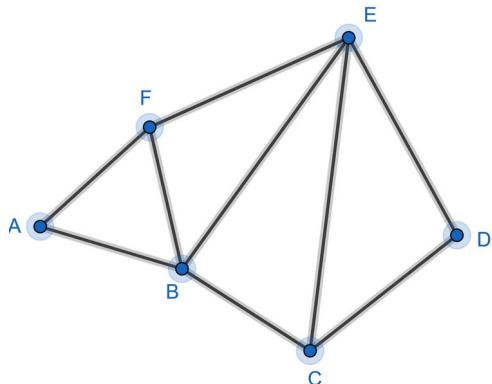


c) The mayor of Konigsberg wants to build another bridge so that she can go for a walk, starting from the north bank, crossing every bridge once (and only once) and ending on the island. Where should she build this new bridge?

4)

Here is a street map of a town (drawn to scale):

Find the shortest postman route starting and finishing at A.



## SOLUTIONS

1)

- a) No odd vertices. So there is a closed Euler tour.
- b) Four odd vertices. So there is no Euler tour.
- c) Two odd vertices. So there is an open Euler tour.

2)

- a) No odd vertices. Answer: Yes
- b) Four odd vertices. Answer: No

3)

- a) Two odd vertices. Answer: Yes
- b) No odd vertices: Answer: Yes
- c) The bridge must go between the south bank and the east area.

4)

F and C are odd vertices so let's find an open tour starting at F and ending at C

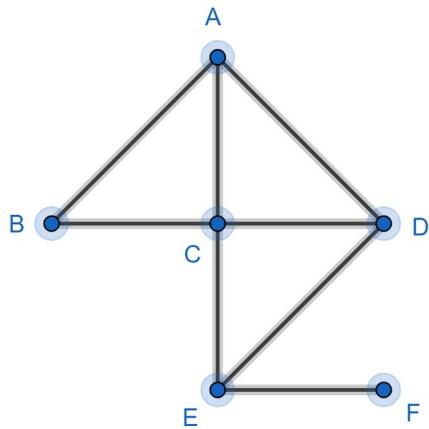
for example: FEDCEBAFBC

Now let's add on the shortest route from C back to F to get FEDCEBAFBCBF

Now let's start/end this tour at A to get AFBCBFEDCEBA

## Hamilton Tours

### Example 1



If you walk along the edges of this graph and visit the vertices in the order BADCEF then you have completed a Hamilton tour because you have visited every vertex once (and only once).

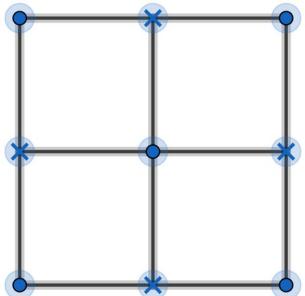
This is an open Hamilton tour because the end vertex (F) is not the same as the start vertex (B).

Unlike Euler tours, there are no simple rules to decide if Hamilton tours exists.

Sometimes you can find a Hamilton tour by trial and error. Sometimes you can prove a Hamilton tour does not exist. Sometimes you just don't know.

### Example 2

Look at the graph below where each vertex is marked with a cross or a dot:



I can find an open Hamilton tour by trial and error. Can you?

I can prove a closed Hamilton tour does not exist:

any Hamilton tour must visit a dot vertex then a cross vertex then a dot vertex then ...

so a closed Hamilton tour must have the same number of dot and cross vertices

but there are 5 dot vertices and 4 cross vertices

## Travelling Salesman Problem

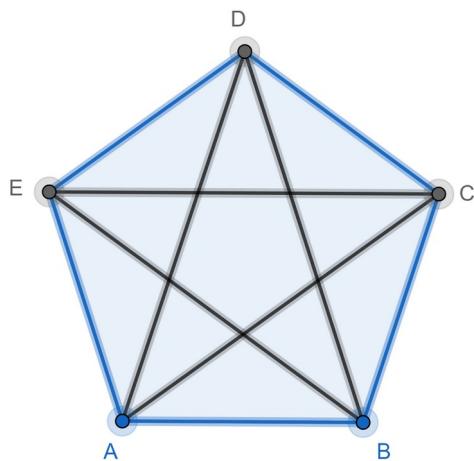
### Example 2

Here are the distances between five airports A, B, C, D, E:

	A	B	C	D	E
A	-	75	132	125	73
B	75	-	65	96	109
C	132	65	-	72	137
D	125	96	72	-	91
E	73	109	137	91	-

There are direct flights between all these airports.

Think of the flights as edges and the airports as vertices and we have a graph. (not drawn to scale)



The salesman starts at A, visits every airport once (and only once) and then returns to A. The problem is to find the shortest route. The salesman is looking for the shortest closed Hamilton tour.

The salesman could try the nearest neighbour algorithm:

start at A then fly to the nearest airport not already visited then fly to the nearest airport not already visited then ... then return to A

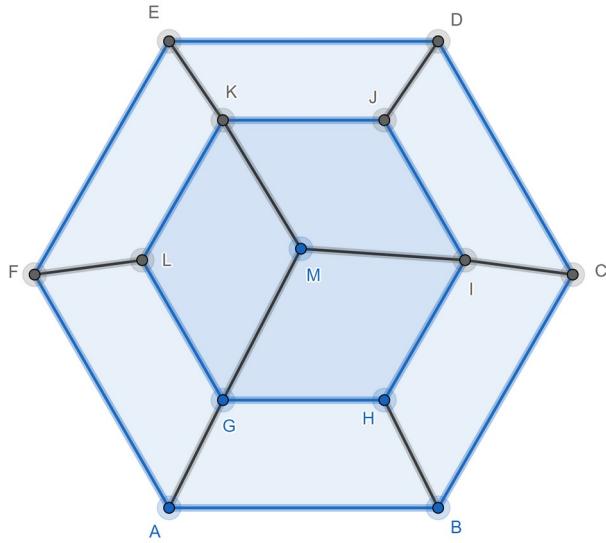
This gives the route: AEDCBA which has length 376

Unfortunately, this algorithm does not always find the shortest route.

So why don't I give you the algorithm that does always find the shortest route? Because no-one has found such an algorithm!

## EXERCISE

1) Does this graph have a Hamilton tour?



2) There are 4 flowers (A, B, C, D) in a field. A bee starts on flower A, visits each of the other flowers once (and only once) to collect pollen and returns to flower A. Use the nearest neighbour algorithm to find a route.

Here are the distances between the flowers:

	A	B	C	D
A	-	85	105	92
B	85	-	73	115
C	105	73	-	65
D	92	115	65	-

## SOLUTIONS

1) Here is an open tour: ABCDEFLGHJKM. I found it by trial and error.

We can prove there is no closed tour

Colour vertices A, C, E, L, H, J, M green. Colour vertices B, D, F, G, I, K pink.

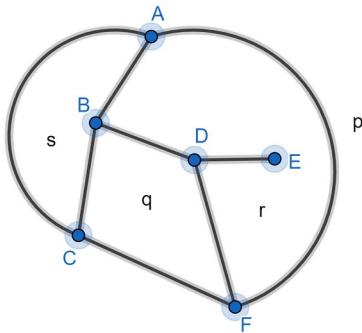
Any tour must alternate green, pink, green, pink, ...

A closed tour must have the same number of green and pink vertices but there are 7 green vertices and 6 pink vertices.

2) ABCDA

## Euler's Formula

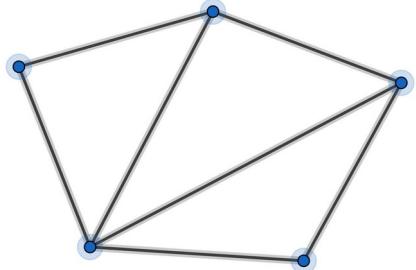
Here is a planar graph:



It is planar because no two edges cross-over each other.

The graph divides the plane into regions  $p, q, r, s$  (called faces).

## Euler's formula for planar graphs



For this planar graph:

the number of vertices is:  $V=5$

the number of edges is:  $E=7$

the number of faces is:  $F=4$  (remember to include the outer face)

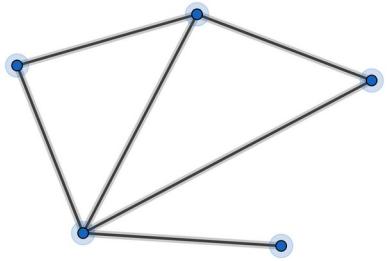
## Euler's formula:

For any planar graph  $F+V-E=2$

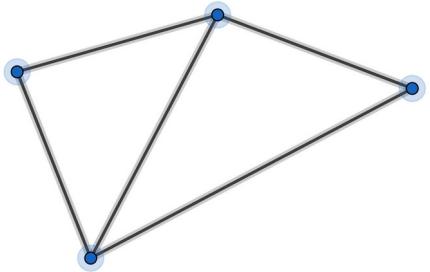
### Proof

Start with the graph above.

You can rub-out an edge so  $E \rightarrow E-1$  and  $F \rightarrow F-1$  and  $F+V-E$  stays unchanged.



You can rub-out an edge so  $E \rightarrow E - 1$  and  $V \rightarrow V - 1$  and  $F + V - E$  stays unchanged.



Once all the rubbing-out has been done, you will be left with:

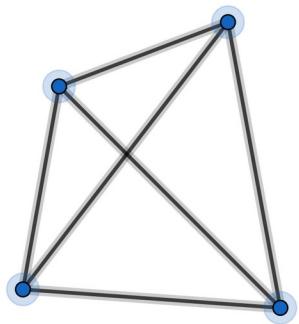
one face  $F = 1$  one vertex  $V = 1$  no edges  $E = 0$  and  $F + V - E = 2$

But all the rubbing-out leaves  $F + V - E$  unchanged.

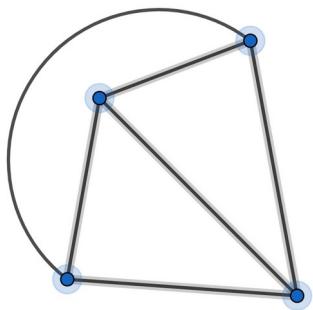
So  $F + V - E = 2$  for the original graph.

## EXAMPLE

We can redraw this graph:

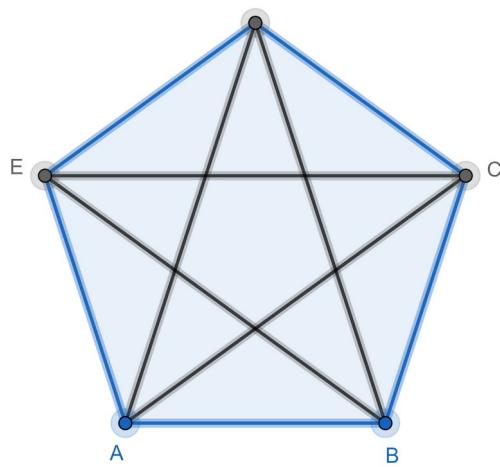


so that it is planar:



Theorem

We cannot redraw this graph so that it is planar:



Proof (by contradiction)

Assume we can redraw this graph so that it is planar.

$$V=5$$

Each vertex is joined to 4 edges.

So:

$$E=4 \times 5 \text{ No!}$$

Each edge is shared with 2 vertices.

So:

$$E=\frac{4 \times 5}{2}=10$$

So by Euler's formula  $F=7$

Each face has at least 3 edges.

So:

$$E \geq 3F \text{ No!}$$

Each edge is shared by 2 faces.

So:

$$E \geq \frac{3F}{2}$$

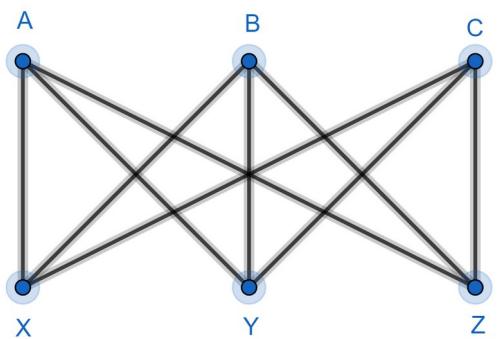
So:

$$10 \geq \frac{3 \times 7}{2}$$

Contradiction.

Theorem

We cannot redraw this graph so that it is planar:



Proof (by contradiction)

Assume we can redraw this graph so that it is planar.

$$V=6 \text{ and } E=9 \text{ so by Euler's formula } F=5$$

A face cannot have just 3 edges – try drawing one!

Each face has at least 4 edges.

So:

$$E \geq 4F \text{ No!}$$

Each edge is shared by 2 faces.

So:

$$E \geq \frac{4F}{2}$$

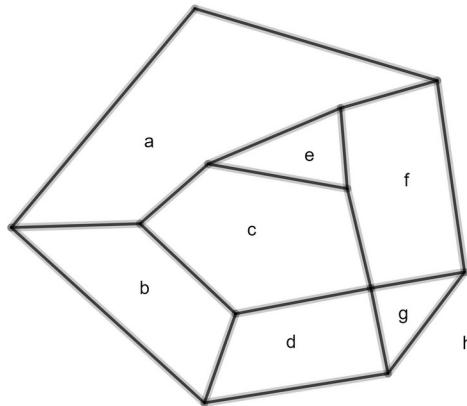
So:

$$9 \geq \frac{4 \times 5}{2} \text{ Contradiction.}$$

This is known as the utilities problem. Imagine A, B, C are houses and X, Y, Z are gas, water, electricity supply points. Each house needs to be connected, by pipe, to each utility. Can we do this without any pipes crossing over each-other? No!

## Map Colouring

Here is a map:



This map has 8 regions  $a, b, c, d, e, f, g, h$ . We want to colour the regions. Two regions that share a border like  $c$  and  $f$  must have different colours. Two regions that meet at a point like  $c$  and  $g$  can have the same colour. What is the minimum number of colours required?

Think of the regions as faces. Think of the borders as edges. Put a vertex where borders meet. We have a planar graph and we can use Euler's formula.

### Theorem

Every planar graph has a face with five (or fewer) edges.

Proof (by contradiction)

Assume there is a planar graph where every face has at least six edges.

Every face has at least six edges.

So:

$$E \geq 6F \text{ No!}$$

Each edge is shared by 2 faces.

So:

$$E \geq \frac{6F}{2} \text{ so } F \leq \frac{E}{3}$$

Every vertex has at least three edges.

So:

$$E \geq 3V \text{ No!}$$

Each edge is shared by two vertices.

So:

$$E \geq \frac{3V}{2} \text{ so } V \leq \frac{2E}{3}$$

So:

$$F+V-E \leq \frac{E}{3} + \frac{2E}{3} - E$$

So:

$$F+V-E \leq 0 \quad \text{But, by Euler's formula, } F+V-E=2$$

Contradiction

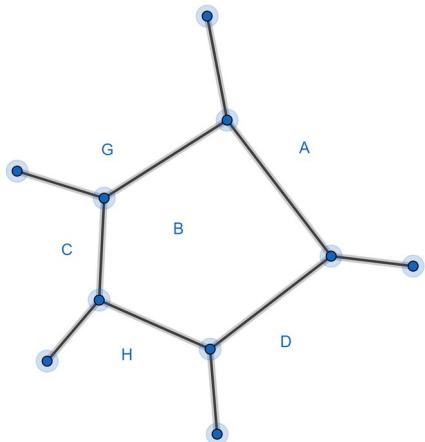
Six colour theorem

Every map can be coloured with at most six colours.

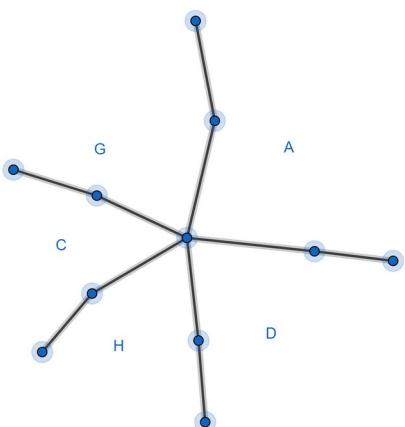
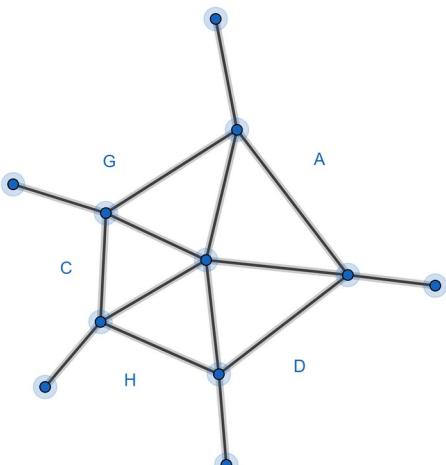
Proof

Say a map has 17 faces. We find a face with five (or fewer) edges.

The diagram below is just part of this map. Face B has five (or fewer) edges.



Remove this face in the following way:



We now have a map with 16 faces. If we can colour the 16 face map with just six colours then we can colour the 17 face map with just six colours because we will only use five colours for the faces A, D, H, C, G and this leaves a sixth colour for when we reinstate face B.

We can now repeat the process.

We start with the 16 face map. We find a face with five (or fewer) edges.

We remove this face ...

We start with the 15 face map ...

Eventually

We start with the 6 face map. We can colour this with six colours.

Then we go back and replace all the faces we have removed. Job done.

#### Four Colour Theorem

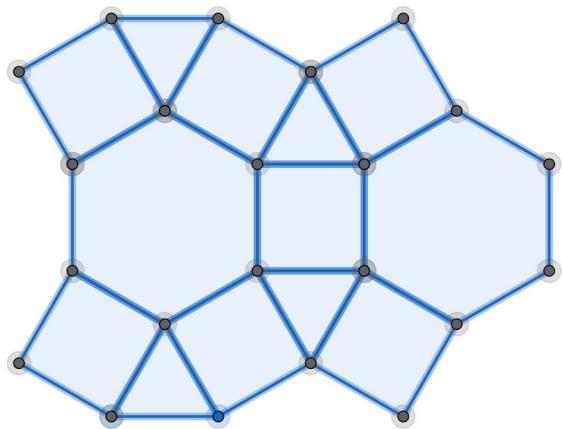
Every map can be coloured with at most four colours.

#### Proof

This was proved in 1976 by Appel and Haken. The proof is very difficult.

## Tessellations

Here is part of a tessellation:



It is a tiling of the plane, with no gaps. You have to imagine the tiling extends in all directions. If you walk (clockwise) around any vertex you will pass through a triangle then a square then a hexagon and then a square. We call this the  $3, 4, 6, 4$  tessellation.

The angles at a vertex must add-up to  $360^\circ$

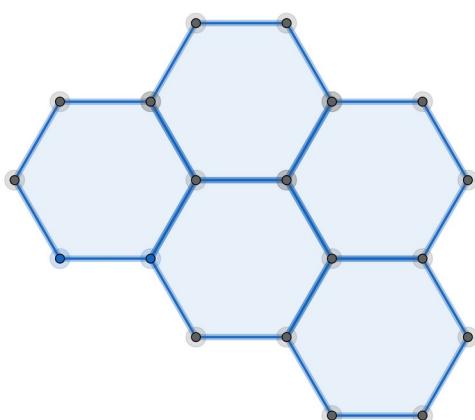
Here  $60^\circ + 90^\circ + 120^\circ + 90^\circ = 360^\circ$

In case you had forgotten, for regular polygons:

Number of sides	3	4	5	6	$n$
Internal angle	$60^\circ$	$90^\circ$	$108^\circ$	$120^\circ$	$180^\circ - \frac{360^\circ}{n}$

The regular tessellations:

Here is the  $6, 6, 6$  tessellation:



This is a regular tessellation because:

- All the faces are identical.
- All the faces are regular polygons.
- All the vertices are surrounded by the same number of faces.

Theorem

There are only 3 regular tessellations

See Exercise 1

The semi-regular tessellations:

Look at the above  $3,4,6,4$  tessellation:

This is a semi-regular tessellation because:

- All the triangles are identical.
- All the squares are identical.
- All the hexagons are identical.
- All the faces are regular polygons.
- All the vertices are surrounded by the same set of faces in the same order

Theorem

There are only 8 semi-regular tessellations

There are no semi-regular tessellations involving pentagons. Why not?

Remember, the angles at a vertex must add up to  $360^\circ$

see Exercise 2

## EXERCISE 1

Find the other 2 regular tessellations.

## EXERCISE 2

Find the other 7 semi-regular tessellations. This is not easy!

## SOLUTIONS 1

Hint: The angles at a vertex must add-up to  $360^\circ$

This gives us the following regular tessellations:

$4,4,4,4$  and  $3,3,3,3,3,3$

## SOLUTIONS 2

Hint: The angles at a vertex must add-up to  $360^\circ$

This gives us the following semi-regular tessellations:

6,3,6,3    4,8,8    3,3,4,3,4    3,3,3,4,4    3,3,3,3,6    3,12,12 and 6,4,12

## Polyhedrons

Here is a football:

WE NEED A PICTURE OF A FOOTBALL

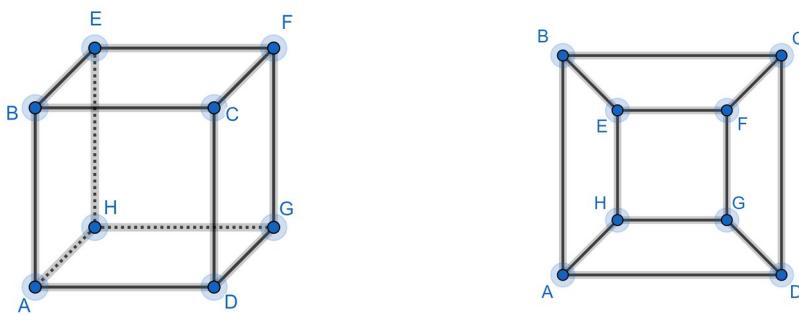
Flatten each face and we have a polyhedron.

WE NEED A DIAGRAM

Euler's Formula:

$F+V=E+2$  applies to any planar graph. It also applies to any polyhedron.

Here is a cube and we can represent it by a planar graph:



The cube has 8 vertices, the graph has 8 vertices. The cube has 12 edges, the graph has 12 edges.

The cube has 6 faces, the graph has 6 faces.

The face  $EFGH$  on the cube corresponds to the face  $EFGH$  on the planar graph. etc

The face  $ABCD$  on the cube corresponds to the outside face on the planar graph.

The cube and the planar graph have their vertices connected in the same way.

So the Euler formula must apply to the cube just as it applies to the planar graph.

Interior angles:

A cube has 6 faces. Each face has 4 interior angles. Each interior angle is  $90^\circ$

So the sum of all the interior angles of a cube is  $6 \times 4 \times 90^\circ = 2160^\circ$

Theorem

For any polyhedron

$$\sum (\text{interior angles}) = (V-2)360^\circ$$

Proof

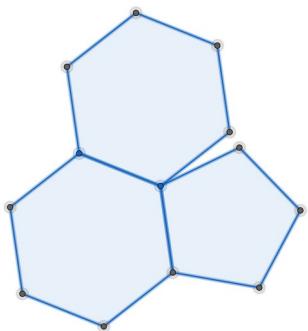
See footnote 1

Let's check this out for the cube:

$$V=8 \text{ so } (V-2)360^\circ = 2160^\circ \text{ as expected}$$

Gaps:

Look at the football polyhedron. At each vertex, a regular pentagon and two regular hexagons meet. If you put a regular pentagon and two regular hexagons together on a flat table then there is a gap:



Each interior angle of a regular pentagon is  $108^\circ$

Each interior angle of a regular hexagon is  $120^\circ$

So:

$$108^\circ + 120^\circ + 120^\circ + \text{gap} = 360^\circ$$

So:

$$\text{gap} = 12^\circ$$

Descartes' theorem

Take any polyhedron. Find the gap at each vertex. The sum of all these gaps will be  $720^\circ$

Proof

see footnote 2

Example 1

A polyhedron has 3 regular pentagons meeting at each vertex. How many vertices are there?

$$108^\circ + 108^\circ + 108^\circ + \text{gap} = 360^\circ \text{ so } \text{gap} = 36^\circ$$

Now:

$$\frac{720}{36} = 20 \text{ so this polyhedron has 20 vertices.}$$

Example 2

A polyhedron has 2 regular pentagons and a square meeting at each vertex. How many vertices are there?

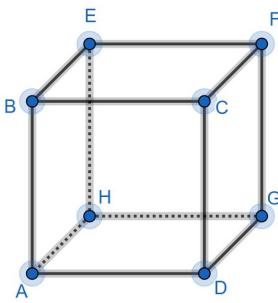
$$108^\circ + 108^\circ + 90^\circ + \text{gap} = 360^\circ \text{ so } \text{gap} = 54^\circ$$

Now:

$$\frac{720}{54} = 13.3 \text{ so this polyhedron does not exist.}$$

The regular polyhedrons.

Look at this cube:



This is a regular polyhedron because:

- All the faces are identical.
- All the faces are regular polygons.
- All the vertices are surrounded by the same number of faces.

### Theorem

There are only 5 regular polyhedrons

### Proof

Consider a regular polyhedron where each face has  $n$  sides and  $r$  faces meet at each vertex.

Note:

$n \geq 3$  and  $r \geq 3$  Can you see why?

If  $n=3$  and  $r=3$  then three triangles meet at each vertex.

$$60^\circ + 60^\circ + 60^\circ + \text{gap} = 360^\circ \text{ so } \text{gap} = 180^\circ \text{ and } \frac{720}{180} = 4 \text{ so we have 4 vertices}$$

If  $n=3$  and  $r=4$  then four triangles meet at each vertex.

$$60^\circ + 60^\circ + 60^\circ + 60^\circ + \text{gap} = 360^\circ \text{ so } \text{gap} = 120^\circ \text{ and } \frac{720}{120} = 6 \text{ so we have 6 vertices}$$

If  $n=3$  and  $r=5$  then five triangles meet at each vertex.

$$60^\circ + 60^\circ + 60^\circ + 60^\circ + 60^\circ + \text{gap} = 360^\circ \text{ so } \text{gap} = 60^\circ \text{ and } \frac{720}{60} = 12 \text{ so we have 12 vertices}$$

If  $n=4$  and  $r=3$  then three squares meet at each vertex.

$$90^\circ + 90^\circ + 90^\circ + \text{gap} = 360^\circ \text{ so } \text{gap} = 90^\circ \text{ and } \frac{720}{90} = 8 \text{ so we have 8 vertices}$$

If  $n=5$  and  $r=3$  then three pentagons meet at each vertex.

$$108^\circ + 108^\circ + 108^\circ + \text{gap} = 360^\circ \text{ so } \text{gap} = 36^\circ \text{ and } \frac{720}{36} = 20 \text{ so we have 20 vertices}$$

If  $n=3$  and  $r \geq 6$  or  $n=4$  and  $r \geq 4$  or  $n=5$  and  $r \geq 4$  or  $n \geq 6$  and  $r \geq 3$   
then you can easily check that the gaps are zero or negative and this is no good.

So there are only these 5 possibilities.

Example 3

Let's check out the  $n=5$  and  $r=3$  polygon.

We know  $V=20$  What about  $E$  and  $F$  ?

Three faces meet at each vertex, so 3 edges meet at each vertex.

So  $E=3V$  No!

Each edge is shared with 2 vertices.

$$\text{So } E = \frac{3V}{2} = 30$$

But  $F+V=E+2$  so  $F=12$

This polyhedron is called a dodecahedron.

see Exercise 1

The semi-regular polyhedrons.

Look at the football polyhedron:

This is semi-regular polyhedron because:

All the pentagons are identical

All the hexagons are identical.

All the faces are regular polygons.

All the vertices are surrounded by the same set of faces in the same order.

Theorem

There are only 13 semi-regular polyhedrons.

We will not prove this and we will not try to find them all.

But let's see if we can find some.

Example 4

Let's check out the football polyhedron.

One pentagon and two hexagons meet at each vertex.

$$\text{gap} = 12^\circ \text{ and } \frac{720}{12} = 60 \text{ So } V=60 \text{ What about } E \text{ and } F \ ?$$

Three faces meet at each vertex. So 3 edges meet at each vertex.

So  $E=3V$  No!

Each edge is shared with 2 vertices.

$$\text{So } E = \frac{3V}{2} = 90$$

But  $F+V=E+2$  So  $F=32$

We have 32 faces.  $P$  pentagons and  $H$  hexagons.

One pentagon meets at each vertex.

So  $P=V$  No!

Each pentagon joins five vertices.

$$\text{So } P = \frac{V}{5} = 12$$

Two hexagons meet at each vertex.

So  $H=2V$  No!

Each hexagon joins six vertices.

$$\text{So } H = \frac{2V}{6} = 20$$

Check:  $T+H=F$  Good!

## WARNING

We have been a bit sloppy.

SEE NOTES IN LEVER ARCH FILE

There are some polyhedrons, called prisms and anti-prisms, that seem to fit the description of a semi-regular polyhedron but are not included in the 13 semi-regular polyhedrons – check them out see Exercise 2

see Exercise 3

## EXERCISE 1

Check out the other 4 regular polyhedrons

## EXERCISE 2

- 1) Can you find a semi-regular polyhedron where one triangle and two hexagons meet at each vertex?
- 2) Can you find a semi-regular polyhedron where one square and two pentagons meet at each vertex? CHANGE THIS – SAME AS EXAMPLE 2

## EXERCISE 3

Use the pigeon-hole principle to show that you cannot have a polyhedron where every face has a different number of edges.

### SOLUTIONS 1

tetrahedron	$n=3$	$r=3$	$V=4$	$E=\frac{3V}{2}=6$	$F=4$
octahedron	$n=3$	$r=4$	$V=6$	$E=\frac{4V}{2}=12$	$F=8$
icosahedron	$n=3$	$r=5$	$V=12$	$E=\frac{5V}{2}=30$	$F=20$
cube	$n=4$	$r=3$	$V=8$	$E=\frac{3V}{2}=12$	$F=6$

### SOLUTIONS 2

1)  $gap=60^\circ$  and  $\frac{720}{60}=12$  So  $V=12$

Three faces meet at each vertex. So 3 edges meet at each vertex. So  $E=3V$  No!

Each edge is shared with two vertices. So  $E=\frac{3V}{2}=18$

But  $F+V=E+2$  So  $F=8$

We have 8 faces.  $T$  triangles and  $H$  hexagons.

One triangle meets at each vertex. So  $T=V$  No!

Each triangle joins three vertices. So  $T=\frac{V}{3}=4$

Two hexagons meet at each vertex. So  $H=2V$  No!

Each hexagon joins six vertices. So  $H=\frac{2V}{6}=4$

Check:  $T+H=F$  Good!

2)  $gap=54^\circ$  and  $\frac{720}{54}=13.33$  So this is no good! CHANGE THIS – SAME AS EXAMPLE 2

### SOLUTIONS 3

A polyhedron has 10 faces.

I have 7 boxes, labelled 3, 4, 5, 6, 7, 8, 9. I put each face in a box.

If a face has 7 edges then I put it in the box with 7 on the label. etc

There are 7 boxes and 10 faces. One (or more) box must contain two (or more) faces.

So two (or more) faces have the same number of edges.

note: each face has at least 3 edges

note: there are only 10 faces so a face cannot have 10 or more edges because each edge is connected to another face.

This proof will work however many faces the polyhedron has.

### Footnote 1

Interior angles rule

Let's find the sum of all the interior angles of any polyhedron.

The first face of our polyhedron has  $n_1$  sides.

The interior angles of this face add up to  $n_1(180^\circ) - 360^\circ$  (remember?)

The second face of our polyhedron has  $n_2$  sides.

The interior angles of this face add up to  $n_2(180^\circ) - 360^\circ$

etc

There are  $F$  faces

So:

$$\sum (\text{interior angles}) = (n_1 + n_2 + n_3 + \dots + n_F)180^\circ - F(360^\circ)$$

Now:

$$E = n_1 + n_2 + n_3 + \dots + n_F \text{ No!}$$

Each edge is shared with two faces.

So:

$$E = \frac{1}{2}(n_1 + n_2 + n_3 + \dots + n_F) \text{ So } n_1 + n_2 + n_3 + \dots + n_F = 2E$$

So:

$$\sum (\text{interior angles}) = 2E(180^\circ) - F(360^\circ) = (E - F)360^\circ$$

Now:

$$F + V = E + 2 \text{ so } E - F = V - 2$$

So:

$$\sum (\text{interior angles}) = (V - 2)360^\circ$$

### Footnote 2

To find  $\sum (\text{interior angles})$  we looked at the faces of our polyhedron.

We looked at the faces of a cube and said:

A cube has 6 faces. Each face has 4 interior angles. Each interior angle is  $90^\circ$

So the sum of all the interior angles of a cube is  $6 \times 4 \times 90^\circ = 2160^\circ$

In general, we proved:

$$\sum (\text{interior angles}) = (V - 2)360^\circ$$

by finding the sum of the interior angles of each face and then adding these up.

An alternative approach

We will look at the vertices of our polyhedron.

We look at the vertices of a cube and say:

A cube has 8 vertices. Each vertex is surrounded by 3 interior angles. Each interior angle is  $90^\circ$

So the sum of all the interior angles of a cube is  $8 \times 3 \times 90^\circ = 2160^\circ$

We will use this approach to prove Descartes' theorem.

At each vertex:

$$\text{interior angles} + \text{gap} = 360^\circ$$

So if we visit each vertex and add up all these angles:

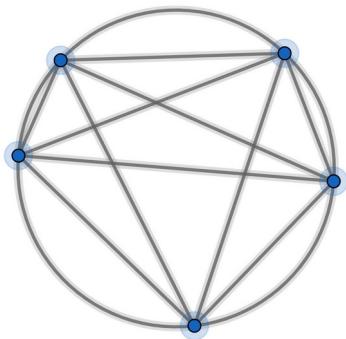
$$\sum(\text{interior angles}) + \sum(\text{gap}) = \sum 360^\circ$$

Now:

$$\sum(\text{interior angles}) = (V - 2)360^\circ \quad \text{and} \quad \sum 360^\circ = (V)360^\circ \quad \text{so} \quad \sum(\text{gap}) = 720^\circ$$

## Points and Regions

We put 5 points on a circle and join these points with straight lines:



This divides the circle into a maximum of 16 regions (count them)

Note: to get the maximum number of regions, we must not allow three or more lines to cross at the same point.

If you draw diagrams and count the regions then you will find:

number of points on a circle	1	2	3	4	5
maximum number of regions	1	2	4	8	16

Instead of drawing diagrams and counting the regions, let's calculate.

What is the maximum number of regions with 5 points on a circle?

Think of the lines as edges and the regions as faces and put a vertex wherever two lines or a line and the circle intersect and we have a planar graph.

As we are not counting the region on the outside, Euler's formula becomes  $F+V=E+1$

Let's calculate the number of vertices:

(a) There are 5 points on the circle. That's 5 vertices.

(b) For every choice of 4 points on the circle, you can draw two lines that intersect.

There are  $(5C4)=5$  ways to choose 4 points on the circle so there are 5 lines that intersect giving us another 5 vertices.

So  $V=5+5=10$

Let's calculate the number of edges:

(a) There are 5 points on the circle. Each of these points is attached to 6 edges.

That's  $(5 \times 6) = 30$  edges. No!

Each edge is shared with two points.

So that's  $\frac{30}{2} = 15$  edges.

(b) There are  $(5C4)$  points where two lines intersect. Each of these points is attached to 4 edges.

That's  $(5C4) \times 4 = 20$  edges. No!

Each edge is shared with two points.

So that's  $\frac{20}{2} = 10$  edges.

$$\text{So } E = 15 + 10 = 25$$

Let's calculate the number of faces:

$$F + V - E = 1 \text{ so } F = 16 \text{ as expected.}$$

Repeat this calculation for 6 points on the perimeter. You should find there are 31 regions.

(surprised?)

Repeat this calculation for  $n$  points on the perimeter.

Let's calculate the number of vertices:

$$V = n + (nC4)$$

Let's calculate the number of edges:

$$E = \frac{n(n+1) + 4(nC4)}{2}$$

Let's calculate the number of faces:

$$F = \frac{n(n+1) + 4(nC4)}{2} + 1 - (n + (nC4))$$

You can simplify this to:  $F = 1 + (nC2) + (nC4)$

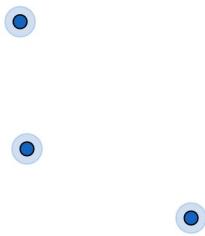
Or if you prefer:  $F = \frac{1}{24}(n^4 - 6n^3 + 23n^2 - 18n + 24)$

## Sprouts

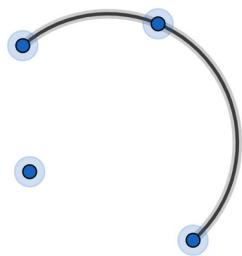
A game for two players

Start with three dots on a piece of paper. Players take turns to draw a line starting on a dot and ending on the same or a different dot and then putting another dot on this line. A line must not cross another line. A dot cannot be attached to more than three lines. The first player who cannot go is the loser.

position at start



possible position after one turn



Can you think of a good strategy to play this game? (I can't)

Note: each dot can attach to three lines and each turn uses up two attachments and creates one new attachment so the game must eventually end.

Note: you can vary the number of dots at the start.

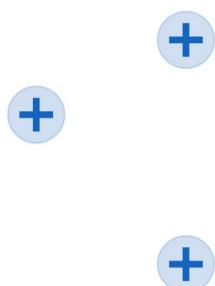
Note: think of the dots as vertices and the lines as edges and then every position is a planar graph.

## Brussel sprouts

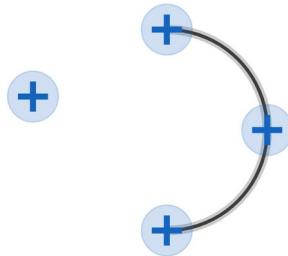
A game for two players

Start with three crosses on a piece of paper. Players take turns to draw a line starting on an arm of a cross and ending on an arm of the same or a different cross and then putting another cross on this line. A line must not cross another line. The first player who cannot go is the loser.

position at start



possible position after one turn



Note: each cross can attach to four lines and each turn uses up two attachments and creates two new attachments so it is not obvious if the game will ever end.

Note: you can vary the number of crosses at the start.

Note: think of the crosses as vertices and the lines as edges and then every position is a planar graph.

Brussel Sprouts is a con. If you start with three crosses then the game will always end after 13 turns. So the first player will always win.

Play a game and look at the final diagram. We start with 3 crosses, that's 12 attachments. At the end of the game each attachment is in a separate face, so  $F=12$

If the game ends after  $n$  turns:

Each turn adds one vertex.

So:

$$V=3+n$$

Each turn adds 2 edges.

So:

$$E=2n$$

Euler's formula says:

$$F+V=E+2$$

So:

$$12+(3+n)=2n+2$$

So:

$$n=13$$

In general:

if we start with  $c$  crosses, that's  $4c$  attachments.

If the game ends after  $n$  turns:

Then:

$$F=4c \quad V=c+n \quad E=2n$$

Euler's formula says:

$$F+V=E+2$$

So:

$$4c+(3c+n)=2n+2$$

So:

$$n=5c-2$$

## Topology

In geometry we study rigid objects and we are concerned with lengths, areas, volumes, angles, etc  
This is not the case in topology.

### Example 1

When you are planning how to travel between two stations on the London underground, you need to know the order of the stations along the lines and where the lines connect. You don't need to know anything about lengths or angles. The London underground map is topological.

### Example 2

In the chapter: Polyhedrons, we proved there are only 5 regular polyhedrons.

The proof relied on all the faces being regular polygons. This means that every edge has the same length and every interior angle is the same. We were doing geometry.

Here is another proof:

Consider a polyhedron where each face has  $n$  sides and  $r$  faces meet at each vertex.

Note:

If  $r$  faces meet at each vertex then  $r$  edges meet at each vertex.

Note:

$$n \geq 3 \text{ and } r \geq 3$$

There are  $F$  faces and each face has  $n$  edges.

So:  $E = Fn$  No!

Each edge is shared by 2 faces.

$$\text{So } E = \frac{Fn}{2}$$

There are  $V$  vertices and each vertex is joined to  $r$  edges.

So  $E = Vr$  No!

Each edge is shared by 2 vertices.

$$\text{So } E = \frac{Vr}{2}$$

$$\text{Now } E = \frac{Fn}{2} \text{ and } E = \frac{Vr}{2} \text{ so } \frac{Fn}{2} = \frac{Vr}{2} \text{ so } V = \frac{Fn}{r}$$

$$\text{Now } F + V = E + 2$$

$$\text{So } F + \frac{Fn}{r} = \frac{Fn}{2} + 2$$

$$\text{So } 2rF + 2Fn = Fn(r + 4)$$

$$\text{So } F(2n - nr + 2r) = 4r$$

$$\text{So } 2n - nr + 2r > 0$$

So  $2n+2r > nr$

Together with  $n \geq 3$  and  $r \geq 3$  we get just five possible  $n$  and  $r$  values:

$n$	$r$	$2n+2r$	$nr$
3	3	12	9
3	4	14	12
3	5	16	15
4	3	14	12
5	3	16	15

In this proof we have not talked about regular polygons. The proof works even if the edges have different lengths and the interior angles are not the same. The edges don't even have to be straight. We have only assumed that all the faces have the same number of edges and all the vertices are connected to the same number of edges. So our result is more general. It is really a topological not a geometrical result.

Example 3

Can we find any polyhedrons whose faces are pentagons and hexagons with three faces meeting at each vertex?

If there are  $P$  pentagons and  $H$  hexagons then:

$$F = P + H$$

Each pentagon has 5 edges and each hexagon has 6 edges.

So  $E = 5P + 6H$  No!

Each edge is shared with 2 faces.

$$\text{So } E = \frac{1}{2}(5P + 6H)$$

Three faces meet at each vertex so 3 edges meet at each vertex.

So  $E = 3V$  No!

Each edge is shared with 2 vertices.

$$\text{So } E = \frac{3V}{2}$$

$$\text{So } V = \frac{1}{3}(5P + 6H)$$

Now  $F + V = E + 2$

So  $P = 12$

## Group Theory

### a) Groups

We can combine two numbers, using addition, to get another number:

$$5+7=12$$

We can combine two sets, using union, to get another set:

$$(a,b,e,g)\cup(a,c,e,h,k)=(a,b,c,e,g,h,k)$$

etc

A binary operation \* combines two “things” to get another “thing”.

A binary operation \* is commutative if  $p*q$  is always the same as  $q*p$

For example, if we are combining numbers:

addition is commutative	$4+8=8+4$
subtraction is not commutative	$10-3 \neq 3-10$
multiplication is commutative	$3\times 5 = 5\times 3$
division is not commutative	$24\div 6 \neq 6\div 24$

A binary operation \* is associative if  $p*(q*r)$  is always the same as  $(p*q)*r$

For example, if we are combining numbers:

addition is associative	$4+(3+8)=(4+3)+8$
subtraction is not associative	$20-(12-8) \neq (20-12)-8$
multiplication is associative	$3\times(4\times 5) = (3\times 4)\times 5$
division is not associative	$24\div(6\div 2) \neq (24\div 6)\div 2$

### Example 1

Set  $\{1,2,3,4,5,6\}$

Binary operation \* where  $p*q=pq \bmod 7$

For example:

$$5*6=5\times 6=30=2 \bmod 7$$

Here is the combination table:

*	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3

5	5	3	1	6	4	2
6	6	5	4	3	2	1

Note:  $5*6$  appears in the 5 row and the 6 column etc

Note: the binary operation \* is commutative because  $5*6=6*5$  etc

(a) The set is closed under the binary operation. This means:

For all  $p$  and  $q$  in the set  $p*q$  is in the set.

So all the numbers in the combination table are in the set.

(b) The set contains an identity element  $e$  This means:

For all  $p$  in the set  $p*e=p$  and  $e*p=p$

Here the identity element is 1

$$\begin{array}{ccccccc} 1*1=1 & 2*1=2 & 3*1=3 & 4*1=4 & 5*1=5 & 6*1=6 \\ 1*1=1 & 1*2=2 & 1*3=3 & 1*4=4 & 1*5=5 & 1*6=6 \end{array}$$

(c) Every element in the set has an inverse element in the set. This means:

For all  $p$  in the set there is an element  $p'$  in the set where  $p*p'=e$  and  $p'*p=e$

1 is it's own inverse  $1*1=1$

2 and 4 are inverses  $2*4=1$  and  $4*2=1$

3 and 5 are inverses  $3*5=1$  and  $5*3=1$

6 is it's own inverse  $6*6=1$

(d) The binary operation is associative.

You can check this for the above combination table.

Rules for a group:

A set of elements and a binary operation \* is a group if:

The set is closed under \*

The set contains an identity element

Every element in the set has an inverse element in the set

\* is associative

So the set  $\{1, 2, 3, 4, 5, 6\}$  with the binary operation \* where  $p*q=pq \bmod 7$  is a group.

See Exercise

## EXERCISE

1) Set  $\{0,1,2,3\}$

Binary operation \* where  $p*q = p+q \text{ mod } 4$

Complete the combination table and show we have a group.

2) We have these functions:  $e(x)=x$      $f(x)=\frac{1}{x}$      $g(x)=-x$      $h(x)=-\frac{1}{x}$

Set  $\{e, f, g, h\}$

Binary operation \* where  $f(x)*g(x)=f(g(x))$

Complete the combination table and show we have a group.

## SOLUTIONS

1)

*	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Closed: all the numbers in the combination table are in the set.

Identity: 0

Inverses: 0 is its own inverse              1 and 3 are inverses              2 is its own inverse

Associative: you can check this for the above combination table.

2)

*	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

Closed: all the functions in the combination table are in the set.

Identity: e

Inverses: every function is its own inverse

Associative: you can check this for the above combination table.

## Group Theorems

We have a group:

Set  $\{e, a, b, c, d, f, g, \dots\}$  where  $e$  is the identity element

Binary operation \*

If we can prove a theorem, just using the rules for a group, then this theorem applies to all groups.

### 1. Cancellation theorem part 1

If  $a*d = a*p$  then  $d = p$

Proof

$$a*d = a*p$$

$$a'*(a*d) = a'*(a*p)$$

$$(a'*a)*d = (a'*a)*p$$

$$e*d = e*p$$

$$d = p$$

### 2. Cancellation theorem part 2

If  $d*a = p*a$  then  $d = p$

Can you prove this?

Note: if  $a*d = p*a$  then we can't cancel to get  $d = p$

### 3. Latin square theorem

Every group combination table is a Latin square.

(every element appears exactly once in each row and each column of the combination table)

Proof: (by contradiction) part 1

Assume  $c$  appears twice in the  $a$  row of the combination table.

Say  $a*b=c$  and  $a*f=c$  where  $b$  and  $f$  are different elements.

So  $a*b=a*f$  so  $b=f$  by the cancellation theorem. Contradiction.

Proof: (by contradiction) part 2

Assume  $c$  appears twice in the  $a$  column of the combination table.

Say  $b*a=c$  and  $f*a=c$  where  $b$  and  $f$  are different elements

So  $b*a=f*a$  so  $b=f$  by the cancellation theorem. Contradiction.

Note: not every Latin square is a group combination table.

This Latin square is not a group combination table. There is no identity.

*	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

#### 4. Equation solving theorem part 1

If  $p*x = q$  then  $x = p'^*q$

Proof

$$p*x = q$$

$$p'^*(p*x) = p'^*q$$

$$(p'^*p)*x = p'^*q$$

$$e*x = p'^*q$$

$$x = p'^*q$$

#### 5. Equation solving theorem part 2

If  $x*p = q$  then  $x = q*p'$

Can you prove this?

#### 6. If $a*p = a$ then $p = e$

Proof

$$a*p = a$$

$$a'^*(a*p) = a'^*a$$

$$(a'^*a)*p = e$$

$$e*p = e$$

$$p = e$$

#### 7. If $a*p = e$ then $p = a'$

Can you prove this?

#### 8. Inverse theorem

the inverse of  $p*q$  is  $q'^*p'$

recall: if  $a$  and  $a'$  are inverses then  $a*a' = e$  and  $a'*a = e$

So we need to prove  $(p*q)*(q'^*p') = e$  and  $(q'^*p')*(p*q) = e$

Proof part 1

$$(p*q)*(q'*p') = p*(q*q')*p' = p*(e)*p' = (p*p)*p' = p*p' = e$$

Proof part 2

$$(q'*p')*(p*q) = \dots = e$$

9. There is only one group with 3 elements

Proof

Set  $\{e, a, b\}$

Let's start filling in the combination table.

*	e	a	b
e	e	a	b
a	a		
b	b		

There is only one way we can complete the table as a Latin square (try it)

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

We can check that this is a group (being a Latin square is necessary but not sufficient)

Closed: all the elements in the combination table are in the set.

Identity:  $e$

Inverses:  $e$  is its own inverse       $a$  and  $b$  are inverses

Associative: you can check this for the above combination table.

Example

Set  $\{0, 1, 2\}$

Binary operation \*  $a*b=a+b, \text{mod } 3$

*	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

We can match up these elements with the elements  $\{e, a, b\}$

$0 \leftrightarrow e$

$1 \leftrightarrow a$

$2 \leftrightarrow b$

and the two group tables will be the same.

10. There are only two groups with 4 elements

Proof

Set  $\{e, a, b, c\}$

Let's start filling in the combination table.

*	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

There are only four ways we can complete the table as a Latin square (try it)

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

*	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

*	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

Look at the second table and make the following changes:

change every  $a$  to  $b$  change every  $b$  to  $c$  change every  $c$  to  $a$

then rewrite the table so that the rows and columns are in the order  $e, a, b, c$

You then get the third table.

Look at the second table and make the following changes:

change every  $a$  to  $c$  change every  $b$  to  $a$  change every  $c$  to  $b$

then rewrite the table so that the rows and columns are in the order  $e, a, b, c$

You then get the fourth table.

So the second, third and fourth tables are really the same. So there are only two different ways we can complete the table as a Latin square and we can check that both are groups.

It can be shown that:

Number of elements	1	2	3	4	5	6	7	8	9	10	...
Number of groups	1	1	1	2	1	2	1	5	2	2	...

## 11. Symmetry theorem

The symmetries of any object form a group.

See chapters, Symmetries of a Rectangle, Symmetries of a Triangle

## 12. Lagrange's theorem

The set  $\{e, a, b, c\}$  with the binary operation \* has four members. It is a group.

Lagrange's theorem says:

If you take any member of the set, say  $b$  then  $b*b*b*b=e$

In general:

The set  $\{e, a, b, c\}$  with the binary operation \* has  $n$  members. It is a group.

Lagrange's theorem says:

If you take any member of the set, say  $b$  then  $b*b*b*b*...*b=e$

Proof – too difficult

### Example

The set  $\{1, 2, 3, 4, 5, 6\}$  with the binary operation \* where  $p*q=pq \text{ mod } 7$  has six members. It is a group.

Lagrange's theorem says:

If you take any member of the set, say 5 then:

$$5*5*5*5*5=1$$

But:

$$5*5*5*5*5=5^6, \text{mod} 7$$

So Lagrange's theorem says:

$$5^6=1, \text{mod} 7$$

Also:

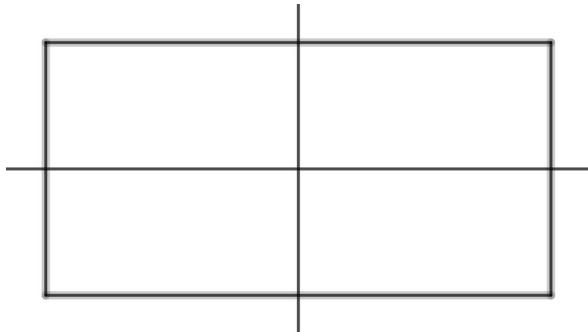
$$1^6=1, \text{mod} 7 \quad 2^6=1, \text{mod} 7 \quad 3^6=1, \text{mod} 7 \quad 4^6=1, \text{mod} 7 \quad 6^6=1, \text{mod} 7$$

But this is Fermat's little theorem.

So Fermat's little theorem can now be seen as a special case of a more general theorem.

## Symmetries of a Rectangle

If you take a rectangle and rotate it  $180^\circ$  about the centre then it looks exactly the same as it did before. We say the rectangle has rotation symmetry.



The symmetries of the rectangle are:

- $e$  do nothing
- $a$  rotate  $180^\circ$  about the centre
- $b$  rotate  $180^\circ$  about the  $x$  axis
- $c$  rotate  $180^\circ$  about the  $y$  axis

We can combine symmetries.

$a*b$  means you do  $b$  and then you do  $a$ . This means you do  $b$  first.

Take a piece of card, in the shape of a rectangle.

If you do  $b$  and then do  $a$  it will end up in the same position as if you had just done  $c$

Try it.

So  $a*b$  is the same as  $c$ . So  $a*b=c$

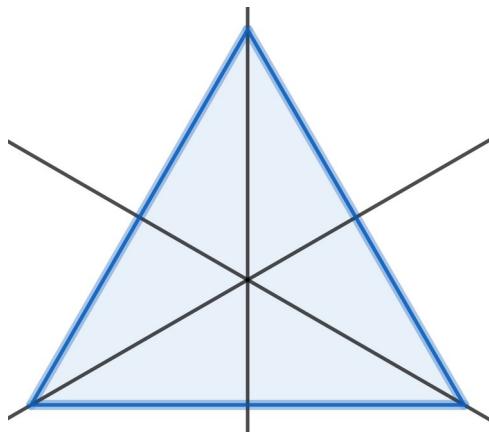
Here is the combination table. You should check some of these.

*	$e$	$a$	$b$	$c$
$e$	$e$	$a$	$b$	$c$
$a$	$a$	$e$	$c$	$b$
$b$	$b$	$c$	$e$	$a$
$c$	$c$	$b$	$a$	$e$

Note:  $a*b$  goes in the  $a$  row and the  $b$  column.

The set  $\{e, a, b, c\}$  with the binary operation  $*$  forms a group.

## Symmetries of a Triangle



The symmetries of the equilateral triangle are:

- $e$  do nothing
- $a$  rotate  $120^\circ$  about the centre (anticlockwise)
- $b$  rotate  $240^\circ$  about the centre (anticlockwise)
- $p$  rotate  $180^\circ$  about the line through the bottom left-hand corner
- $q$  rotate  $180^\circ$  about the line through the bottom right-hand corner
- $r$  rotate  $180^\circ$  about the line through the top corner

We can combine symmetries.

$a*p$  means you do  $p$  and then you do  $a$ . This means you do  $p$  first.

Take a piece of card, in the shape of an equilateral triangle.

If you do  $p$  and then do  $a$  it will end up in the same position as if you had just done  $r$

Try it.

So  $a*p$  is the same as  $r$ . So  $a*p=r$

Show that  $p*a=q$ . So  $a*p$  and  $p*a$  are not the same.

\* is not commutative.

Here is the combination table. You should check some of these.

*	e	p	q	r	a	b
e	e	p	q	r	a	b
p	p	e	a	b	q	r
q	q	b	e	a	r	p
r	r	a	b	e	p	q
a	a	r	p	q	b	e
b	b	q	r	p	e	a

Note  $a*p$  goes in the  $a$  row and the  $p$  column.

And  $p*a$  goes in the  $p$  row and the  $a$  column.

The set  $\{e, p, q, r, a, b\}$  with the binary operation \* forms a group.

## Rearrangements

I have three ornaments in a line on my mantelpiece.

Let's call the left hand end of the mantelpiece, position 1. The middle, position 2 and the right hand end of the mantelpiece, position 3

Occasionally I decide to rearrange these ornaments. This means that I put them in a different order on the mantelpiece. The possible rearrangements are:

$P_1$  Don't do anything

$P_2$  Swap over the ornaments in positions 2 and 3

$P_3$  Swap over the ornaments in positions 1 and 3

$P_4$  Swap over the ornaments in positions 1 and 2

$P_5$  Move each ornament one position to the left. The ornament that started in position 1 falls off the mantelpiece and is then put in position 3

$P_6$  Move each ornament one position to the right. The ornament that started in position 3 falls off the mantelpiece and is then put in position 1

Let's call the ornaments  $A$  and  $B$  and  $C$

If the ornaments start in the order  $A, B, C$  and I do  $P_5$  they will end up in the order  $B, C, A$

If the ornaments start in the order  $C, B, A$  and I do  $P_5$  they will end up in the order  $B, A, C$  etc

We can combine rearrangements.

$P_4 * P_2$  means you do  $P_2$  and then you do  $P_4$  This means you do  $P_2$  first.

Put the ornaments on the mantelpiece in any order.

If you do  $P_2$  and then do  $P_4$  they will end up in the same order as if you had just done  $P_6$

Try it.

So  $P_4 * P_2 = P_6$

Show that  $P_2 * P_4 = P_5$  So  $P_4 * P_2$  and  $P_2 * P_4$  are not the same.

\* is not commutative.

Here is the combination table. You should check some of these.

*	P1	P2	P3	P4	P5	P6
P1	P1	P2	P3	P4	P5	P6
P2	P2	P1	P6	P5	P4	P3
P3	P3	P5	P1	P6	P2	P4
P4	P4	P6	P5	P1	P3	P2
P5	P5	P3	P4	P2	P6	P1
P6	P6	P4	P2	P3	P1	P5

Note  $P2 * P4$  goes in the P2 row and the P4 column.

And  $P4 * P2$  goes in the P4 row and the P2 column.

The set  $\{P1, P2, P3, P4, P5, P6\}$  with the binary operation \* forms a group.

A final thought ...

Look at the chapter: Symmetry of a Triangle. We can pair-up these rearrangements with the symmetries of the triangle:

$$P1 \rightarrow e \quad P2 \rightarrow p \quad P3 \rightarrow q \quad P4 \rightarrow r \quad P5 \rightarrow b \quad P6 \rightarrow a$$

We find that these two groups are basically the same.

For example:

$$P3 * P5 = P2 \text{ and } q * b = p$$

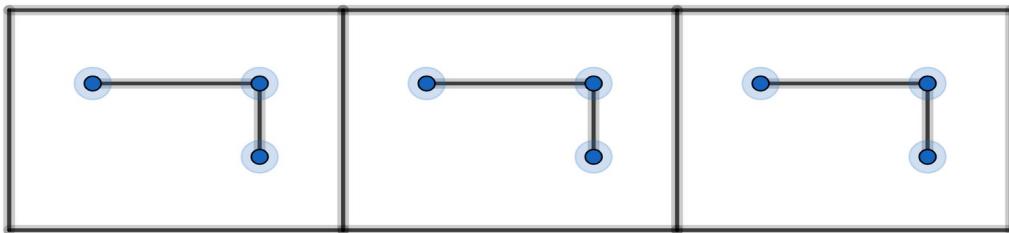
$$P2 * P4 = P5 \text{ and } p * r = b$$

$$P3 * P2 = P5 \text{ and } q * p = b$$

etc

We say these two groups are isomorphic which is a fancy way of saying they are basically the same.

## Friezes



Here we have a row of identical tiles that extends indefinitely in both directions. The diagram shows just three of these tiles. Each tile has a design on it. This is called a frieze.

All friezes have translation symmetry with repeat distance  $d$  the length of the tile. (see footnote)

We can classify friezes by their other symmetries which can include:

horizontal mirror line along the middle of the frieze

vertical mirror lines that are  $d/2$  apart

centres of  $180^\circ$  rotation that are  $d/2$  apart

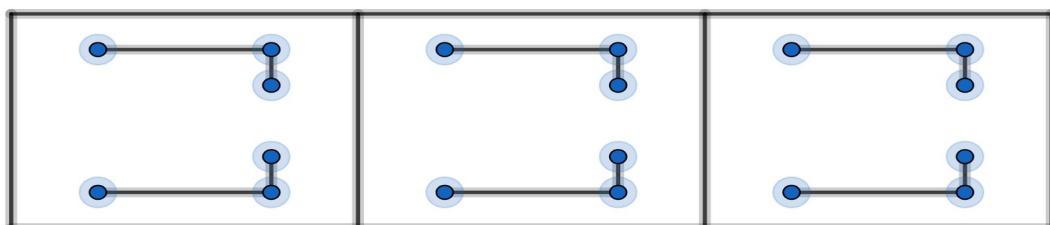
glide-reflections with a glide distance  $d/2$

### Example 1

no other symmetries

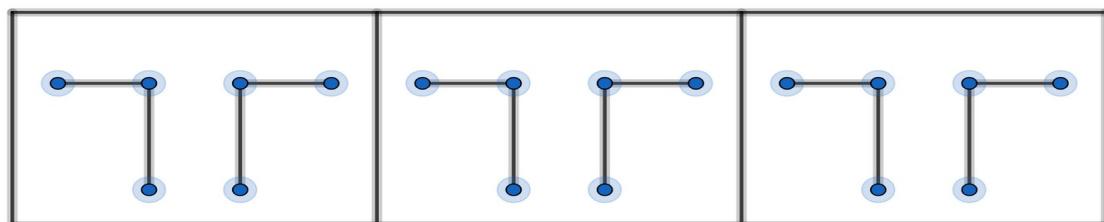
### Example 2

horizontal mirror line – can you mark this on the diagram?



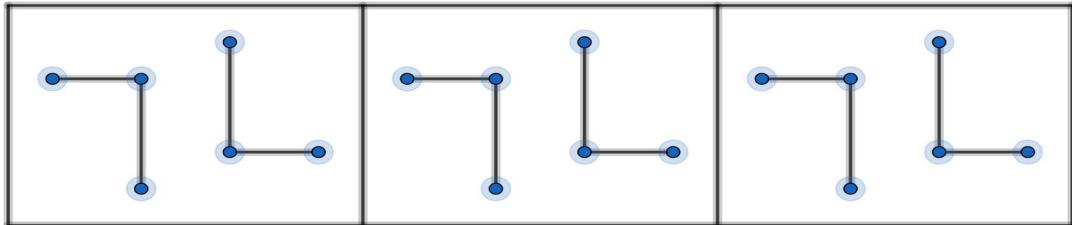
### Example 3

vertical mirror lines – can you mark these on the diagram?



#### Example 4

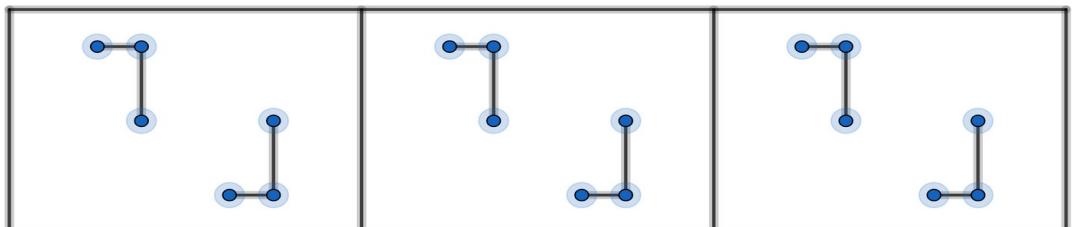
rotation – can you mark the centres of rotation on the diagram?



#### Example 5

glide-reflection

note: a glide-reflection is a combination of a translation and a reflection in a horizontal mirror line



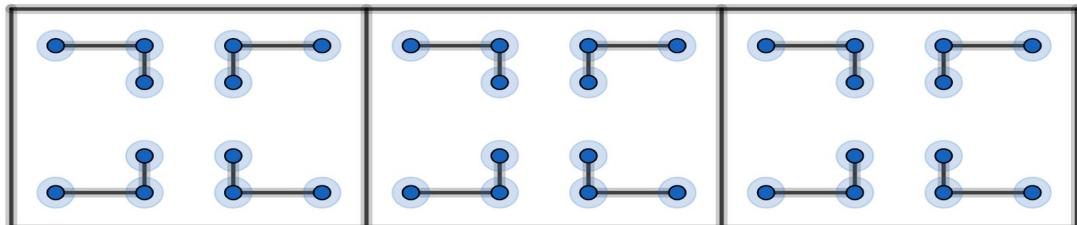
#### Example 6

horizontal mirror line

vertical mirror lines

rotation

can you mark these on the diagram?



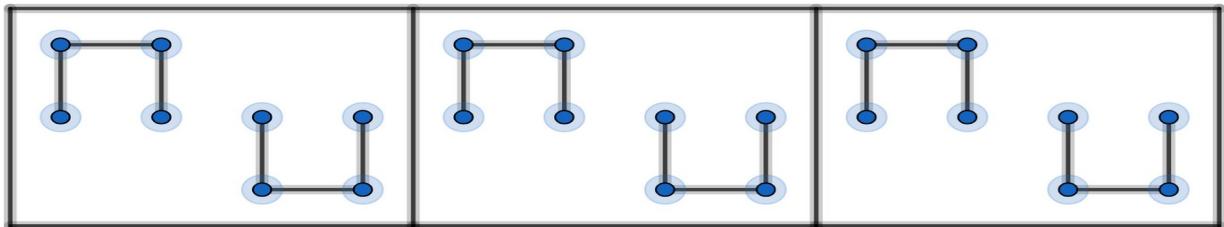
#### Example 7

vertical mirror lines

rotation

glide-reflection

can you mark these on the diagram?

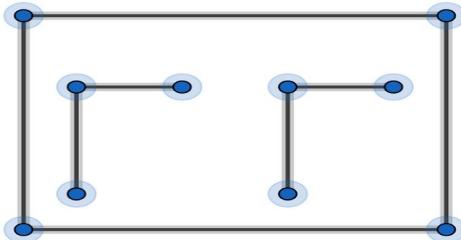


There are no more examples. There are only 7 frieze-symmetry-types. So every possible frieze can be classified as one of these 7 types.

Friezes repeat in one direction. Wallpapers repeat in two directions. It turns out that there are only 17 wallpaper-symmetry-types. So every possible wallpaper can be classified as one of these 17 types.

footnote:

What if our tile had length  $D$  and looked like this?



This individual tile has translation symmetry.

To keep things simple we will regard this as two tiles, each of length  $d=D/2$

## Propositions

A proposition is a statement that is either true or false.

Newton was born in England	this is a true proposition
Fermat was born in Poland	this is a false proposition
Please shut the door	this is not a proposition

### Example

$$a : \text{Today is Monday} \quad b : \text{I go to work today}$$

We can combine two propositions using AND

$$a \wedge b : \text{Today is Monday and I go to work today}$$

Today is Monday and I go to work today is true if:

Today is Monday is true

and I go to work today is true

Otherwise it is false.

So  $a \wedge b$  is true if  $a$  is true and  $b$  is true, otherwise it is false.

We can set this out in a truth table where 0 means false and 1 means true:

$a$	$b$	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

We can combine two propositions using OR

$$a \vee b : \text{Today is Monday or I go to work today (or both)}$$

Today is Monday or I go to work today is true if:

Today is Monday is true

or I go to work today is true

or both are true

Otherwise it is false.

So  $a \vee b$  is true if  $a$  is true or  $b$  is true (or both), otherwise it is false.

Truth table:

$a$	$b$	$a \vee b$
0	0	0
0	1	1
1	0	1
1	1	1

## Notes:

In ordinary English we use OR in two different ways.

I will buy you a beer or a lemonade (but not both)

You will get the job if you can sing or dance (or both)

$a \vee b$  always means  $a$  or  $b$  or both

## Negation

The negation of  $a$  is  $a'$

*a* : Today is Monday

$a'$  : Today is not Monday

Truth table:

$a$	$a'$
0	1
1	0

## Examples

Fill in the truth table for  $(a \vee b)'$

$a$	$b$	$a \vee b$	$(a \vee b)'$
0	0	0	1
0	1	1	0
1	0	1	0
1	1	1	0

Fill in the truth table for  $a \vee(b \wedge c)$

$a$	$b$	$c$	$b \wedge c$	$a \vee (b \wedge c)$
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	1
1	0	1	0	1
1	1	0	0	1
1	1	1	1	1

see EXERCISE 1

Look at Exercise 1, questions (3) and (4)

You should have found that the columns for  $(a \wedge b) \vee (a \wedge c)$  and  $a \wedge (b \vee c)$  are the same.

We say  $(a \wedge b) \vee (a \wedge c) = a \wedge (b \vee c)$

See EXERCISE 2

Note:

$$a \wedge 1 = 1 \text{ if } a = 1 \text{ and } a \wedge 1 = 0 \text{ if } a = 0 \text{ so } a \wedge 1 = a$$

$$a \vee 1 = 1 \text{ if } a = 1 \text{ and } a \vee 1 = 1 \text{ if } a = 0 \text{ so } a \vee 1 = 1$$

Similarly:

$$a \wedge 0 = 0 \text{ and } a \vee 0 = a$$

Use truth tables to prove the following rules: (no need to do them all)

$$(a')' = a$$

$$a \wedge a = a$$

$$a \vee a = a$$

$$a \wedge a' = 0$$

$$a \vee a' = 1$$

$$a \wedge b = b \wedge a$$

$$a \vee b = b \vee a$$

$$(a \wedge b) \wedge c = a \wedge (b \wedge c)$$

$$(a \vee b) \vee c = a \vee (b \vee c)$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

$$(a \wedge b)' = a' \vee b'$$

$$(a \vee b)' = a' \wedge b'$$

$$a \wedge (a \vee b) = a$$

$$a \vee (a \wedge b) = a$$

It's like a new type of algebra!

EXERCISE 1

1) fill in the truth table:

$a$	$b$	$b'$	$a \wedge b'$
0	0		
0	1		
1	0		
1	1		

2) fill in the truth table:

$a$	$b$	$a'$	$a' \vee b$
0	0		
0	1		
1	0		

1	1		
---	---	--	--

3) fill in the truth table:

$a$	$b$	$c$	$a \wedge b$	$a \wedge c$	$(a \wedge b) \vee (a \wedge c)$
0	0	0			
0	0	1			
0	1	0			
0	1	1			
1	0	0			
1	0	1			
1	1	0			
1	1	1			

4) fill in the truth table:

$a$	$b$	$c$	$b \vee c$	$a \wedge (b \vee c)$
0	0	0		
0	0	1		
0	1	0		
0	1	1		
1	0	0		
1	0	1		
1	1	0		
1	1	1		

## EXERCISE 2

Use truth tables to show that:

1)  $(a \wedge b)' = a' \vee b'$

2)  $(a \vee b)' = a' \wedge b'$

## SOLUTIONS 1

1)

$a$	$b$	$b'$	$a \wedge b'$
0	0	1	0
0	1	0	0
1	0	1	1
1	1	0	0

2)

$a$	$b$	$a'$	$a' \vee b$
0	0	1	1

0	1	1	1
1	0	0	0
1	1	0	1

3)

$a$	$b$	$c$	$a \wedge b$	$a \wedge c$	$(a \wedge b) \vee (a \wedge c)$
0	0	0	0	0	0
0	0	1	0	0	0
0	1	0	0	0	0
0	1	1	0	0	0
1	0	0	0	0	0
1	0	1	0	1	1
1	1	0	1	0	1
1	1	1	1	1	1

4)

$a$	$b$	$c$	$b \vee c$	$a \wedge (b \vee c)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

## SOLUTIONS 2

1)

$a$	$b$	$a \wedge b$	$(a \wedge b)'$	$a'$	$b'$	$a' \vee b'$
0	0	0	1	1	1	1
0	1	0	1	1	0	1
1	0	0	1	0-	1	1
1	1	1	0	0	0	0

2)

$a$	$b$	$a \vee b$	$(a \vee b)'$	$a'$	$b'$	$a' \wedge b'$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

If ... Then

Example

$p$  : Today is Friday                     $q$  : I go to yoga today

We can combine two propositions using IF ... THEN

$p \Rightarrow q$  : If today is Friday then I go to yoga today

What does this tell you?

If today is Friday then it tells you that I go to yoga today.

If today is not Friday then it tells you nothing.

If I go to yoga today then it tells you nothing.

If I do not go to yoga today then it tells you that today is not Friday.

The only way

If today is Friday then I go to yoga today

can be false, is if:

today is Friday, is true

and I go to yoga today, is false.

The only way  $p \Rightarrow q$  can be false is if  $p$  is true and  $q$  is false.

So we have this truth table:

$p$	$q$	$p \Rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

$p \Rightarrow q$  can be read as:

if  $p$  then  $q$

$p$  implies  $q$

$q$  if  $p$

$p$  only if  $q$

$q$  is necessary for  $p$

$p$  is sufficient for  $q$

$p \Rightarrow q$  is not the same as  $p' \Rightarrow q'$

Compare:

If today is Friday then I go to yoga today

If today is not Friday then I do not go to yoga today

$p \Rightarrow q$  is not the same as  $q \Rightarrow p$

Compare:

If today is Friday then I go to yoga today

If I go to yoga today then today is Friday

Note:  $q \Rightarrow p$  is called the converse of  $p \Rightarrow q$

$p \Rightarrow q$  is the same as  $q' \Rightarrow p'$

Compare:

If today is Friday then I go to yoga today

If I do not go to yoga today then today is not Friday

Note:  $q' \Rightarrow p'$  is called the contrapositive of  $p \Rightarrow q$

Note: A common error or fudge is to prove  $p \Rightarrow q$  and then pretend you have proved  $q \Rightarrow p$

For example, in the chapter Euler Tours, we proved:

If a closed Euler tour exists then every vertex is even.

We then pretended to have proved:

If every vertex is even then a closed Euler tour exists.

This is very naughty.

see Exercise 1

We can combine two propositions using IF AND ONLY IF

$p \Leftrightarrow q$  :Today is Friday if and only if I go to yoga today

What does this tell you?

If today is Friday then it tells you that I go to yoga today.

If today is not Friday then it tells you that I do not go to yoga today.

If I go to yoga today then it tells you that today is Friday.

If I do not go to yoga today then it tells you that today is not Friday.

So  $p \Leftrightarrow q$  is true if  $p$  and  $q$  are both true or both false, otherwise it is false.

Truth table:

$p$	$q$	$p \Leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

$p \Leftrightarrow q$  can be read as:

$p$  if and only if  $q$

$p$  is necessary and sufficient for  $q$

To prove  $p \Leftrightarrow q$  we have to prove  $p \Rightarrow q$  and we have to prove  $q \Rightarrow p$

For example, in the chapter Rationals and Irrationals, we proved:

$x$  is rational  $\Leftrightarrow x$  is a terminating or recurring decimal

See Exercise 2

### EXERCISE 1

1.

Use a truth table to show that:

$p \Rightarrow q$  is not the same as  $p' \Rightarrow q'$

$p \Rightarrow q$  is not the same as  $q \Rightarrow p$

$p \Rightarrow q$  is the same as  $q' \Rightarrow p'$

2. Use a truth table to show that:

$$(p \Rightarrow q) = (p' \vee q) \text{ and } (p \Rightarrow q) = (p \wedge q')'$$

3.

Fill in the truth table

$p$	$q$	$r$	$p \Rightarrow q$	$q \Rightarrow r$	$(p \Rightarrow q) \wedge (q \Rightarrow r)$	$p \Rightarrow r$	$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
0	0	0					
0	0	1					
0	1	0					
0	1	1					
1	0	0					
1	0	1					

1	1	0					
1	1	1					

## SOLUTIONS 1

1.

$p$	$q$	$p \Rightarrow q$	$p'$	$q'$	$p' \Rightarrow q'$	$q \Rightarrow p$	$q' \Rightarrow p'$
0	0	1	1	1	1	1	1
0	1	1	1	0	0	0	1
1	0	0	0	1	1	1	0
1	1	1	0	0	1	1	1

2.

$p$	$q$	$p \Rightarrow q$	$p'$	$p' \vee q$	$q'$	$p \wedge q'$	$(p \wedge q')'$
0	0	1	1	1	1	0	1
0	1	1	1	1	0	0	1
1	0	0	0	0	1	1	0
1	1	1	0	1	0	0	1

3.

$p$	$q$	$r$	$p \Rightarrow q$	$q \Rightarrow r$	$(p \Rightarrow q) \wedge (q \Rightarrow r)$	$p \Rightarrow r$	$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

So  $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$  is always true, regardless of the truth of  $p$ ,  $q$ ,  $r$ . We call this a tautology.

## EXERCISE 2

For each of the following, does  $p \Rightarrow q$  or  $q \Rightarrow p$  or  $p \Leftrightarrow q$  ?

- | $p$                            | $q$                     |
|--------------------------------|-------------------------|
| a) $x=4$                       | $2x=8$                  |
| b) $n$ is a multiple of 5      | $n$ is a multiple of 15 |
| c) $n$ is not a multiple of 10 | $n$ is a prime          |
| d) $ABCD$ is a parallelogram   | $ABCD$ is a square      |
| e) $x^2 - 6x + 8 = 0$          | $x=2$                   |
| f) $x^2 - 4x + 4 = 0$          | $x=2$                   |
| g) $x=4$                       | $x^2=16$                |
| h) $x > 7$                     | $x > 4$                 |
| i) $x$ is an integer           | $x$ is rational         |
| j) $x > 2$                     | $x^2 > 4$               |
| k) $x < 4$                     | $x^2 < 16$              |

## SOLUTIONS 2

- a)  $p \Leftrightarrow q$  b)  $q \Rightarrow p$  c)  $q \Rightarrow p$  d)  $q \Rightarrow p$  e)  $q \Rightarrow p$  f)  $p \Leftrightarrow q$   
g)  $p \Rightarrow q$  h)  $p \Rightarrow q$  i)  $p \Rightarrow q$  j)  $p \Rightarrow q$  k)  $q \Rightarrow p$

## Arguments with If ... Then

### Example 1

If today is Monday then I go to work today

Today is Monday

So I go to work today

This argument consists of three propositions:

Premise: If today is Monday then I go to work today

Premise: Today is Monday

Conclusion: I go to work today

We are not interested in whether these propositions are true or false. We are interested in whether this argument is valid or invalid. An argument is only valid if the conclusion must be true whenever both the premises are true.

$p$  : Today is Monday       $q$  : I go to work today

$p'$  : Today is not Monday       $q'$  : I do not go to work today

The above argument is valid and has the form:

$p \Rightarrow q$

$p$

So  $q$

### Example 2

If today is Monday then I go to work today

I do not go to work today

So today is not Monday

This argument is valid and has the form:

$p \Rightarrow q$

$q'$

So  $p'$

### Example 3

If today is Monday then I go to work today

Today is not Monday

So I do not go to work today

This argument is invalid and has the form:

$p \Rightarrow q$

$p'$

So  $q'$

#### Example 4

If today is Monday then I go to work today

I go to work today

So today is Monday

This argument is invalid and has the form:

$p \Rightarrow q$

$q$

So  $p$

#### See Exercise 1

I have stated which of the above arguments are valid and which are invalid. It is just obvious.

Well ... we can do better than this. We can test arguments using truth tables.

#### Example

Test the argument:

$p \Rightarrow q$

$q'$

So  $p'$

$p$	$q$	$p \Rightarrow q$	$q'$	$p'$
0	0	1	1	1
0	1	1	0	1
1	0	0	1	0
1	1	1	0	0

Remember, an argument is only valid if the conclusion must be true whenever both the premises are true.

Both the premises are true in line 1 and the conclusion is true.

So this argument is valid.

### Example

$$p \Rightarrow q$$

$$p'$$

$$\text{So } q'$$

$p$	$q$	$p \Rightarrow q$	$p'$	$q'$
0	0	1	1	1
0	1	1	1	0
1	0	0	0	1
1	1	1	0	0

Both the premises are true in line 2 but the conclusion is false.  
So this argument is invalid.

See Exercise 2

If an argument is invalid then we might be able to show this by finding a counter-example.

Consider the argument

$$p \Rightarrow q$$

$$p'$$

$$\text{So } q'$$

If we put:

$$p \text{ dogs are birds} \quad q \text{ dogs are animals}$$

then we get:

If dogs are birds then dogs are animals

Dogs are not birds

So dogs are not animals

An argument is only valid if the conclusion must be true whenever both the premises are true. But here, both premises are true and the conclusion is false. So the argument must be invalid.

See Exercise 3

### EXERCISE 1

$$p : \text{It is raining} \quad q : \text{I take my umbrella}$$

$$p' : \text{It is not raining} \quad q' : \text{I do not take my umbrella}$$

Which of the following arguments are valid?

- 1) If it is raining then I take my umbrella  
I do not take my umbrella  
So it is not raining
- 2) If it is raining then I take my umbrella  
I take my umbrella  
So it is raining
- 3) If it is raining then I take my umbrella  
It is not raining  
So I do not take my umbrella
- 4) If it is raining then I take my umbrella  
It is raining  
So I take my umbrella

## EXERCISE 2

Test the following arguments using truth tables:

1.

$$p \Rightarrow q$$

$$p$$

$$\text{So } q$$

2.

$$p \Rightarrow q$$

$$q$$

$$\text{So } p$$

3.

$$(p \wedge q)'$$

$$p'$$

$$\text{So } q$$

4.

$$p \vee q$$

$$p'$$

$$\text{So } q$$

5.

$$p \vee q$$

$p \Rightarrow r$

$q \Rightarrow r$

So  $r$

6.

$p \Rightarrow q$

$q \Rightarrow r$

So  $p \Rightarrow r$

### EXERCISE 3

Show that the negation of  $p \Rightarrow q$  is  $p \wedge q'$

### SOLUTIONS 1

1) This argument has the form:

$p \Rightarrow q$

$q'$

So  $p'$

Like example 2, this is valid.

2) This argument has the form:

$p \Rightarrow q$

$q$

So  $p$

Like example 4, this is invalid.

3) This argument has the form:

$p \Rightarrow q$

$p'$

So  $q'$

Like example 3, this is invalid.

4) This argument has the form:

$p \Rightarrow q$

$p$

So  $q$

Like example 1, this is valid.

## SOLUTIONS 2

1.

$p$	$q$	$p \Rightarrow q$	$p$	$q$
0	0	1	0	0
0	1	1	0	1
1	0	0	1	0
1	1	1	1	1

Look at line 4. This argument is valid.

2.

$p$	$q$	$p \Rightarrow q$	$q$	$p$
0	0	1	0	0
0	1	1	1	0
1	0	0	0	1
1	1	1	1	1

Look at line 2. This argument is invalid.

3.

$p$	$q$	$p \wedge q$	$(p \wedge q)'$	$p'$	$q$
0	0	0	1	1	0
0	1	0	1	1	1
1	0	0	1	0	0
1	1	1	0	0	1

Look at line 1. This argument is invalid.

4.

$p$	$q$	$p \vee q$	$p'$	$q$
0	0	0	1	0
0	1	1	1	1
1	0	1	0	0
1	1	1	0	1

Look at line 2. This argument is valid.

5.

$p$	$q$	$r$	$p \vee q$	$p \Rightarrow r$	$q \Rightarrow r$	$r$
0	0	0	0	1	1	0
0	0	1	0	1	1	1
0	1	0	1	1	0	0
0	1	1	1	1	1	1
1	0	0	1	0	1	0
1	0	1	1	1	1	1
1	1	0	1	0	0	0
1	1	1	1	1	1	1

Look at lines 4, 6 and 8. This argument is valid.

6.

$p$	$q$	$r$	$p \Rightarrow q$	$q \Rightarrow r$	$p \Rightarrow r$
0	0	0	1	1	1
0	0	1	1	1	1
0	1	0	1	0	1
0	1	1	1	1	1
1	0	0	0	1	0
1	0	1	0	1	1
1	1	0	1	0	0
1	1	1	1	1	1

Look at lines 1, 2, 4, 8. This argument is valid

### SOLUTIONS 3

$p$	$q$	$p \Rightarrow q$	$(p \Rightarrow q)'$	$q'$	$p \wedge q'$
0	0	1	0	1	0
0	1	1	0	0	0
1	0	0	1	1	1
1	1	1	0	0	0

The columns for  $(p \Rightarrow q)'$  and  $p \wedge q'$  are the same.

## Arguments with All, None, Some

### Example 1

All teachers are honest

All honest people like sprouts

So all teachers like sprouts

This argument consists of two premises and a conclusion:

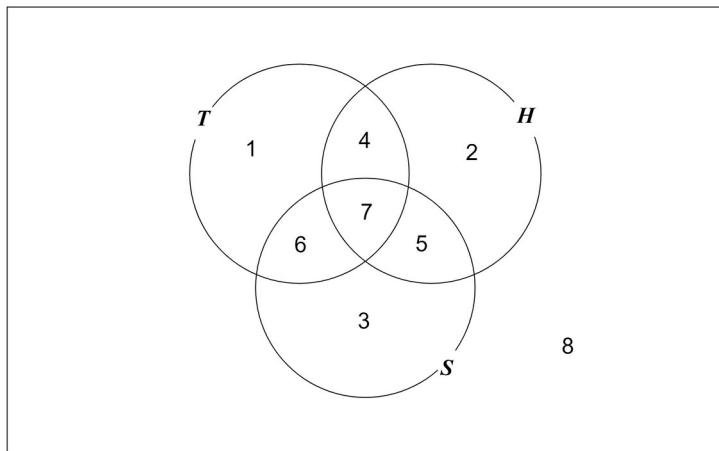
Premise: All teachers are honest

Premise: All honest people like sprouts

Conclusion: All teachers like sprouts

We are not interested in whether the premises are true or false. We are interested in whether the argument is valid or invalid. An argument is only valid if the conclusion must be true whenever both the premises are true. We can use a Venn diagram to decide if an argument is valid or invalid.

We have a rectangular room and there are three loops drawn on the floor.



Everyone is standing somewhere in the room. Teachers must stand inside the T loop. Honest people must stand inside the H loop. People who like sprouts must stand inside the S loop.

People standing inside region 1 are teachers, not honest, do not like sprouts

People standing inside region 5 are not teachers, honest, do like sprouts

People standing inside region 7 are teachers, honest, do like sprouts

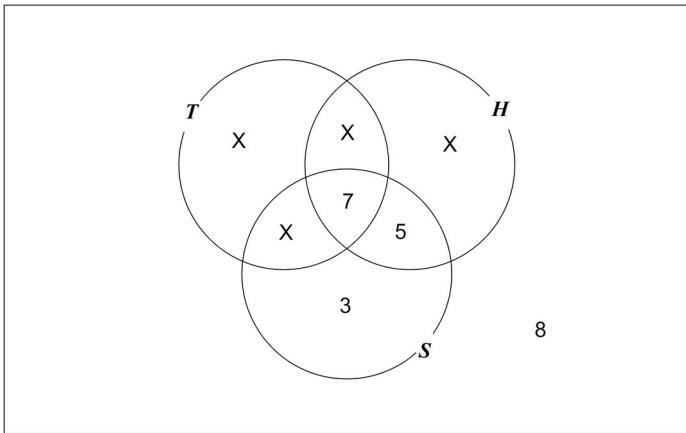
etc

Premise: All teachers are honest

This means there is no-one standing in regions 1 or 6. So we put a cross in each of these regions.

Premise: All honest people like sprouts

This means there is no-one standing in regions 2 or 4. So we put a cross in each of these regions.



Conclusion: All teachers like sprouts

This means there should be crosses in regions 1 and 4. Yes!

So if both premises are true then the conclusion must be true. So the argument is valid.

We are not really interested in teachers, honest people and people who like sprouts. We are interested in the form of the argument. We could say:

All A are B

All B are C

So all A are C

This argument form is valid. So any argument of this form is valid, such as:

All lawyers are happy

All happy people like Beethoven

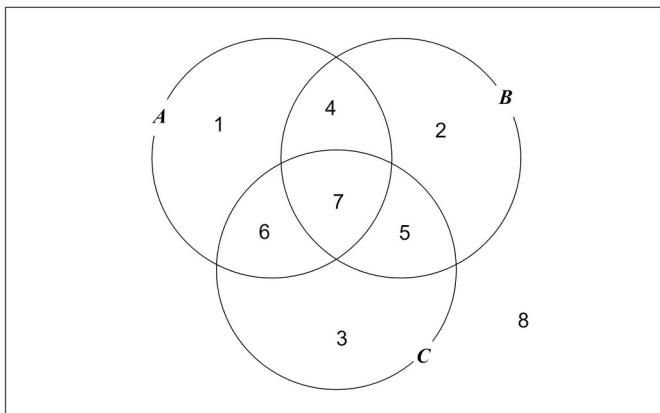
So all lawyers like Beethoven

Example 2

All A are B

No C are A

So no C are B

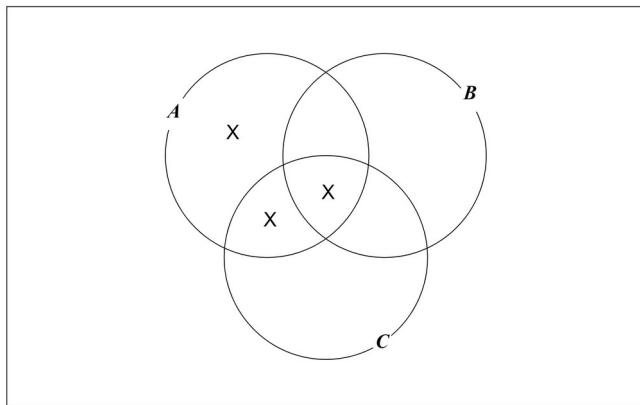


Premise: All A are B

This means there is no-one standing in regions 1 or 6

Premise: No C are A

This means there is no-one standing in regions 6 or 7



Conclusion: No C are B

This means there should be crosses in regions 5 and 7. No!

So the argument is invalid. So any argument of this form is invalid, such as:

All dentists are polite.

No hoodlums are dentists.

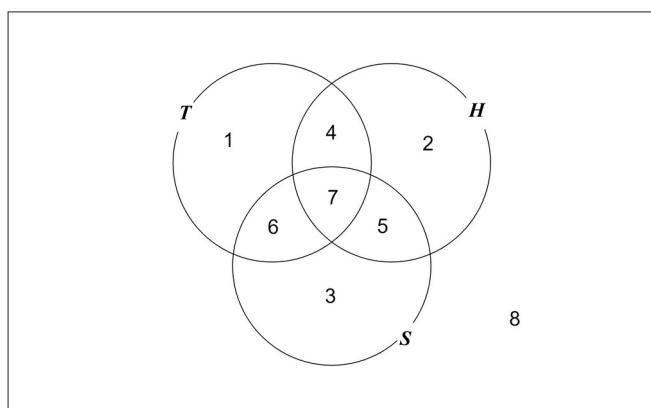
So no hoodlums are polite.

### Example 3

All teachers are honest

Some teachers like sprouts

So some honest people like sprouts



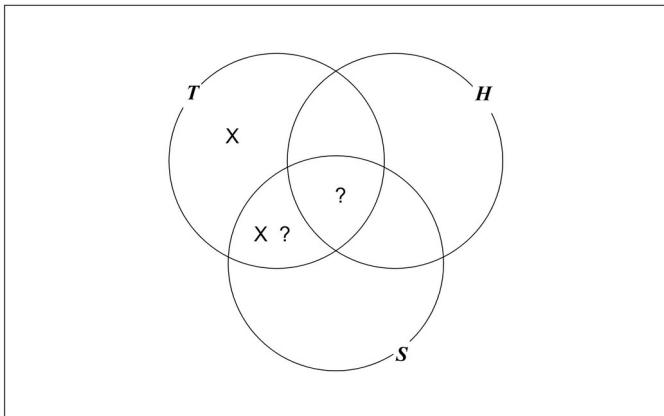
All teachers are honest

we put a cross in regions 1 and 6

## Some teachers like sprouts

this means that there is at least one teacher who likes sprouts,

so there is at least one person in region 6 or 7, so we put question-marks in regions 6 and 7



Conclusion: Some honest people like sprouts

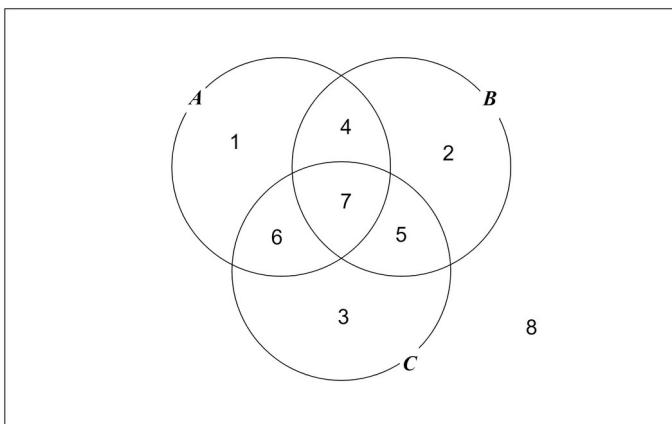
There is at least one person in region 6 or 7, but there is no-one in region 6 (because region 6 has a cross), so there must be at least one person in region 7, so there must be at least one person who is honest and likes sprouts, so some honest people like sprouts, so the argument is valid.

### Example 4

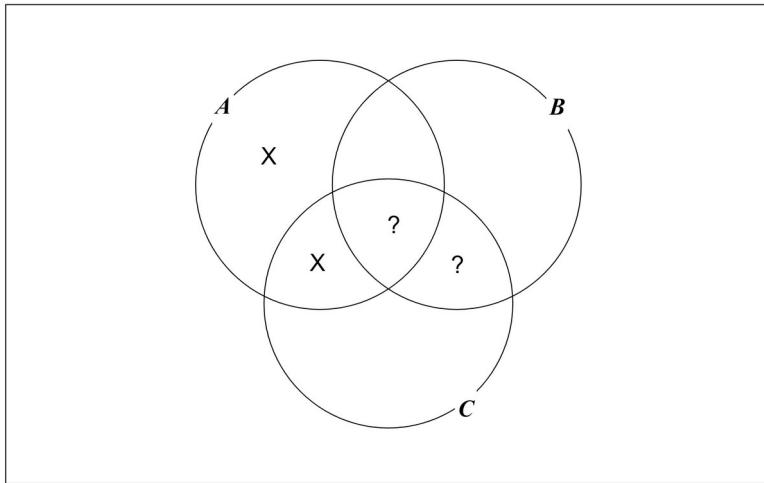
All A are B

Some B are C

So some A are C



- All A are B      put crosses in regions 1 and 6
- Some B are C      put question-marks in regions 5 and 7



Conclusion:      Some A are C

There is at least one person in region 5 or 7, but we cannot be certain that there is anybody in region 7

So the argument is invalid. So any argument of this form is invalid, such as:

All cats are mammals.

Some mammals are ferocious.

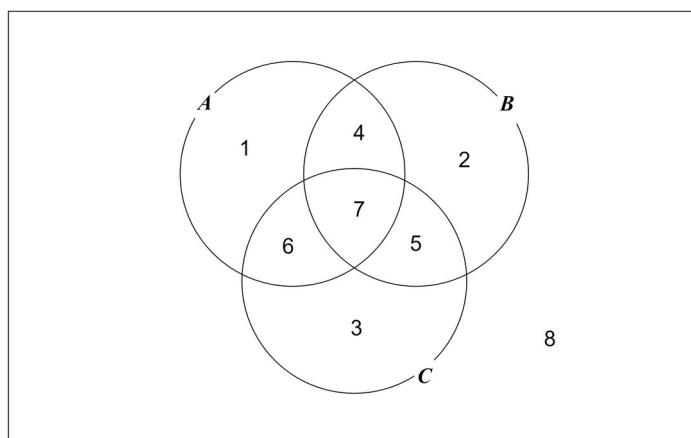
So some cats are ferocious.

Example 5

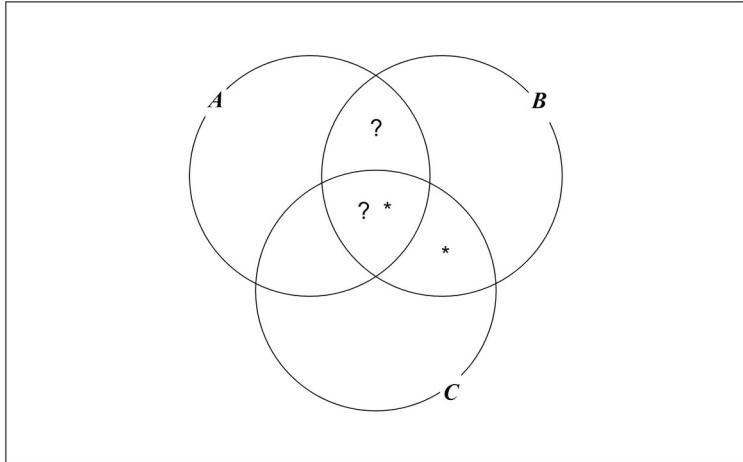
Some A are B

Some B are C

So some A are C



Some A are B      put question-marks in regions 4 and 7  
Some B are C      we cannot just put question-marks in regions 5 and 7 because we will get  
these mixed up with the question-marks from Some A are B, so we will use asterisks instead



Conclusion      Some A are C  
There is at least one person in regions 4 or 7 and there is at least one person in regions 5 or 7, but  
we cannot be certain that there is anybody in region 7  
So the argument is invalid.

In fact, if our two premisses both begin with Some ... then the argument will always be invalid.  
Think about it!

#### EXERCISE

Show that these two arguments are invalid:

1.    All A are B  
      All C are B  
      So all C are A
2.    All A are B  
      All A are C  
      So all C are B

Now try these:

3.    No bankers are poor.  
      No poor people eat carrots.  
      So all bankers eat carrots.

4. All plumbers are rich.  
No rich people are happy.  
So no plumbers are happy.
5. No dentists eat sugar.  
All communists eat sugar.  
So no dentists are communists.
6. All astronauts are handsome.  
All handsome people like jazz.  
So all astronauts like jazz.
7. Some teachers eat bananas.  
All teachers like spaghetti.  
So some people who like spaghetti eat bananas.
8. No A are B  
Some B are C  
So no A are C
9. All A are B  
Some C are B  
So some A are C

10. The negation of:

it is raining

is:

it is not raining

Write down the negations of the following:

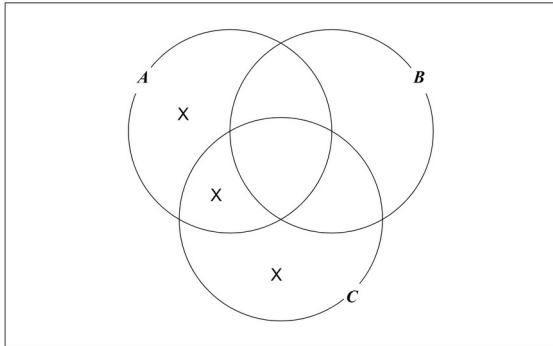
- a) All astronauts like jazz
- b) No astronauts like jazz
- c) Some astronauts like jazz
- d) All A are B
- e) No A are B
- f) Some A are B
- g) Some A are not B

11. Only A are B                  All B are A

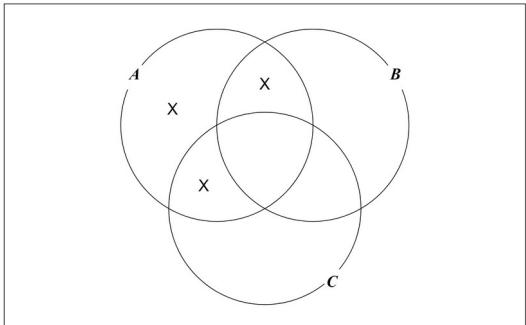
Do these mean the same thing?

## SOLUTIONS

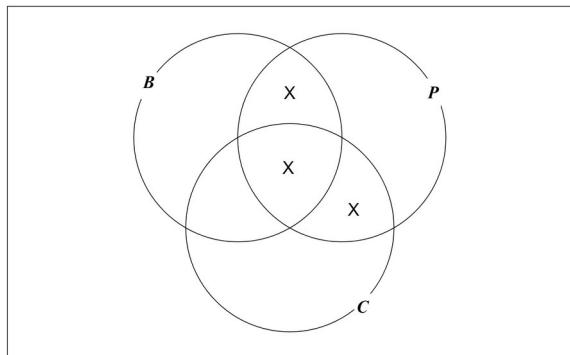
1. invalid



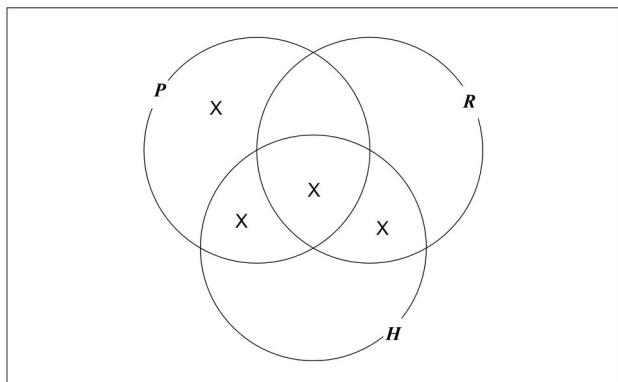
2. invalid



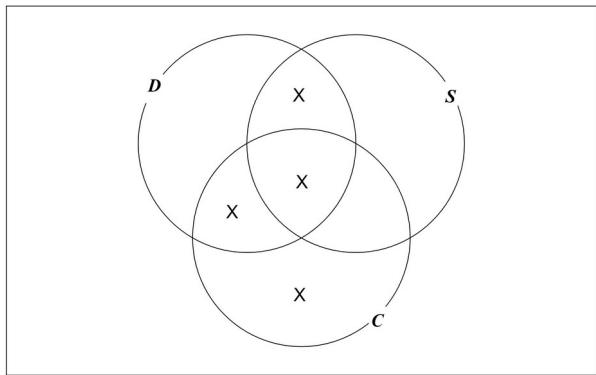
3. invalid



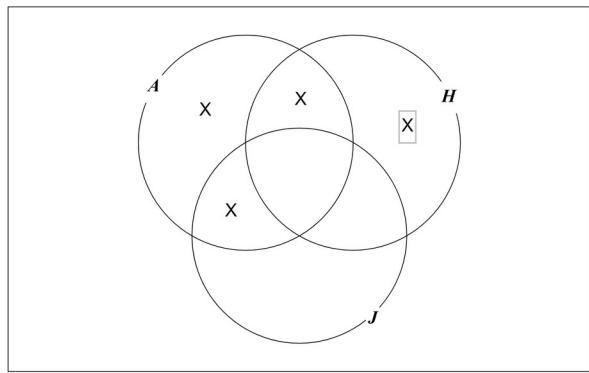
4. valid



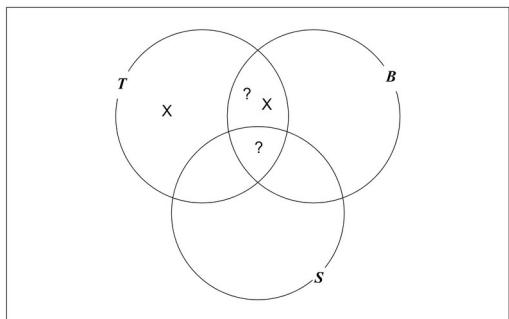
5. valid



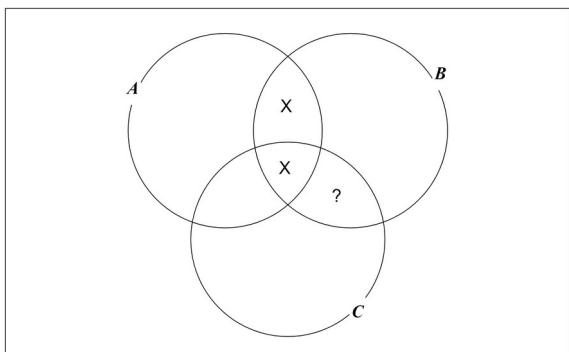
6. valid



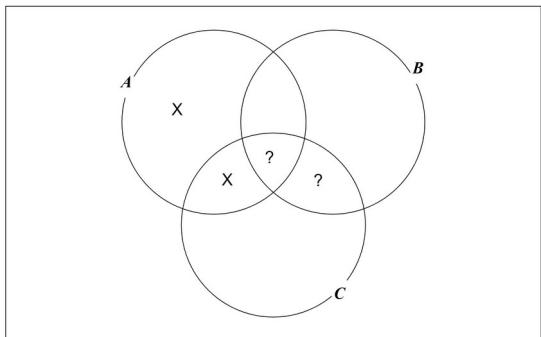
7. valid



8. invalid



9. invalid



10.

- a) Some astronauts do not like jazz
- b) Some astronauts like jazz
- c) No astronauts like jazz
- d) Some A are not B
- e) Some A are B
- f) Some A are B
- g) All A are B

11. Yes

## Hat Puzzles

There are three players called A, B and C. Each player is capable of making logical deductions.

I place a hat on the head of each player. I have three silver coloured hats and two gold coloured hats to choose from. No player can see their own hat. Each player tries to deduce the colour of their own hat. If a player can deduce the colour of their own hat then they shout.

The players stand in a queue.

A (at the back of the queue) can see B's hat and C's hat

B (in the middle of the queue) can see C's hat

C (at the front of the queue) can see no hats

Who can deduce the colour of their own hat in these examples?

- |                       |                    |                    |
|-----------------------|--------------------|--------------------|
| a) A has a silver hat | B has a gold hat   | C has a gold hat   |
| b) A has a silver hat | B has a silver hat | C has a gold hat   |
| c) A has a silver hat | B has a silver hat | C has a silver hat |

## SOLUTIONS

a) A thinks:

I can see two gold hats. So my hat must be silver.

b) B thinks:

If my hat is gold then A can deduce her hat is silver (see previous example). So if A does not shout then my hat is silver.

c) C thinks:

If my hat is gold then B can deduce his hat is silver (see previous example). So if B does not shout then my hat is silver.

## Fundamental Theorem of Arithmetic

Some positive integers are prime numbers.

2, 3, 5, 7, 11, 13, 17, 19....

All the others can be written, in just one way, as a product of prime numbers. For example:

$$60 = 6 \times 10 = 2 \times 3 \times 2 \times 5 = (2^2)(3)(5)$$

In general:

If  $N$  is any positive integer (except 1) then  $N = (2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$

where  $a, b, c, \dots$  are zero or positive integers.

### Example 1

Highest common factor (HCF) and Lowest common multiple (LCM)

the factors of 24 are: 1, 2, 3, 4, 6, 8, 12, 24

the factors of 30 are: 1, 2, 3, 5, 6, 10, 15, 30

the common factors of 24 and 30 are: 1, 2, 3, 6

So  $HCF(24, 30) = 6$

the multiples of 24 are: 24, 48, 72, 96, 120, 144, 168, 192, 216, 240, 264 ...

the multiples of 30 are: 30, 60, 90, 120, 150, 180, 210, 240, 270, 300, 330 ...

the common multiples of 24 and 30 are: 120, 240, ...

So  $LCM(24, 30) = 120$

### Example 2

$$A = (2^5)(3^1)(5^0)(7^6)(11^2) \text{ and } B = (2^3)(3^7)(5^4)(7^8)(11^0)$$

$2^5$  is a factor of  $A$  and  $2^3$  is a factor of  $B$  so HCF is a multiple of  $2^3$

$3^1$  is a factor of  $A$  and  $3^7$  is a factor of  $B$  so HCF is a multiple of  $3^1$

etc

So  $HCF(A, B) = (2^3)(3^1)(5^0)(7^6)(11^0)$

$A$  is a multiple of  $2^5$  and  $B$  is a multiple of  $2^3$  so LCM is a multiple of  $2^5$

$A$  is a multiple of  $3^1$  and  $B$  is a multiple of  $3^7$  so LCM is a multiple of  $3^7$

etc

So  $LCM(A, B) = (2^5)(3^7)(5^4)(7^8)(11^2)$

note

$$HCF(A,B) \times LCM(A,B) = (2^8)(3^8)(5^4)(7^{14})(11^2) = AB$$

Example 3

$$N = (2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$$

If  $N$  is a multiple of 5 then  $c \geq 1$ . If  $N$  is not a multiple of 5 then  $c=0$

If  $N$  is a multiple of 3 and a multiple of 7 then  $b \geq 1$  and  $d \geq 1$

So  $N$  is a multiple of 21

If  $N$  is a multiple of 6 then  $N$  is a multiple of 2 and a multiple of 3 so  $a \geq 1$  and  $b \geq 1$

If  $N$  is a multiple of 15 then  $N$  is a multiple of 3 and a multiple of 5 so  $b \geq 1$  and  $c \geq 1$

So if  $N$  is a multiple of 6 and a multiple of 15 then  $N$  must be a multiple of 30

In general:

If  $N$  is a multiple of  $a$  and a multiple of  $b$  then  $N$  is a multiple of  $LCM(a,b)$

Example 4

$$N = (2)(3^2)(13^4) \quad M = (5^3)(7^5)(13)(23) \text{ so } NM = (2)(3^2)(5^3)(7^5)(13^5)(23)$$

$NM$  is a multiple of 3 because  $N$  is a multiple of 3

$NM$  is a multiple of 7 because  $M$  is a multiple of 7

$NM$  is not a multiple of 17 because neither  $N$  nor  $M$  is a multiple of 17

but:

$NM$  is a multiple of 14 even though neither  $N$  nor  $M$  is a multiple of 14

this is because  $14 = 2 \times 7$  and  $N$  is a multiple of 2 and  $M$  is a multiple of 7

also:

$NM$  is a multiple of 35 but  $N$  and 35 have no common factor. So all the factors of 35 must appear in  $M$ . So  $M$  must be a multiple of 35

In general: if  $p$  is prime:

$NM$  is a multiple of  $p$  only if  $N$  or  $M$  (or both) is a multiple of  $p$

In general: if  $N$  and  $r$  have no common factor:

$NM$  is a multiple of  $r$  only if  $M$  is a multiple of  $r$

see Exercise 1

Theorem

$\sqrt{2}$  is irrational

Proof (by contradiction)

Assume  $\sqrt{2}$  is rational

So:

$$\sqrt{2} = \frac{p}{q} \text{ where } p \text{ and } q \text{ are positive integers}$$

So:

$$2q^2 = p^2$$

Now:

We can write  $q$  as a product of primes:

$$q = (2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$$

So:

$$q^2 = (2^{2a})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(\dots) \text{ the powers of all the primes are even}$$

So:

$$2q^2 = (2^{2a+1})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(\dots) \text{ the power of 2 is odd}$$

Now:

We can write  $p$  as a product of primes:

$$p = \dots$$

So:

$$p^2 = \dots \text{ all the powers of all the primes are even}$$

But:

$$2q^2 = p^2$$

LHS, power of 2 is odd. RHS, power of 2 is even.

Contradiction.

There is another proof that  $\sqrt{2}$  is irrational in the chapter: Proof by Contradiction

But this proof is better, because it suggests why the result is true and it suggests further results.

See Exercise 2

EXERCISE 1

- 1) Write 5619250 in the form  $(2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$
- 2) Find  $HCF(36652, 38698)$  and  $LCM(36652, 38698)$
- 3)  $532400 = (2^4)(5^2)(11^3)$  How many factors has 532400 got?
- 4) This question is difficult
  - a) If  $n^2$  is a multiple of 7 show that  $n$  is a multiple of 7
  - b) If  $n^2$  is a multiple of 6 show that  $n$  is a multiple of 6
  - c) If  $n^2$  is a multiple of 12 show that  $n$  might not be a multiple of 12
  - d) For what values of  $m$  is the following true:  
If  $n^2$  is a multiple of  $m$  then  $n$  must be a multiple of  $m$  ?

## EXERCISE 2

- 1) Prove  $5^{1/3}$  is irrational
- 2) What happens when we try to prove  $\sqrt[3]{4}$  is irrational?

## SOLUTIONS 1

- 1)  $5619250 = (2)(5^3)(7)(13^2)(19)$
- 2)  $36652 = (2^2)(7^2)(11^1)(17^1)$  and  $38698 = (2^1)(11^1)(1759^1)$   
 $HCF(36652, 38698) = (2^1)(11^1) = 22$   
 $LCM(36652, 38698) = (2^2)(7^2)(11^1)(17^1)(1759^1) = 64470868$
- 3)  $532400 = (2^4)(5^2)(11^3)$  so any factor can be written as  $(2^p)(5^q)(11^r)$   
where  $p=0,1,2,3,4$  and  $q=0,1,2$  and  $r=0,1,2,3$   
We have 5 choices for the value of  $p$  and 3 choices for the value of  $q$  and 4 choices for the value of  $r$  So there are  $5 \times 3 \times 4 = 60$  choices for  $p, q, r$   
So 532400 has 60 factors (including 1 and 532400)

- 4)  $n = (2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$   
 $n^2 = (2^{2a})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(\dots)$

proof by contrapositive

- a) If  $n$  is not a multiple of 7 then  $d=0$  and  $n^2$  is not a multiple of 7
- b) If  $n$  is not a multiple of 6 then  $a=0$  or  $b=0$  and  $n^2$  is not a multiple of 6
- c) If  $n$  is not a multiple of 12 then we cannot say  $a=0$  or  $b=0$  because we could have  $a=1$  and  $b=1$  for example if  $n=6$

$6^2$  is a multiple of 12 but 6 is not a multiple of 12

d)  $m = (2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$

The statement is true if  $a=0,1$      $b=0,1$      $c=0,1$  etc

## SOLUTIONS 2

1) Assume  $5^{1/3}$  is rational

$$5^{1/3} = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers}$$

$$5q^3 = p^3$$

We can write  $q$  as a product of powers of primes:

$$q = (2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$$

$q^3 = (2^{3a})(3^{3b})(5^{3c})(7^{3d})(11^{3e})(\dots)$  all the powers of all the primes are multiples of three.

$5q^3 = (2^{3a})(3^{3b})(5^{3c+1})(7^{3d})(11^{3e})(\dots)$  the power of 5 is not a multiple of three.

We can write  $p$  as a product of powers of primes:

$$p = \dots$$

$p^3 = \dots$  all the powers of all the primes are multiples of three

$$5q^3 = p^3$$

LHS, power of 5 is not a multiple of three. RHS, power of 5 is a multiple of three.

Contradiction.

2) Claim

$\sqrt{4}$  is irrational

Attempted proof (by contradiction)

Assume  $\sqrt{4}$  is rational

$$\sqrt{4} = \frac{p}{q} \text{ where } p \text{ and } q \text{ are positive integers}$$

$$4q^2 = p^2$$

We can write  $q$  as a product of primes:

$$q = (2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$$

$q^2 = (2^{2a})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(\dots)$  the powers of all the primes are even

$4q^2 = (2^{2a+2})(3^{2b})(5^{2c})(7^{2d})(11^{2e})(\dots)$  the power of 2 is still even!

This is where our proof falls apart.

## Euclid's Algorithm

An algorithm is a set of precise instructions that will solve a problem. Euclid's algorithm will solve the problem of finding the highest common factor of two positive integers.

Here is Euclid's algorithm for finding  $HCF(3458, 651)$

$$d = HCF(3458, 651)$$

We divide 3458 by 651

$$3458 = (5)(651) + 203$$

If 3458 and 651 are both multiples of  $d$  then 651 and 203 are both multiples of  $d$

We now repeat the procedure:

$$651 = (3)(203) + 42$$

If 651 and 203 are both multiples of  $d$  then 203 and 42 are both multiples of  $d$

$$203 = (4)(42) + 35$$

If 203 and 42 are both multiples of  $d$  then 42 and 35 are both multiples of  $d$

$$42 = (1)(35) + 7$$

If 42 and 35 are both multiples of  $d$  then 35 and 7 are both multiples of  $d$

$$35 = (5)(7) + 0 \quad \text{STOP}$$

So  $d = 7$

See Exercise 1

We can now write  $HCF(3458, 651)$  in the form  $3458n + 651m$  for integers  $n$  and  $m$

Working back up the page:

$$7 = (42) + (-1)(35) \quad \text{But } 35 = 203 + (-4)(42)$$

$$7 = (-1)(203) + (5)(42) \quad \text{But } 42 = 651 + (-3)(203)$$

$$7 = (5)(651) + (-16)(203) \quad \text{But } 203 = 3458 + (-5)(651)$$

$$7 = (-16)(3458) + (85)(651)$$

We can use Euclid's algorithm to solve some Diophantine equations. A Diophantine equation requires integer solutions.

Example

Solve  $3458x + 651y = 47894$  where  $x, y$  are integers

Run Euclid's algorithm to find  $HCF(3458, 651)$

We have just done this and we found:

$$HCF(3458, 651) = 7$$

Then we found:

$$7 = (-16)(3458) + (85)(651) \text{ so } (3458)(-16) + (651)(85) = 7$$

Now  $\frac{47894}{7} = 6842$  so we multiply both sides by 6842

So:

$$(3458)(-109472) + (651)(581570) = 47894$$

We have a solution to our equation:  $x = -109472$        $y = 581570$

There are more solutions. The general solution is:

$$x = -109472 + 93t \text{ and } y = 581570 - 494t \quad \text{for any integer } t \quad \text{Can you see why?}$$

See exercise 2

### EXERCISE 1

Find the highest common factor of 41325 and 5814

### SOLUTION 1

$$41325 = (7)(5814) + (627)$$

$$5814 = (9)(627) + (171)$$

$$627 = (3)(171) + (114)$$

$$171 = (1)(114) + (57)$$

$$114 = (2)(57) + (0) \quad \text{STOP}$$

$$d = 57$$

### EXERCISE 2

1) Oranges cost 23p and apples cost 17p. I buy some and the cost is 549p

How many oranges and how many apples did I buy?

Hint: If I buy  $x$  oranges and  $y$  apples then  $23x + 17y = 549$

2) In the following equations, we are looking for solutions where  $x, y$  are integers.

Why won't we find any?

a)  $7x = 43$    b)  $(x-3)^2 = 10$    c)  $4x = 2y+1$    d)  $2^x = 3^y$

e)  $6^x = 10^y$

## SOLUTIONS 2

$$1) \quad 23 = (1)(17) + (6)$$

$$17 = (2)(6) + (5)$$

$$6 = (1)(5) + (1)$$

$$5 = (5)(1) + 0 \quad \text{STOP}$$

$d=1$  (this was obvious as 23 and 17 are primes)

Working back up the page

$$1 = (6) + (-1)(5) \quad \text{But } (5) = (17) + (-2)(6)$$

$$1 = (-1)(17) + (3)(6) \quad \text{But } (6) = (23) + (-1)(17)$$

$$1 = (3)(23) + (-4)(17)$$

$$\text{So } (23)(3) + (17)(-4) = 1 \quad \text{multiplying by 549 gives}$$

$$(23)(1647) + (17)(-2196) = 549$$

We have a solution to our equation  $x = 1647$  and  $y = -2196$

So I buy 1647 oranges and -2196 apples

This is not a very practical solution.

The general solution is:  $x = 1647 - 17t$  and  $y = -2196 + 23t$

We want  $1647 - 17t \geq 0$  and  $-2196 + 23t \geq 0$

So  $t \leq 96.9$  and  $t \geq 95.5$  and remember  $t$  is an integer, so  $t = 96$

This gives  $x = 15$  and  $y = 12$

2)

- a) LHS is a multiple of 7 but RHS is not a multiple of 7
- b) No integer squared is equal to 10
- c) LHS is even but RHS is odd
- d) LHS is even but RHS is odd
- e) LHS is a multiple of 3 but the RHS is not a multiple of 3

## Prime Numbers

Theorems about prime numbers:

### 1. Euclid's theorem

There are an infinite number of prime numbers

Proof

Eric says  $2, 3, 5, 7, 11$  is a list of all the prime numbers.

But consider the number  $N = (2 \times 3 \times 5 \times 7 \times 11) + 1$

If  $N$  is prime, then Eric's list is not complete.

If  $N$  is not prime, then it is a multiple of primes. But  $N$  is not a multiple of 2, 3, 5, 7 or 11 so  $N$  is a multiple of some other primes. So Eric's list is not complete.

We can repeat this argument for any list that Eric can come up with. So it is impossible to write down a list of all the primes. So there must be an infinite number of primes.

### 2. We can find an arbitrarily long sequence of consecutive non-primes.

Proof

$6!$  is a multiple of 2, so  $2+6!$  is a multiple of 2.

$6!$  is a multiple of 3, so  $3+6!$  is a multiple of 3

...

$6!$  is a multiple of 6, so  $6+6!$  is a multiple of 6

So we have found a sequence of 5 consecutive non-primes.

In general:

$(2+n!), (3+n!), (4+n!), \dots, (n+n!)$  is a sequence of  $n-1$  consecutive non-primes for any positive integer  $n$

### 3. We cannot find an arithmetic sequence where all the terms are primes.

Proof

Here is an arithmetic sequence:  $7, 157, 307, 457, 607, 757, 907\dots$

The first seven terms are all primes.

Now:

$$a=7 \text{ and } d=150 \text{ and } u_n=7+(n-1)150$$

So:

$$u_8=7+(7)150 \text{ and this is a multiple of 7 and therefore not a prime.}$$

In general:

Consider the arithmetic sequence;  $a, a+d, a+2d, a+3d, \dots$

Now:

$u_n = a + (n-1)d$  so  $u_{a+1} = a + ad$  and this is a multiple of  $a$  and therefore not prime.

Note:

if  $a=1$  our proof does not work but if  $a=1$  then the first term of the arithmetic sequence is not prime.

Dirichlet's theorem:

If  $a$  and  $d$  have no common factor then the arithmetic sequence  $a, a+d, a+2d, a+3d, \dots$  will contain an infinite number of primes.

So the terms of  $7, 157, 307, 457, 607, 757, 907, \dots$  cannot all be prime, only an infinite number of them.

It is difficult to prove Dirichlet's theorem but we can prove that there are an infinite number of primes in the arithmetic sequence:

5, 9, 13, 17, 21, 23, ...

These are the integers of the form  $4k+3$

So we want to prove that there are an infinite number of primes of the form  $4k+3$

Before we start the proof:

All primes (except 2) are of the form  $4k+1$  or  $4k+3$

The product of primes of the form  $4k+1$  is also of this form because:

$$(4k+1)(4q+1) = \dots = 4(4kq+k+q)+1$$

Proof

Eric says  $3, 7, 11, 19, 23$  is a list of all the  $4k+3$  primes.

But consider the number  $N = 4(3 \times 7 \times 11 \times 19 \times 23) + 3$

$N$  is of the form  $4k+3$

If  $N$  is prime, then Eric's list is not complete.

If  $N$  is not prime, then it is a multiple of primes. But  $N$  is not a multiple of 3, 7, 11, 19 or 23 so  $N$  is a multiple of some other primes. If these other primes were all of the form  $4k+1$  then  $N$  would be of the form  $4k+1$  as we saw above. So at least one of these other primes must be of the form  $4k+3$ . So Eric's list is not complete.

We can repeat this argument for any list that Eric can come up with. So it is impossible to write down a list of all the  $4k+3$  primes. So there must be an infinite number of  $4k+3$  primes.

4.

$f(n) = n^2 - n + 41$  is prime for  $n = 1, 2, 3, \dots, 40$

and

$$f(n) = n^2 - 79n + 1601 \text{ is prime for } n=1, 2, 3, \dots, 79$$

But:

No quadratic polynomial  $f(n)$  with integer coefficients, is prime for all values of  $n$

Proof

$$f(n) = an^2 + bn + c \quad \text{where } a, b, c \text{ are integers}$$

$$f(1) = a+b+c \quad \text{let } q = a+b+c$$

$$f(q+1) = a(q+1)^2 + b(q+1) + c = \dots = q(aq + 2a + b + 1)$$

If  $q=0$  then  $f(1)=0$  and therefore not a prime.

If  $q=1$  then  $f(1)=1$  and therefore not a prime.

If  $q \geq 2$  then  $f(q+1)$  is a multiple of  $q$  and therefore not a prime.

In general:

No polynomial  $f(n)$  with integer coefficients, is prime for all values of  $n$

5. For every integer  $n \geq 1$  there is a prime  $p$  where  $n \leq p \leq 2n$

Proof – too difficult

6.  $x$  and  $n$  are positive integers

If  $x^n - 1$  is prime then  $x=2$

For example, when  $n=5$

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$$

So  $(x-1)$  is a factor of  $(x^5 - 1)$  so  $(x^5 - 1)$  cannot be prime unless  $(x-1)=1$  so  $x=2$

So we can see that if  $x \neq 2$  then  $x^n - 1$  is not prime.

Note: This does not mean, if  $x=2$  then  $x^n - 1$  is prime - try  $n=4$

7.  $n$  is a positive integer

If  $2^n - 1$  is prime then  $n$  is prime.

For example, when  $n=15$

$$2^{15} - 1 = (2^3)^5 - 1 = 8^5 - 1 \text{ and this is not prime by theorem 6.}$$

So we can see that if  $n$  is not prime then  $2^n - 1$  is not prime.

Note: This does not mean, if  $n$  is prime then  $2^n - 1$  is prime - try  $n=11$

Primes of the form  $2^n - 1$  are called Mersenne primes.

Some people like looking for large primes. Many of these are Mersenne primes, such as

$2^{82589933} - 1$  because there are short cuts to check if numbers of the form  $2^n - 1$  are prime, such as the Lucas – Lehmer test (look it up!)

8.  $x$  and  $n$  are positive integers

If  $x^n + 1$  is prime then  $n$  is even

For example, when  $n=5$

$$x^5 + 1 = (x+1)(x^4 - x^3 + x^2 - x + 1)$$

So  $(x+1)$  is a factor of  $(x^5 + 1)$  so  $(x^5 + 1)$  cannot be prime.

So we can see that if  $n$  is odd then  $x^n + 1$  is not prime.

Note: This does not mean, if  $n$  is even then  $x^n + 1$  is prime – try  $x=3$  and  $n=2$

9.  $n$  is a positive integer

If  $2^n + 1$  is prime then  $n = 2^k$  for some positive integer  $k$

For example, when  $n=28$

$$2^{28} + 1 = (2^4)^7 + 1 = 16^7 + 1 \text{ and this cannot be prime by theorem 8.}$$

So we can see that if  $n \neq 2^k$  then  $2^n + 1$  is not prime.

Note: this does not mean, if  $n = 2^k$  then  $2^n + 1$  is prime – try  $n=32$

Numbers of the form  $2^n + 1$  where  $n = 2^k$  are called Fermat numbers.

The first five Fermat numbers are all prime but the sixth Fermat number is 4,294,967,297 and Euler showed that this is not prime. In fact, no other Fermat primes have been discovered.

Conjectures about primes:

1. There are an infinite number of Mersenne primes.
2. There are an infinite number of Fermat primes.

3. There are an infinite number of Fibonacci primes.
4. There are an infinite number of prime pairs (primes like 17 and 19 that differ by 2).
5. For every positive integer  $n$  there is a prime  $p$  where  $n^2 < p < (n+1)^2$
6. There are infinitely many primes of the form  $n^2 + 1$  where  $n$  is a positive integer
7.  $2^k - 2$  is a multiple of  $k$  if and only if  $k$  is a prime number.

Actually this is not a conjecture. The statement is true for  $k=1, 2, 3, 4, \dots, 340$  but not for  $k=341$

### 8. The Goldbach conjecture

Every even integer, greater than 4, is the sum of two odd primes.

$$6 = 3 + 3 \quad 8 = 3 + 5 \quad 10 = 3 + 7 \quad \text{etc}$$

This is the most famous conjecture about primes. It arose in a letter Goldbach wrote to Euler in 1742. In 1931, Schnirelmann proved that every even integer, greater than 4, is the sum of no more than 300,000 primes, which is a start.

Incidentally, Goldbach had another conjecture:

Every odd positive integer, greater than 1, is a prime or the sum of a prime and twice a square.

$$9 = 7 + 2(1^2) \quad 15 = 7 + 2(2^2) \quad 21 = 3 + 2(3^2) \quad 25 = 7 + 2(3^2) \quad \text{etc}$$

We now know that this conjecture is false. The smallest counter-example is 5777.

## Modulo Arithmetic

Let's write the integers  $0, 1, 2, 3, 4, 5, 6, 7, \dots$  in four columns:

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
...	...	...	...

If  $n$  is in the 0 column then:

$$n=4k \text{ for some integer } k \text{ for example } 12=(4\times 3)$$

$n$  has remainder 0 when divided by 4

we say that  $n=0, \text{mod } 4$

If  $n$  is in the 1 column then:

$$n=4k+1 \text{ for some integer } k \text{ for example } 21=(4\times 5)+1$$

$n$  has remainder 1 when divided by 4

we say that  $n=1, \text{mod } 4$

If  $n$  is in the 2 column then:

$$n=4k+2 \text{ for some integer } k \text{ for example } 14=(4\times 3)+2$$

$n$  has remainder 2 when divided by 4

we say that  $n=2, \text{mod } 4$

If  $n$  is in the 3 column then:

$$n=4k+3 \text{ for some integer } k \text{ for example } 7=(4\times 1)+3$$

$n$  has remainder 3 when divided by 4

we say that  $n=3, \text{mod } 4$

If  $n$  and  $m$  are both in the  $r$  column then:

$$n=4s+r \text{ and } m=4t+r \text{ for some integers } s \text{ and } t$$

$n$  and  $m$  both have remainder  $r$  when divided by 4

$n-m$  is a multiple of 4

$$n=m+4k \text{ for some integer } k$$

we say that  $n \equiv m \pmod{4}$

I don't want to keep writing mod 4 so here is a shorthand. If you see:

mod 4:

...

end of mod 4

then everything in-between "mod 4" and "end of mod 4" will be in mod 4.

for example

mod 4:

$$16=0 \quad 13=1 \quad 22=2 \quad 15=3$$

$$20=12 \quad 17=9 \quad 22=6 \quad 23=19$$

end of mod 4

Looks weird but you'll get the hang of it.

mod 4:

$$23=7 \text{ and } 13=5$$

Check the following:

$$23+13=7+5$$

$$23-13=7-5$$

$$23\times 13=7\times 5$$

$$23^2=7^2$$

$$23+147=13+147$$

$$147\times 23=147\times 13$$

end of mod 4

In general:

mod 4:

If  $a=A$  and  $b=B$  then the following six rules apply:

$$\text{rule 1} \quad a+b=A+B$$

$$\text{rule 2} \quad a-b=A-B$$

rule 3             $ab = A B$   
 rule 4             $a^n = A^n$  for any integer  $n$   
 rule 5             $a+n = A+n$  for any integer  $n$   
 rule 6             $na = nA$  for any integer  $n$   
 end of mod 4

### Proof of rule 1

$$\begin{aligned}
 a &= A \text{ mod } 4 \text{ so } a = A + 4k \text{ for some integer } k \\
 b &= B \text{ mod } 4 \text{ so } b = B + 4l \text{ for some integer } l \\
 a+b &= (A+4k)+(B+4l) = (A+B)+4(k+l) \text{ So } a+b = A+B \text{ mod } 4
 \end{aligned}$$

You can prove rules 2 to 6 in the same way.

What about division?

rule 7 – the cancellation rule

If  $3p = 3q \text{ mod } 4$  then  $3p = 3q + 4k$  for some integer  $k$   
 So  $3p - 3q = 4k$  so  $3(p-q) = 4k$  so  $3(p-q)$  is a multiple of 4

In the chapter: Fundamental Theorem of Arithmetic we saw that:

If  $n$  and  $r$  have no common factor then:

$nm$  is a multiple of  $r$  only if  $m$  is a multiple of  $r$

3 and 4 have no common factor so:

$3m$  is a multiple of 4 only if  $m$  is a multiple of 4

Now  $3(p-q)$  is a multiple of 4 so  $(p-q)$  is a multiple of 4

So  $p = q \text{ mod } 4$

mod 4:

In general:

If  $np = nq$  then  $p = q$  provided  $n$  and 4 have no common factor.

This is the nearest we are going to get to doing division.

$$15 = 39$$

we can divide both sides by 3 (note: 3 and 4 do not have a common factor)

$$5 = 13$$

But

$$10 = 34$$

we cannot divide both sides by 2 (note: 2 and 4 do have a common factor)

$$5 \neq 17$$

end of mod 4

We must be careful and stick to our 7 rules.

For example  $5^2 = 7^2$  but  $5 \neq 7$  etc

We can extend these ideas to include negative integers

for example,  $-17 = -20 + 3 = (4 \times -5) + 3 = 3, \text{mod } 4$

Everything we have said about mod 4 applies to mod 2, mod 3 etc

So what is the point of all this? Well, it can make proving some results a lot easier.

Example 1

No square is of the form  $3k+2$

Proof

mod 3:

$$x=0, 1, 2 \text{ so } x^2=0, 1 \text{ so } x^2 \neq 2$$

end of mod 3

Get it? Here is some more explanation:

$x=0, 1, 2$  means that if  $x$  is any integer then:

$$x=0, \text{mod } 3 \text{ or } x=1, \text{mod } 3 \text{ or } x=2, \text{mod } 3$$

If  $x=0, \text{mod } 3$  then  $x^2=0^2=0, \text{mod } 3$

If  $x=1, \text{mod } 3$  then  $x^2=1^2=1, \text{mod } 3$

If  $x=2, \text{mod } 3$  then  $x^2=2^2=4=1, \text{mod } 3$

So  $x^2=0, \text{mod } 3$  or  $x^2=1, \text{mod } 3$

So

$x^2 \neq 2, \text{mod } 3$  so  $x^2$  cannot be of the form  $3k+2$

Example 2

Show that the last digit of a square cannot be 2, 3, 7 or 8

Before we do the proof ...

for any positive integer, say 127, we can write:

$$127=120+7=(10 \times 12)+7=7, \text{mod } 10$$

In general

mod 10:

$$n = \text{last digit of } n$$

end of mod 10

Proof

mod 10:

$$x=0,1,2,3,4,5,6,7,8,9 \text{ so } x^2=0,1,4,5,6,9 \text{ so } x^2 \neq 2,3,7,8$$

end of mod 10

Example 3

No integer of the form  $4k+2$  is the difference of two squares.

Proof

mod 4:

$$a=0,1,2,3 \text{ so } a^2=0,1 \text{ and } b=0,1,2,3 \text{ so } b^2=0,1 \text{ so } a^2-b^2=0,1,3 \text{ so } a^2-b^2 \neq 2$$

end of mod 4

see Exercise

If you don't think that mod arithmetic is a brilliant idea, then do this Exercise without it.

## EXERCISE

Show that:

1. No square is of the form  $4k+2$  or  $4k+3$  Hint: mod 4
2. Every odd square is of the form  $8k+1$  Hint: mod 8
3. If  $x$  and  $y$  are odd integers then  $x^2-y^2$  is a multiple of 8 Hint: see(2)
4. No even square is the sum of two odd squares Hint: mod 4
5. The sum of two consecutive squares is one more than a multiple of 4 Hint: mod 4
6. Every cube is of the form  $9k$ ,  $9k+1$  or  $9k+8$  Hint: mod 9
7. The sum of three consecutive cubes is a multiple of 9. Hint: mod 9
8. The sum of 3 squares cannot be of the form  $8k+7$  Hint: mod 8
9. No cube is of the form  $4k+2$  Hint: mod 4
10.  $x^4+y^4=z^4+4$  has no integer solution. Hint: mod 8
11.  $x^3-x$  is a multiple of 6 for any integer  $x$  Hint: mod 6
12. If  $x$  is an integer and not a multiple of 2 or 3 then  $x^2-1$  is a multiple of 24

Hint: mod 24

13. If  $p$  is a prime greater than 3 then  $p^2+2$  is a multiple of 3

Hint: mod 3

14. Every prime (except 2 and 3) is of the form  $6k+1$  or  $6k+5$

Hint: mod 6

## SOLUTIONS

1) mod 4:

$x=0,1,2,3$  so  $x^2=0,1$  so  $x^2 \neq 2,3$

end of mod 4

2) mod 8:

if  $x$  is odd then  $x=1,3,5,7$  so  $x^2=1$

end of mod 8

3) mod 8:

if  $x$  is odd then  $x=1,3,5,7$  so  $x^2=1$

if  $y$  is odd then  $y=1,3,5,7$  so  $y^2=1$

so  $x^2-y^2=0$

end of mod 8

4) mod 4:

if  $x$  is even then  $x=0,2$  so  $x^2=0$

if  $y$  is odd then  $y=1,3$  so  $y^2=1$

if  $z$  is odd then  $z=1,3$  so  $z^2=1$

so  $x^2 \neq y^2+z^2$

end of mod 4

5) mod 4:

$x$	0	1	2	3
$y$	1	2	3	0
$x^2$	0	1	0	1
$y^2$	1	0	1	0
$x^2+y^2$	1	1	1	1

end of mod 4

6) mod 9:

$x=0,1,2,3,4,5,6,7,8$  so  $x^3=0,1,8$

end of mod 9

7) mod 9:

$x$	0	1	2	3	4	5	6	7	8
$y$	1	2	3	4	5	6	7	8	0
$z$	2	3	4	5	6	7	8	0	1
$x^3$	0	1	8	0	1	8	0	1	8
$y^3$	1	8	0	1	8	0	1	8	0
$z^3$	8	0	1	8	0	1	8	0	1
$x^3 + y^3 + z^3$	9	9	9	9	9	9	9	9	9

end of mod 9

8) mod 8:

$$x=0,1,2,3,4,5,6,7 \text{ so } x^2=0,1,4$$

$$y=0,1,2,3,4,5,6,7 \text{ so } y^2=0,1,4$$

$$z=0,1,2,3,4,5,6,7 \text{ so } z^2=0,1,4$$

$$x^2 + y^2 + z^2 = 0,1,2,3,4,5,6 \text{ so } x^2 + y^2 + z^2 \neq 7$$

end of mod 8

9) mod 4:

$$x=0,1,2,3 \text{ so } x^3=0,1,3 \text{ so } x^3 \neq 2$$

end of mod 4

10) mod 8:

$$x=0,1,2,3,4,5,6,7 \text{ so } x^4=0,1$$

$$y=0,1,2,3,4,5,6,7 \text{ so } y^4=0,1$$

$$x^4 + y^4 = 0,1,2$$

$$z=0,1,2,3,4,5,6,7 \text{ so } z^4=0,1 \text{ so } z^4+4=5,6$$

$$\text{so } x^4 + y^4 \neq z^4 + 4$$

end of mod 8

11) mod 6

$x$	0	1	2	3	4	5
$x^3$	0	1	2	3	4	5

$$x^3 - x = 0$$

end of mod 6

12) mod 24:

if  $x$  is not a multiple of 2 or 3 then  $x=1,5,7,11,13,17,19,23$  so  $x^2=1$  so  $x^2 - 1 = 0$

end of mod 24

13) mod 3:

if  $p$  is a prime greater than 3 then  $p=1, 2$  so  $p^2=1$  so  $p^2+2=3=0$

end of mod 3

14)

$p$  is a prime greater than 3

if  $p \equiv 0 \pmod{6}$  then  $p$  is a multiple of 6

if  $p \equiv 2 \pmod{6}$  then  $p$  is a multiple of 2

if  $p \equiv 3 \pmod{6}$  then  $p$  is a multiple of 3

if  $p \equiv 4 \pmod{6}$  then  $p$  is a multiple of 2

so  $p \equiv 1, 5 \pmod{6}$

## Chinese Remainder Theorem

I have a large bag of sweets. If I share them equally among my 10 children there are 2 sweets left over. If I share them equally among my 7 grandchildren there are 3 sweets left over. How many sweets are in my bag?

If there are  $x$  sweets in the bag then  $x=2, \text{mod } 10$  and  $x=3, \text{mod } 7$

### Theorem

This problem has a unique solution for  $x=1, 2, \dots, 70$

Proof (by contradiction)

Assume there are two solutions  $x=p$  and  $x=q$

$$p=2, \text{mod } 10 \quad p=3, \text{mod } 7$$

$$q=2, \text{mod } 10 \quad q=3, \text{mod } 7$$

Say  $p > q$

$$p=2, \text{mod } 10 \quad q=2, \text{mod } 10$$

So  $p=q+10m$  for some positive integer  $m$

$$p=3, \text{mod } 7 \quad q=3, \text{mod } 7$$

So  $p=q+7n$  for some positive integer  $n$

So  $q+10m=q+7n$  so  $10m=7n$

So  $10m$  is a multiple of 7

But 10 and 7 have no common factor so  $m$  is a multiple of 7

So  $m=7k$  for some positive integer  $k$

So:

$$p=q+10m \quad m=7k$$

So  $p=q+70k$

But:

$$1 \leq p \leq 70 \quad 1 \leq q \leq 70$$

Contradiction!

In general:

The simultaneous equations:

$$x=a, \text{mod } m \quad x=b, \text{mod } n \quad \text{where } m \text{ and } n \text{ have no common factor}$$

have a unique solution for  $x=1,2,\dots mn$

A tedious method to find this solution:

$$x \equiv 2 \pmod{10} \text{ so } x = 2, 12, 22, 32, 42, 52, 62$$

$$x \equiv 3 \pmod{7} \text{ so } x = 3, 10, 17, 24, 31, 38, 45, 52, 59, 66$$

This gives the solution  $x=52$

Note:

The smallest number of sweets I could have in my bag is 52.

But I could have  $52+70L$  sweets in my bag where  $L$  is any positive integer.

Can you see why?

## Fermat's Last Theorem

A primitive Pythagorean triple is a set of three positive integers  $x, y, z$  where:

$$x^2 + y^2 = z^2 \text{ and } x, y, z \text{ have no common factor.}$$

for example:

5,12,13

### Theorem

All primitive Pythagorean triples are of the form:

$$x=2pq \quad y=p^2-q^2 \quad z=p^2+q^2$$

where  $p$  and  $q$  are any positive integers such that:

$$p > q$$

$p$  and  $q$  have no common factor

$p$  and  $q$  are not both odd

$p$  and  $q$  are not both even

for example  $p=7$  and  $q=4$  gives  $x=56$   $y=33$   $z=65$

### Proof(?)

We can easily check that:

$$(2pq)^2 + (p^2 - q^2)^2 = (p^2 + q^2)^2$$

But this does not prove that all primitive Pythagorean triples are of this form. Why not?

### See Exercise

## Fermat's Last Theorem:

There is no set of three positive integers  $x, y, z$  where:

$$x^3 + y^3 = z^3 \text{ or } x^4 + y^4 = z^4 \text{ or } x^5 + y^5 = z^5 \dots \text{etc}$$

Fermat had the annoying habit of announcing theorems that he had discovered but not providing proofs. It was left to later mathematicians (Euler usually) to supply the proofs. Fermat's last theorem (1637) was the last of these theorems to be proved (1995)

### EXERCISE

Prove the following about primitive Pythagorean triples.

- 1)  $x$  and  $y$  can't both be even hint: mod 2
- 2)  $x$  and  $y$  can't both be odd hint: mod 4
- 3)  $z$  is odd

- |   |              |
|---|--------------|
| 4) $x$ or $y$ is a multiple of 3        | hint: mod 3  |
| 5) $x$ or $y$ is a multiple of 4        | hint: mod 16 |
| 6) $x$ or $y$ or $z$ is a multiple of 5 | hint: mod 5  |
| 7) $xyz$ is a multiple of 60            |              |

## SOLUTIONS

1) proof by contradiction

assume  $x$  and  $y$  are both even

mod 2:

$$x=0 \text{ so } x^2=0$$

$$y=0 \text{ so } y^2=0$$

$x^2+y^2=z^2$  so  $z^2=0$  so  $z=0$  so  $x, y, z$  are all even so  $x, y, z$  have a common factor

Contradiction

end of mod 2

2) proof by contradiction

assume  $x$  and  $y$  are both odd

mod 4:

$$x=1,3 \text{ so } x^2=1$$

$$y=1,3 \text{ so } y^2=1$$

$x^2+y^2=z^2$  so  $z^2=2$  but if  $z=0, 1, 2, 3$  then  $z^2=0, 1$

Contradiction

end of mod 4

3) parts (1) and (2) tell us that  $x^2+y^2$  is odd so  $z^2$  is odd so  $z$  is odd

4) proof by contradiction

assume neither  $x$  nor  $y$  is a multiple of 3

mod 3:

$$x=1,2 \text{ so } x^2=1$$

$$y=1,2 \text{ so } y^2=1$$

$x^2+y^2=z^2$  so  $z^2=2$  but if  $z=0, 1, 2$  then  $z^2=0, 1$

Contradiction

end of mod 3

5) proof by contradiction

assume neither  $x$  nor  $y$  is a multiple of 4

mod 16:

$x=1,2,3,5,6,7,9,10,11,13,14,15$  so  $x^2=1,4,9$

$y=1,2,3,5,6,7,9,10,11,13,14,15$  so  $y^2=1,4,9$

$x^2+y^2=z^2$  so  $z^2=2,5,8,10,13$

but if  $Z=0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15$  then  $z^2=0,1,4,9$

Contradiction

end of mod 16

6) proof by contradiction

assume neither  $x$  nor  $y$  nor  $z$  is a multiple of 5

mod 5:

$x=1,2,3,4$  so  $x^2=1,4$

$y=1,2,3,4$  so  $y^2=1,4$

$x^2+y^2=z^2$  so  $z^2=0,2,3$  but if  $z=1,2,3,4$  then  $z^2=1,4$

Contradiction

end of mod 5

7) this follows from parts (4), (5) and (6)

## Fermat's Little Theorem

### Theorem

$n^7 - n$  is a multiple of 7, for  $n=1, 2, 3, \dots$

for example  $153^7 - 153$  is a multiple of 7

### Proof (by induction)

part 1:

If  $n=1$  then  $n^7 - n = 0$

So  $n^7 - n$  is a multiple of 7 when  $n=1$

part 2:

If  $n^7 - n$  is a multiple of 7 when  $n=k$  then:

$k^7 - k$  is a multiple of 7, so  $k^7 - k = 7r$  for some integer  $r$

$$\text{Now } (k+1)^7 - (k+1) = (k^7 + 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k + 1) - (k+1)$$

$$\text{So } (k+1)^7 - (k+1) = (k^7 - k) + (7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k)$$

$$\text{So } (k+1)^7 - (k+1) = 7r + 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k)$$

So  $(k+1)^7 - (k+1)$  is a multiple of 7

So  $n^7 - n$  is a multiple of 7 when  $n=k+1$

Note: our proof worked because the coefficients in the binomial theorem: 7, 21, 35, 35, 21, 7 are all multiples of 7

$$\text{A typical coefficient is: } (7C3) = \frac{7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1}{(3 \times 2 \times 1)(4 \times 3 \times 2 \times 1)}$$

After lots of cancelling, we are left with a positive integer. The 7 on the top of the fraction can't be cancelled out by numbers on the bottom of the fraction because 7 is prime. So  $(7C3)$  must be a multiple of 7

In general:

If  $p$  is prime then all the coefficients in the expansion of  $(k+1)^p$  will be a multiple of  $p$  (apart from the 1's at each end)

In general:

Fermat's Little Theorem (FLT) for prime number  $p$  and  $n=1, 2, 3, \dots$

$n^p - n$  is a multiple of  $p$

We can prove this for prime number  $p$  as we proved it above for prime number 7

Now:

$n^7 - n$  is a multiple of 7, so  $n(n^6 - 1)$  is a multiple of 7

So:

if  $n$  is not a multiple of 7 then  $n^6 - 1$  is a multiple of 7

So we can rephrase:

Fermat's Little Theorem (FLT) for prime number  $p$  and  $n=1,2,3,\dots$

$n^{(p-1)} - 1$  is a multiple of  $p$  provided  $n$  is not a multiple of  $p$

We can rephrase using mod arithmetic:

Fermat's Little Theorem (FLT) for prime number  $p$  and  $n=1,2,3,\dots$

$n^p - n \equiv 0 \pmod{p}$  so  $n^p \equiv n \pmod{p}$

Or:

$n^{(p-1)} - 1 \equiv 0 \pmod{p}$  so  $n^{(p-1)} \equiv 1 \pmod{p}$  provided  $n$  is not a multiple of  $p$

We will now use FLT to evaluate expressions of the form  $a^b \pmod{p}$  where  $p$  is prime.

Such expressions can be tricky to evaluate if  $a$  is large or  $b$  is large. Luckily there are two theorems that can help us.

Theorem

If  $a \equiv A \pmod{p}$  then  $a^n \equiv A^n \pmod{p}$  where  $n=1,2,3,\dots$

(this theorem is true whether  $p$  is prime or not)

for example  $273 \equiv 3 \pmod{5}$  so  $273^{24} \equiv 3^{24} \pmod{5}$

Proof

See section, Modular Arithmetic

Theorem

If  $a \equiv A \pmod{p-1}$  then  $a^n \equiv A^n \pmod{p}$  where  $n=1,2,3,\dots$  and  $n$  is not a multiple of  $p$

(this theorem is only true if  $p$  is prime)

for example  $387 \equiv 3 \pmod{4}$  so  $97^{387} \equiv 97^3 \pmod{5}$

Proof

We will show that:

$153 \equiv 3 \pmod{6}$  so  $n^{153} \equiv n^3 \pmod{7}$

You can prove the general result in the same way.

$$n^6 \equiv 1 \pmod{7} \text{ from FLT}$$

where  $n=1, 2, 3, \dots$  and  $n$  is

not a multiple of  $p$

So

$$n^{153} = n^{(6 \times 25) + 3} = n^{(6 \times 25)} \times n^3 = (n^6)^{25} \times n^3 = 1^{25} \times n^3 = 1 \times n^3 = n^3 \pmod{7}$$

Example

$$\text{Evaluate } 2518^{10} \pmod{17}$$

Now:

$$2518 \equiv 2 \pmod{17} \text{ so } 2518^{10} \equiv 2^{10} \pmod{17}$$

And:

$$2^{10} = 1024 \equiv 4 \pmod{17}$$

Example

$$\text{Evaluate } 3^{220} \pmod{19}$$

Now:

$$220 \equiv 4 \pmod{18} \text{ so } 3^{220} \equiv 3^4 \pmod{19}$$

And:

$$3^4 = 81 \equiv 5 \pmod{19}$$

Example

$$\text{Evaluate } 875^{302} \pmod{13}$$

Now:

$$875 \equiv 4 \pmod{13} \text{ so } 875^{302} \equiv 4^{302}$$

Now:

$$302 \equiv 2 \pmod{12} \text{ so } 4^{302} \equiv 4^2 \pmod{13}$$

And:

$$4^2 = 16 \equiv 3 \pmod{13}$$

We will now use FLT to find the last digit of numbers of the form  $a^b$

Note:

$$\text{If } N = 32748 \text{ then } N = 32740 + 8 = (3274 \times 10) + 8 \text{ so } N \equiv 8 \pmod{10}$$

Finding the last digit of  $N$  is the same as finding  $N \pmod{10}$

Note:

If  $N \equiv 7 \pmod{10}$  then  $N = 10k + 7$  for some positive integer  $k$

So:

$$N = 2(5k + 3) + 1 \text{ so } N \equiv 1 \pmod{2}$$

And:

$$N = 5(2k + 1) + 2 \text{ so } N \equiv 2 \pmod{5}$$

We can repeat these calculations for  $N = 1, 2, 3, 4, 5, 6, 8, 9 \pmod{10}$  to get this table.

$N \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$N \pmod{2}$	0	1	0	1	0	1	0	1	0	1
$N \pmod{5}$	0	1	2	3	4	0	1	2	3	4

So if we know  $N \pmod{2}$  and  $N \pmod{5}$  we can find  $N \pmod{10}$

for example, if  $N \equiv 0 \pmod{2}$  and  $N \equiv 3 \pmod{5}$  then  $N \equiv 8 \pmod{10}$

Example

Find the last digit of  $13^{270}$

$\pmod{2}$

$13^{270}$  is odd so  $13^{270} \equiv 1 \pmod{2}$

$\pmod{5}$

a)  $13 \equiv 3 \pmod{5}$  so  $13^{270} \equiv 3^{270} \pmod{5}$

b)  $270 = 2 \cdot 135$  so  $3^{270} \equiv 3^2 \equiv 9 \equiv 4 \pmod{5}$

iii) Now  $13^{270} \equiv 1 \pmod{2}$  and  $13^{270} \equiv 4 \pmod{5}$  so from the table  $13^{270} \equiv 9 \pmod{10}$

So the last digit of  $13^{270}$  is 9

In 1640, Fermat announced FLT. In 1978, Rivest, Shamir and Adleman announced the RSA encryption system. RSA encryption relies on FLT. It has many applications. For example, it enables us to buy stuff online.

See chapter: Encryption

see Exercise

Another proof of FLT

Show that

$$(a+b)^7 - (a^7 + b^7)$$
 is a multiple of 7

Show that

$$(a+b+c)^7 - (a^7 + b^7 + c^7)$$
 is a multiple of 7

Show that

$$(a+b+c+d+\dots)^7 - (a^7 + b^7 + c^7 + d^7 + \dots)$$
 is a multiple of 7

If there are  $n$  numbers  $a, b, c, d, \dots$  and we set them all equal to 1 then

$$n^7 - n$$
 is a multiple of 7

etc

Yet another proof of FLT

Take any number from  $1, 2, 3, 4, 5, 6$  and write down its first six multiples

for example, take the number 3

$$1 \times 3 = 3, \text{mod } 7 \quad 2 \times 3 = 6, \text{mod } 7 \quad 3 \times 3 = 2, \text{mod } 7$$

$$4 \times 3 = 5, \text{mod } 7 \quad 5 \times 3 = 1, \text{mod } 7 \quad 6 \times 3 = 4, \text{mod } 7$$

These multiples are just  $1, 2, 3, 4, 5, 6$  in a different order.

Hint: If  $n \times 3 = m \times 3$  then  $n = m$  Why?

$$\text{So } (1 \times 3) \times (2 \times 3) \times (3 \times 3) \times (4 \times 3) \times (5 \times 3) \times (6 \times 3) = 1 \times 2 \times 3 \times 4 \times 5 \times 6$$

$$\text{So } 1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 3^6 = 1 \times 2 \times 3 \times 4 \times 5 \times 6$$

$$3^6 = 1, \text{mod } 7$$

etc

## EXERCISE

1) Show that:

$$n^5 - n$$
 is a multiple of 10 for  $n = 1, 2, 3, \dots$

2) Find:

$$7465^5, \text{mod } 7$$

3) Find:

$$18^{163}, \text{mod } 41$$

4) Find the last digit of:

$$8^{154}$$

## SOLUTIONS

1) 10 is not prime so we cannot use FLT directly, but ...

$n^5 - n$  is a multiple of 5 by FLT

If  $n$  is even then  $n^5 - n$  is a multiple of 2

If  $n$  is odd then  $n^5 - n$  is a multiple of 2

Either way  $n^5 - n$  is a multiple of 2 and a multiple of 5 and hence a multiple of 10.

2)  $7465 \equiv 3 \pmod{7}$  so  $7465^5 \equiv 3^5 \equiv 243 \equiv 5 \pmod{7}$

3)  $163 \equiv 3 \pmod{40}$  so  $18^{163} \equiv 18^3 \equiv 5832 \equiv 10 \pmod{41}$

4)

i) mod 2

a)  $8^{154}$  is even so  $8^{154} \equiv 0 \pmod{2}$

ii) mod 5

a)  $8 \equiv 3 \pmod{5}$  so  $8^{154} \equiv 3^{154} \pmod{5}$

b)  $154 \equiv 2 \pmod{4}$  so  $3^{154} \equiv 3^2 \equiv 9 \equiv 4 \pmod{5}$

iii) from the table

$8^{154} \equiv 4 \pmod{10}$  so the last digit of  $8^{154}$  is 4

## Card Shuffles

I put a pack of eight cards on the table. The top card has an A written on it. The next card has a B written on it, etc

I pick up the top half of the pack, A, B, C, D in my right hand.

I pick up the bottom half of the pack, E, F, G, H in my left hand.

Then I do a riffle shuffle:

I drop the D card from my right hand onto the table, then the H card from my left hand, then the C card from my right hand, then the G card from my left hand, then the B card from my right hand, then the F card from my left hand, then the A card from my right hand, then the E card from my left hand.

The cards are now in the order E, A, F, B, G, C, H, D with the E on the top of the pile. Try it.

Then I shuffle again and again until the cards are back in their original order.

So how have the cards moved?

Order at start	A	B	C	D	E	F	G	H
Order after one shuffle	E	A	F	B	G	C	H	D
Order after two shuffles	G	E	C	A	H	F	D	B
Order after three shuffles	H	G	F	E	D	C	B	A
Order after four shuffles	D	H	C	G	B	F	A	E
Order after five shuffles	B	D	F	H	A	C	E	G
Order after six shuffles	A	B	C	D	E	F	G	H

So the cards are back in their original order after six shuffles.

It will be helpful to look at the position of each card in the pack. Position 1 is the top card etc

Card	A	B	C	D	E	F	G	H
Position at start	1	2	3	4	5	6	7	8
Position after one shuffle	2	4	6	8	1	3	5	7
Position after two shuffles	4	8	3	7	2	6	1	5
Position after three shuffles	8	7	6	5	4	3	2	1
Position after four shuffles	7	5	3	1	8	6	4	2
Position after five shuffles	5	1	6	2	7	3	8	4
Position after six shuffles	1	2	3	4	5	6	7	8

You can check that:

After 1 shuffle, the card starting in position  $m$  will end up in position  $2m \bmod 9$

After 2 shuffles, the card starting in position  $m$  will end up in position  $(2 \times 2)m \bmod 9$

After 3 shuffles, the card starting in position  $m$  will end up in position  $(2 \times 2 \times 2)m \bmod 9$

...

After  $k$  shuffles, the card starting in position  $m$  will end up in position  $2^k m \bmod 9$

If  $2^k m = m \bmod 9$  for  $m=1,2,\dots,8$  then after  $k$  shuffles, the card starting in position  $m$  will end up in position  $m$ . So the cards are back in their original order.

Now  $2^6 = 1 \bmod 9$ . You can check this.

So  $2^6 \times 1 = 1 \bmod 9$  and  $2^6 \times 2 = 2 \bmod 9$  and  $2^6 \times 3 = 3 \bmod 9$  and ...  $2^6 \times 8 = 8 \bmod 9$

So the pack of 8 cards will be back in their original order after 6 shuffles.

In general:

Take a pack of  $N$  cards:

If  $2^k = 1 \bmod (N+1)$  then the cards will be back in their original order after  $k$  shuffles.

We know from Fermat's little theorem that:

$$2^{(p-1)} = 1 \bmod p \quad \text{provided } p \neq 2$$

So:

Take a pack of  $p-1$  cards: where  $p$  is a prime number

Now  $2^{(p-1)} = 1 \bmod p$  so the cards will be back in their original order after  $p$  shuffles.

A pack of 52 cards will be back in its original order after 52 shuffles, because 53 is prime.

## Casting-out Nines

Now:

$$8263 = (8 \times 1000) + (2 \times 100) + (6 \times 10) + (3)$$

So:

$$8263 = (8 \times 999) + (2 \times 99) + (6 \times 9) + (8+2+6+3)$$

So:

$$8263 = (9 \times \dots) + (8+2+6+3)$$

So:

$$8263 = 8+2+6+3, \text{mod } 9$$

So to find  $N, \text{mod } 9$  we just add up the digits of  $N$

If you do an addition, subtraction or multiplication then the answer must be correct in mod 9.

### Example 1

Eric says  $123+35=157$

mod 9:

$$LHS = 123+35 = (1+2+3) + (3+5) = 6+8+14 = 5$$

$$RHS = 157 = 1+5+7 = 13 = 4$$

end of mod 9

So Eric's answer must be incorrect.

### Example 2

Eric says  $3647 \times 7298 = 26615797$

mod 9:

$$LHS = 3647 \times 7298 = (3+6+4+7) \times (7+2+9+8) = 20 \times 26 = 2 \times 8 = 16 = 7$$

$$RHS = 26615797 = 2+6+6+1+5+7+9+7 = 43 = 7$$

end of mod 9

Be careful. We have not shown that Eric's answer must be correct.

We have shown that Eric's answer is either correct or out by a multiple of 9

## Perfect Numbers

### Example 1

The factors of 28 are:

$$1, 2, 4, 7, 14 \quad \text{Note: we have included 1 as a factor but not 28}$$

The sum of the factors of 28 is:

$$1+2+4+7+14=28$$

So 28 equals the sum of its factors. So 28 is a perfect number.

### Example 2

The factors of  $(2^6 p)$  where  $p$  is an odd prime, are:

$$\begin{array}{ccccccc} 1 & & 2 & & 2^2 & & 2^3 \\ p & & 2p & & 2^2 p & & 2^3 p \\ & & & & 2^4 p & & 2^5 p \\ & & & & & & 2^6 \end{array}$$

The sum of the factors of  $(2^6 p)$  is:

$$(1+2+2^2+2^3+2^4+2^5+2^6)+p(1+2+2^2+2^3+2^4+2^5)$$

but:

$$(1+2+2^2+2^3+2^4+2^5+2^6)=2^7-1 \quad \text{a geometric series}$$

and:

$$(1+2+2^2+2^3+2^4+2^5)=2^6-1 \quad \text{a geometric series}$$

So the sum of the factors of  $(2^6 p)$  is:

$$(2^7-1)+p(2^6-1)$$

If:

$$p=2^7-1$$

then:

the sum of the factors of  $(2^6 p)$  is:

$$(2^7-1)+(2^7-1)(2^6-1)=(2^7-1)(1+(2^6-1))=(2^7-1)2^6=2^6 p$$

So  $(2^6 p)$  is a perfect number.

Euclid's theorem:

If  $2^k-1$  is prime then  $2^{k-1}(2^k-1)$  is an even perfect number.

for example:

$2^5-1$  is prime so  $2^4(2^5-1)$  is an even perfect number.

Euler's theorem:

All even perfect numbers are of the form  $2^{k-1}(2^k - 1)$  where  $2^k - 1$  is prime

This is much more difficult to prove.

### Theorem

All even perfect numbers are triangle numbers

### Proof

$$2^{k-1}(2^k - 1) = 2^k 2^{-1}(2^k - 1) = \frac{1}{2}(2^k - 1)(2^k) \text{ which is of the form } \frac{1}{2}n(n+1)$$

A conjecture about even perfect numbers:

there are an infinite number of even perfect numbers

### Theorem

No odd perfect number is prime

### Proof

If  $p$  is prime then its only factor is: 1

If  $p$  is perfect then  $1=p$  and this can't happen

### Theorem

No odd perfect number is a square

### Proof

Factors come in pairs (except for 1)

The factors of 24 are:

1            2 and 12            3 and 8            4 and 6

So every integer has an odd number of factors. No!

The factors of 36 are:

1            2 and 18            3 and 12            4 and 96            6

36 has an even number of factors because 36 is a square

So all squares have an even number of factors and all other integers have an odd number of factors.

225 is an odd square

225 has an even number of factors:

1            3 and 75            5 and 45            9 and 25            15

All the factors of 225 are odd. So the sum of the factors of 225 is even.

So 225 is odd but the sum of its factors is even. So 225 cannot be perfect.

All this applies to any odd square. So no odd square is perfect.

A conjecture about odd perfect numbers:

odd perfect numbers do not exist

Amicable pairs

The factors of 220 are:

1,2,4,5,10,11,20,22,44,55,110

and:

$$1+2+4+5+10+11+20+22+44+55+110=284$$

The factors of 284 are:

1,2,4,71,142

and

$$1+2+4+71+142=220$$

We say 220 and 284 are an amicable pair.

Pythagoras(?) discovered the amicable pair: 220 and 284

Fermat discovered the amicable pair: 17296 and 18416

Descartes discovered the amicable pair: 9363584 and 9437056

Euler then discovered another sixty amicable pairs!

They all missed the pair, 1184 and 1210 which was not discovered until 1866 (by a 16 year old)

## Sums of Squares

Some integers are the sum of two squares, for example:

$$58=3^2+7^2 \text{ and } 64=0^2+8^2$$

Some integers are not the sum of two squares, for example:

$$7 \text{ and } 15$$

We want to know which integers are the sum of two squares and which are not.

### Theorem

If  $m$  and  $n$  are both the sum of two squares then  $mn$  is the sum of two squares.

### Proof

$$m=a^2+b^2 \text{ and } n=c^2+d^2$$

$$mn=\dots=(ac+bd)^2+(ad-bc)^2$$

This also means that if  $m$  is the sum of two squares then any positive power of  $m$  is the sum of two squares.

### Theorem

2 is the sum of two squares

### Proof

$$2=1^2+1^2$$

### Theorem

No integer of the form  $4k+3$  is the sum of two squares

### Proof

mod 4:

$$x=0,1,2,3 \text{ so } x^2=0,1 \text{ and } y=0,1,2,3 \text{ so } y^2=0,1$$

$$\text{so } x^2+y^2=0,1,2 \text{ so } x^2+y^2 \neq 3$$

end of mod 4

So an integer of the form  $4k+3$  cannot be the sum of two squares.

All primes (except 2) are of the form  $4k+1$  or  $4k+3$

We have just proved that no prime of the form  $4k+3$  is the sum of two squares.

Fermat proved that every prime of the form  $4k+1$  is the sum of two squares.

### Theorem

Every even power of an integer is the sum of two squares

Proof

$$6^{10} = (6^5)^2 + 0^2 \text{ etc}$$

We can write any integer  $n$  in the form:

$$n = (2^a)(3^b)(5^c)(7^d)(11^e)(\dots)$$

2 is the sum of two squares

So  $(2)^a$  is the sum of two squares.

5, 13, 17, ... are all of the form  $4k+1$

So 5, 13, 17, ... are all the sum of two squares.

So  $(5)^c, (13)^f, (17)^g, \dots$  are all the sum of two squares.

3, 7, 11, ... are all of the form  $4k+3$

So 3, 7, 11, ... are not the sum of two squares.

But  $(3)^b, (7)^d, (11)^e, \dots$  are all the sum of two squares if  $b, d, e, \dots$  are all even.

So  $n$  is the sum of two squares if all the powers of all the  $4k+3$  primes are even.

So  $(2^5)(3^{10})(5^{14})(7^2)(11^{24})(13^3)(17^1)$  is the sum of two squares

It turns out that:

$n$  is the sum of two squares if and only if all the powers of all the  $4k+3$  primes are even.

So  $(2^1)(3^4)(5^0)(7^3)(11^0)(13^0)(17^8)(19^{20})$  is not the sum of two squares

Difference of two squares

Theorem

No integer of the form  $4k+2$  is the difference of two squares.

Proof

mod 4:

$$x=0, 1, 2, 3 \text{ so } x^2=0, 1 \text{ and } y=0, 1, 2, 3 \text{ so } y^2=0, 1$$

so  $x^2 - y^2 = 0, 1, -1$  so  $x^2 - y^2 = 0, 1, 3$  so  $x^2 - y^2 \neq 2$

end of mod 4

So an integer of the form  $4k+2$  cannot be the difference of two squares.

We can easily verify that:

Theorem

Every integer of the form  $4k$  is the difference of two squares

Proof

$$4k = (k+1)^2 - (k-1)^2$$

Also

$$4k+1 = (2k+1)^2 - (2k)^2$$

And

$$4k+3 = (2k+2)^2 - (2k+1)^2$$

So  $n$  is the difference of two squares if and only if  $n$  is not of the form  $4k+2$

see Exercise

Theorem

Every odd prime can be written as the difference of two squares in just one way.

Proof

If:

$$p = n^2 - m^2 = (n-m)(n+m)$$

then:

$p$  can be factorised and is therefore not a prime unless  $(n-m)=1$  and  $p=(n+m)$

Which means we must have:

$$n = \frac{p+1}{2} \text{ and } m = \frac{p-1}{2}$$

It can be proved that:

Every integer is the sum of:

4 squares

9 cubes

19 fourth powers

37 fifth powers

etc

### EXERCISE

Show that no integer of the form  $8k+7$  is the sum of three squares.

### SOLUTION

mod 8

$$x=0,1,2,3,4,5,6,7 \text{ so } x^2=0,1,4$$

$$y=0,1,2,3,4,5,6,7 \text{ so } y^2=0,1,4$$

$$z=0,1,2,3,4,5,6,7 \text{ so } z^2=0,1,4$$

$$\text{So } x^2+y^2+z^2=0,1,2,3,4,5,6$$

end of mod 8

## Dodgy Probability

Laplace once said that probability is just common sense reduced to calculation.

Well I find probability difficult. Here are some questions and my attempts to answer them.

### Question 1

Spin two coins. What is the probability you get two heads?

Answer

When you spin two coins you can get: two heads or two tails or one of each.

So answer is 1/3

### Question 2

Spin three coins. What is the probability you get either three heads or three tails?

Answer

When you spin three coins, two must land the same way. The other coin is equally likely to be the same or to be different from these two.

So answer is 1/2

### Question 3

Spin 2 coins. Given that one of the coins lands heads, what is the probability that both coins land heads?

Answer

One of the coins lands heads. Consider the other coin. It is equally likely to land heads or tails.

So answer is 1/2

### Question 4

Spin a coin repeatedly, until you get a head followed by a head or a tail followed by a head. Which is more likely?

Answer

HH and TH are all equally likely.

So answer is 1/2

### Question 5

Roll a pair of dice. What is the probability the scores on the dice add up to 8?

Answer

There are 3 ways I can get a total of 8:

2 and 6      3 and 5      double 4

There are 21 possible outcomes

double 1	1 and 2	1 and 3	1 and 4	1 and 5	1 and 6
	double 2	2 and 3	2 and 4	2 and 5	2 and 6
		double 3	3 and 4	3 and 5	3 and 6
			double 4	4 and 5	4 and 6
				double 5	5 and 6
					double 6

So answer is:  $\frac{3}{21}$

### Question 6

A bag contains a ball. It is equally likely to be red or green. A red ball is added to the bag. Then a ball is taken from the bag. It is a red ball.

What is the probability that the other ball in the bag is red?

Answer

We have put in a red ball and then taken out a red ball, so we are back to where we started.

So answer is 1/2

### Question 7

A bag contains three cards. One card is red on both sides, one card is green on both sides, and one card is red on one side and green on the other side. A card is taken from the bag, and placed down on the table, so that only one side can be seen. This side is red.

What is the probability that its other side is red?

Answer

We know that the card on the table is not the green-green card. It is equally likely to be either of the other two cards.

So answer is 1/2

### Question 8 (this is the notorious Monty Hall Problem)

In a game show, the contestant is shown three closed doors. Behind one of these doors is a new car and behind each of the other two doors is a goat. The contestant points to a door. The host then opens one of the other doors, revealing a goat. The contestant is now given the opportunity to stick

with their original choice of door or switch to the other closed door. Assuming the contestant is hoping to choose the door with the car behind it, is it best to switch doors or stick with the original choice?

Answer

The contestant ends up facing two doors. One has a goat behind it, the other a car. The contestant can choose either door. Switch or stick, it makes no difference.

Question 9

There are 23 people in a room. What is the probability that no 2 people have the same birthday?

Answer

There are  $(365 C 23)$  ways you can pick 23 different dates in the year.

There are  $(365)^{23}$  ways you can pick 23 dates in the year.

So answer is  $\frac{(365 C 23)}{(365)^{23}}$

So how did I get on? It turns out that I got them all wrong!

See the section: Probability Exercise 7

## Probability

Here are 8 ways to calculate probabilities.

### 1. Counting

#### Example 1

I pick a card from a pack of cards. What is the probability I get a red picture card?

There are 52 possible outcomes – the 52 cards in the pack.

Each possible outcome is equally.

There are 6 desired outcomes – the 6 red picture cards.

So answer is  $6/52$

#### Example 2

I roll two dice. What is the probability the sum of the scores is 8?

6		*				
5			*			
4				*		
3					*	
2						*
1						
	1	2	3	4	5	6

The numbers along the bottom of the grid are the possible scores on one dice and the numbers up the side of the grid are the possible scores on the other dice.

There are 36 possible outcomes – the 36 cells in the grid

Each possible outcome is equally likely.

There are 5 desired outcomes – the 5 cells marked with a \*

So answer is  $5/36$

see Exercise 1

### 2. Using a table

#### Example 3

We have a group of 50 students.

38 study Art. 32 study Biology. 24 study Art and Biology.

We put the information in a table:

	$A$	$A'$	
$B$	24		32
$B'$			
	38		50

$A$  studies Art       $A'$  does not study Art

$B$  studies Biology       $B'$  does not study Biology

50 goes in the bottom right-hand corner cell.

38 goes at the end of the  $A$  column. This is the total number of students who study Art.

32 goes at the end of the  $B$  row. This is the total number of students who study Biology.

24 goes in the  $A$  column and the  $B$  row because 24 students study both Art and Biology.

When I say 38 students study Art, this is the total number of students who study Art.

24 of these 38 students also study Biology. The other 14 of these 38 students do not study Biology.

So 14 goes in the  $A$  column and the  $B'$  row.

We can now complete the table

	$A$	$A'$	
$B$	24	8	32
$B'$	14	4	18
	38	12	50

The table shows the number of students in each category. We can use this table to read off probabilities:

The probability that the student studies Art:

$$p(A) = \frac{38}{50}$$

The probability that the student studies both Art and Biology:

$$p(A \cap B) = \frac{24}{50}$$

The probability that the student studies Art or Biology or both:

$$p(A \cup B) = \frac{24+14+8}{50} \text{ or if you prefer } p(A \cup B) = \frac{50-4}{50}$$

The probability that the student studies Art given that they study Biology:

$$p(A | B) = \frac{24}{32}$$

etc

We can use this table to explain the laws of probability:

$$1. \quad p(A) + p(A') = \frac{38}{50} + \frac{12}{50} = \frac{50}{50} = 1$$

In general:

$$p(A) + p(A') = 1$$

$$2. \quad p(A \cap B) + p(A \cap B') = \frac{24}{50} + \frac{14}{50} = \frac{38}{50} = p(A)$$

In general:

$$p(A \cap B) + p(A \cap B') = p(A)$$

$$3. \quad p(A \cup B) = \frac{24}{50} + \frac{14}{50} + \frac{8}{50} = \frac{46}{50}$$

And:

$$p(A) + p(B) - p(A \cap B) = \frac{38}{50} + \frac{32}{50} - \frac{24}{50} = \frac{46}{50}$$

In general:

$$p(A \cup B) = p(A) + p(B) - p(A \cap B)$$

$$4. \quad p(A | B) = \frac{24}{32} = \frac{(24/50)}{(32/50)} = \frac{p(A \cap B)}{p(B)}$$

In general:

$$p(A | B) = \frac{p(A \cap B)}{p(B)} \text{ so } p(A \cap B) = p(A | B) \times p(B)$$

$$5. \quad p(A \cup B) = \frac{24}{50} + \frac{14}{50} + \frac{8}{50} = \frac{46}{50} = 1 - \frac{4}{50}$$

In general:

$$p(A \cup B) = 1 - p(A' \cap B')$$

$$6. \quad p(A \cap B) = \frac{24}{50} = 1 - \left( \frac{8}{50} + \frac{4}{50} + \frac{14}{50} \right)$$

In general:

$$p(A \cap B) = 1 - p(A' \cup B')$$

We can divide all the numbers in the table by 50

	A	A'	
B	0.48	0.16	0.64
B'	0.28	0.08	0.36
	0.76	0.24	1

The table shows the probability of students in each category. We can use this table to read off probabilities:

The probability that the student studies Art:

$$p(A) = 0.76$$

The probability that the student studies both Art and Biology:

$$p(A \cap B) = 0.48$$

The probability that the student studies Art or Biology or both:

$$p(A \cup B) = 0.48 + 0.28 + 0.16 \quad \text{or if you prefer} \quad p(A \cup B) = 1 - 0.08$$

The probability that the student studies Art given that they study Biology:

$$p(A | B) = \frac{0.48}{0.64}$$

etc

Example 4

$$p(A' \cap B) = 0.3 \quad p(A \cap B') = 0.2 \quad p(B') = 0.6$$

We can fill in these probabilities

	$A$	$A'$	
$B$		0.3	
$B'$	0.2		0.6
			1

then we can fill in the other probabilities:

	$A$	$A'$	
$B$	0.1	0.3	0.4
$B'$	0.2	0.4	0.6
	0.3	0.7	1

then we can read off any probability we want:

$$p(A')=0.7 \quad p(A \cap B')=0.2 \quad p(A' \cup B)=0.8 \quad p(A' \mid B)=\frac{0.3}{0.4} \text{ etc}$$

### Example 5

$$p(A \cup B)=0.8 \quad p(A)=0.4 \quad p(A \cap B)=0.3$$

We can fill in these probabilities:

$$\text{note: } p(A' \cap B')=1-p(A \cup B)=1-0.8=0.2$$

	$A$	$A'$	
$B$	0.3		
$B'$		0.2	
	0.4		1

then we can fill in the other probabilities:

	$A$	$A'$	
$B$	0.3	0.4	0.7
$B'$	0.1	0.2	0.3
	0.4	0.6	1

then we can read off any probability we want.

Note:

Some people like to use Venn diagrams instead of tables but I prefer tables.

See Exercise 2

### 3. Using the laws of probability

Example 6

Every day I walk to work or I cycle to work.

The probability I walk is 0.8 and the probability I cycle is 0.2

If I walk, the probability I am late is 0.4 and if I cycle, the probability I am late is 0.3

(a) What is the probability I will be late?

(b) What is the probability I walked given that I was late?

a) Now:

$$p(\text{walk} \cap \text{late}) = p(\text{late} | \text{walk}) \times p(\text{walk}) = 0.8 \times 0.4 = 0.32$$

And:

$$p(\text{cycle} \cap \text{late}) = p(\text{late} | \text{cycle}) \times p(\text{cycle}) = 0.2 \times 0.3 = 0.06$$

So:

$$p(\text{late}) = p(\text{walk} \cap \text{late}) + p(\text{cycle} \cap \text{late}) = 0.32 + 0.06 = 0.38$$

b)

$$p(\text{walk} | \text{late}) = p\left(\frac{\text{walk} \cap \text{late}}{p(\text{late})}\right) = \frac{0.32}{0.38}$$

see Exercise 3

### 4. Using a tree diagram

Example 7

Every day I walk to work or I cycle to work.

The probability I walk is 0.8 and the probability I cycle is 0.2

If I walk, the probability I am late is 0.4 and if I cycle, the probability I am late is 0.3

(a) What is the probability I will be late?

(b) What is the probability I walked given that I was late?

WE NEED A TREE DIAGRAM

Note:

$$p(walk \cap late) = p(walk) \times p(late | walk) = 0.8 \times 0.4 = 0.32$$

And:

$$p(cycle \cap late) = p(cycle) \times p(late | cycle) = 0.2 \times 0.3 = 0.06$$

So to find probabilities we just multiply the probabilities along the branches.

WE NEED A TREE DIAGRAM

a)  $p(late) = 0.32 + 0.06 = 0.38$

b)  $p(walk | late) = \frac{p(walk \cap late)}{p(late)} = \frac{0.32}{0.38}$

see Exercise 4

5. Considering a number of cases.

Example 8

Every day I walk to work or I cycle to work.

The probability I walk is 0.8 and the probability I cycle is 0.2

If I walk, the probability I am late is 0.4 and if I cycle, the probability I am late is 0.3

(a) What is the probability I will be late?

(b) What is the probability I walked given that I was late?

Consider 100 days. On average:

I will walk on 80 days and be late on  $0.4 \times 80 = 32$  of these walking days.

I will cycle on 20 days and be late on  $0.3 \times 20 = 6$  of these cycling days.

(a) I will be late on 38 days out of 100 days.

Answer: 38/100

(b) I will walk and be late on 32 days. I will be late on 38 days.

Answer: 32/38

EXPECTED FREQ TREE DIAGRAM? SEE MATHS CAFE NOTES

see Exercise 5

## 6. Using Arrangements and Selections.

See chapter: Arrangements and Selections

See Exercise 6

## 7. Using computer simulation

Example 9

In a game of chuck-a-luck, I roll 3 dice.

If I get 3 sixes, then I win £3.

If I get 2 sixes, then I win £2.

If I get 1 six, then I win £1.

If I get 0 sixes, then I lose £1.

What will be my average winnings, per game, in the long run?

If you can't work this out, you can do a simulation.

Write a computer program to play this game 1,000,000 times and record my total winnings. If my total winnings is, say £58743 then  $\text{£ } 58743/1,000,000$  is an estimate of my average winnings per game.

See Appendix 1

## 8. Doing an experiment

I have a wooden cone. When I throw it up in the air it can land on its side or it can land on its base, point up. What is the probability that it lands on its side?

There are 2 possible outcomes but there is no reason to think that these outcomes are equally likely.

Perhaps, if I was good at Mechanics I could work it out. But I'm not.

I can do an experiment. I can throw it up in the air a very large number of times and record how many times it lands on its side.

See Exercise 7

## EXERCISE 1

1.

I pick a card from a pack of cards. What is the probability I get:

- a) a spade
- b) a picture card

- c) a spade and a picture card
  - d) a spade or a picture card
  - e) a spade or a picture card but not both
- 2.

I roll two dice. What is the probability:

- a) the sum of the scores is 7
- b) the product of the scores is 12
- c) the difference of the scores is less than 4
- d) I get at least one 6

## EXERCISE 2

1.

There are 42 people at a party. 24 drink wine, 22 drink beer and 6 drink neither. Find the probability that a person at the party drinks wine and beer.

2.

There are 40 students in a class.

23 are girls, 17 are boys, 32 are right-handed and 3 are left-handed boys.

If I pick a left-hander, what is the probability they are a girl?

3.

$$p(A \cap B) = 0.2 \quad p(A') = 0.7 \quad p(B') = 0.4 \quad \text{Find } p(B | A)$$

4.

$$p(A \cup B) = 0.8 \quad p(A \cap B) = 0.6 \quad p(B) = 0.7 \quad \text{Find } p(B | A')$$

## EXERCISE 3

1) The probability I revise for a test is 0.3

If I revise, the probability I pass is 0.9 and if I don't revise, the probability I pass is 0.4

What is the probability I pass my next test?

2) 60% of students love jazz. Only  $\frac{1}{3}$  of jazz lovers like carrots.

40% of students hate jazz. Only  $\frac{1}{4}$  of jazz haters like carrots.

I meet a student who likes carrots. What is the probability they like jazz?

## EXERCISE 4

1) The probability I revise for a test is 0.3

If I revise, the probability I pass is 0.9 and if I don't revise, the probability I pass is 0.4

What is the probability I pass my next test?

2) 60% of students love jazz. Only  $\frac{1}{3}$  of jazz lovers like carrots.

40% of students hate jazz. Only  $\frac{1}{4}$  of jazz haters like carrots.

I meet a student who likes carrots. What is the probability they like jazz?

#### EXERCISE 5

1) The probability I revise for a test is 0.3

If I revise, the probability I pass is 0.9 and if I don't revise, the probability I pass is 0.4

What is the probability I pass my next test?

2) 60% of students love jazz. Only  $\frac{1}{3}$  of jazz lovers like carrots.

40% of students hate jazz. Only  $\frac{1}{4}$  of jazz haters like carrots.

I meet a student who likes carrots. What is the probability they like jazz?

#### EXERCISE 6

1) A bag contains 8 red counters and 15 blue counters. I take 5 counters out of the bag (without replacement) What is the probability I get 2 reds and 3 blues?

2) A bag contains 6 red counters and 43 blue counters. I take 6 counters out of the bag (without replacement) What is the probability I get:

- (a) 6 reds
- (b) 4 reds, 2 blues
- (c) 2 reds and 4 blues

Why is this set-up the same as the lottery?

3) A bag contains 5 red, 7 green and 12 yellow counters. I take 5 counters out of the bag (without replacement) What is the probability I get:

- (a) no reds
- (b) at least one red
- (c) all the same colour
- (d) 2 reds, 1 green, 2 yellows

4) In a game of bridge, there are 4 players and each player gets 13 cards. What is the probability that each player gets exactly one ace?

#### EXERCISE 7

Look at the questions in Dodgy Probability

#### SOLUTIONS 1

1.

- a)  $\frac{13}{52}$
- b)  $\frac{12}{52}$
- c)  $\frac{3}{52}$
- d)  $\frac{22}{52}$
- e)  $\frac{19}{52}$

2.

- a)  $\frac{6}{36}$
- b)  $\frac{4}{36}$
- c)  $\frac{30}{36}$
- d)  $\frac{11}{36}$

#### SOLUTIONS 2

1.

We can fill in these numbers:

	wine	not wine	
beer			22
not beer		6	
	24		42

then we can fill in the other numbers:

	wine	not wine	
beer	10	12	22
not beer	14	6	20
	24	18	42

Answer: 10/42

2.

We can fill in these numbers:

	girl	boy	
right-handed			32
left-handed		3	
	23	17	40

then we can fill in the other numbers:

	girl	boy	
right-handed	18	14	32
left-handed	5	3	8
	23	17	40

Answer: 5/8

3.

We can fill in these probabilities:

	$A$	$A'$	
$B$	0.2		
$B'$			0.4
	0.7	1	

Then we can fill in the other probabilities

	$A$	$A'$	
$B$	0.2	0.4	0.6
$B'$	0.1	0.3	0.4
	0.3	0.7	1

$$p(B \mid A) = \frac{p(B \cap A)}{p(A)}$$

Answer: 0.2/0.3

4.

We can fill in these probabilities:

	$A$	$A'$	
$B$	0.6		0.7
$B'$		0.2	
			1

Then we can fill in the other probabilities

	$A$	$A'$	
$B$	0.6	0.1	0.7
$B'$	0.1	0.2	0.3
	0.7	0.3	1

$$p(B \mid A') = \frac{p(B \cap A')}{p(A')}$$

Answer: 0.1/0.3

SOLUTIONS 3

1.

$R$  means I revise  $P$  means I pass

$$p(R \cap P) = p(R) \times p(P | R) = 0.3 \times 0.9 = 0.27$$

$$p(R' \cap P) = p(R') \times p(P | R') = 0.7 \times 0.4 = 0.28$$

$$p(P) = p(R \cap P) + p(R' \cap P) = 0.27 + 0.28 = 0.55$$

2.

$J$  means likes jazz  $C$  means likes carrots

$$p(J \cap C) = p(J) \times p(C | J) = 0.6 \times 1/3 = 0.2$$

$$p(J' \cap C) = p(J') \times p(C | J') = 0.4 \times 1/4 = 0.1$$

$$p(C) = p(J \cap C) + p(J' \cap C) = 0.2 + 0.1 = 0.3$$

$$p(J | C) = p(J \cap C) / p(C) = 0.2 / 0.3$$

## SOLUTIONS 4

1.

### TREE DIAGRAM

$$p(\text{pass}) = 0.27 + 0.28 = 0.55$$

2.

### TREE DIAGRAM

$$p(\text{likes jazz} | \text{likes carrots}) = \frac{p(\text{likes jazz} \cap \text{likes carrots})}{p(\text{likes carrots})} = \frac{0.2}{0.3}$$

## SOLUTIONS 5

1) Consider 100 tests. On average:

I revise for 30 tests and I pass 27 of these tests

I don't revise for 70 tests and I pass 28 of these tests.

I pass 55 tests.

Answer: 55/100

2) Consider 100 students. On average:

60 students love jazz and 20 of these students will like carrots.

40 students hate jazz and 10 of these students will like carrots.

30 students like carrots. Of these 20 like jazz.

Answer: 20/30

## SOLUTIONS 6

1)

There are  $(23C5)$  ways to select 5 counters.

There are  $(8C2)(15C3)$  ways to select 2 reds and 3 blues.

Answer is:  $\frac{(8C2)(15C3)}{(23C5)}$

2)

- (a)  $\frac{(6C6)}{(49C6)}$  (b)  $\frac{(6C4)(43C2)}{(49C6)}$  (c)  $\frac{(6C2)(43C4)}{(49C6)}$

In the lottery there are 6 winning balls and 43 non-winning balls.

3)

- (a)  $\frac{(19C5)}{(24C5)}$  (b)  $1 - \frac{(19C5)}{(24C5)}$  (c)  $\frac{(5C5)+(7C5)+(12C5)}{(24C5)}$   
(d)  $\frac{(5C2)(7C1)(12C2)}{(24C5)}$

4)

We start by giving player A, 13 cards from the pack.

There are  $(52C13)$  ways to give player A, 13 cards.

There are  $(4C1)(48C12)$  ways to give player A, 1 ace and 12 non-aces.

We now give player B, 13 cards from the remaining cards in the pack.

There are  $(39C13)$  ways to give player B, 13 cards.

There are  $(3C1)(36C12)$  ways to give player B, 1 ace and 12 non-aces.

We now give player C, 13 cards from the remaining cards in the pack.

There are  $(26C13)$  ways to give player C, 13 cards.

There are  $(2C1)(24C12)$  ways to give player C, 1 ace and 12 non-aces.

We now give player D the remaining 13 cards.

Answer:  $\frac{(4C1)(48C12)}{(52C13)} \times \frac{(3C1)(36C12)}{(39C13)} \times \frac{(2C1)(24C12)}{(26C13)}$

## SOLUTIONS 7

- 1) These three possible outcomes are not equally likely.

head	*	
tail		
	head	tail

Answer: 1/4

- 2) When you spin three coins there are 8 possible outcomes:

HHH, HHT, HTH, THH, TTH, THT, HTT, TTT

Of these 8 possible outcomes, 2 outcomes are three heads or three tails.

Answer: 2/8

- 3) When you spin 2 coins, there are 4 possible, equally likely, outcomes:

(head, head) (head, tail) (tail, head) (tail, tail)

Given that one of the coins lands heads means that we can eliminate (tail, tail) leaving 3 possible, equally likely, outcomes.

Answer: 1/3

- 4) The only way you get HH before you get TH is if the first two spins are HH (think about it)

The probability of this is 1/4

Amusingly, if you spin a coin repeatedly:

the sequence TTH is likely to appear before the sequence THH

the sequence THH is likely to appear before the sequence HHT

the sequence HHT is likely to appear before the sequence HTT

the sequence HTT is likely to appear before the sequence TTH

Look up the game Penney-Ante

- 5) We must count correctly! Look back to example 2.

- 6) Consider 100 cases

a) Start with a red ball in the bag (50 cases)

In 50 cases we add a red then remove a red, leaving a red.

b) Start with a green ball in the bag (50 cases)

In 25 cases we add a red then remove a red, leaving a green.

In 25 case we add a red then remove a green, leaving a red.

In 75 cases we remove a red and of these, 50 cases we leave a red.

Answer: 50/75

7) Consider 300 cases

a) Card is red/red (100 cases)

In 100 cases we see a red side and the other side is red.

b) Card is green/green (100 cases)

In 100 cases we see a green side and the other side is green.

c) Card is red/green (100 cases)

In 50 cases we see a red card and the other side is green.

In 50 cases we see a green side and the other side is red.

In 150 cases we see a red card and of these, 100 cases the other side is red.

Answer: 100/150

8) You point to one of three closed doors. The probability there is a car behind that door is 1/3

So if you decide to stick, the probability you win the car is 1/3

So if you decide to switch, the probability you win the car is 2/3

9) There is 1 person in the room. Another person walks in. The probability these 2 people have different birthdays is 364/365. Another person walks in. The probability these 3 people have

different birthdays is  $\frac{364}{365} \times \frac{364}{365}$ . Another person walks in ... etc

Answer:  $\frac{364}{365} \times \frac{363}{365} \times \frac{362}{365} \times \dots \times \frac{343}{365}$

Surprisingly, this works out to be approximately 0.5

So with 23 people in a room, there is a probability of 0.5 that at least 2 of them have the same birthday!

## Probability Fallacies

### Example 1

I toss a coin 5 times and get 5 tails.

The probability of getting 5 tails with a fair coin is 0.03 So the probability the coin is fair is 0.03

No! To argue like this is incorrect.

$$p(5 \text{ tails} | \text{fair coin}) = 0.03 \text{ and this is not the same as } p(\text{fair coin} | 5 \text{ tails})$$

### Example 2 Gambler fallacy

A gambler keeps rolling a dice. A six has not occurred for some time. By the law of averages, it should occur soon.

No! To argue like this is to commit the gambler fallacy.

Imagine a conversation between the gambler and the (talking) dice:

Gambler: I notice you haven't come up six for some time.

Dice: Sorry about that. I'll throw in some extra sixes so that things even out.

I don't think so!

Note:

If you are about to roll a dice 20 times then the probability of getting no sixes is  $(5/6)^{20} = 0.026$

But:

If you have already rolled a dice 19 times and not got any sixes then the probability of not getting a six on the 20th roll is  $5/6$

### Example 3 Prosecutor fallacy

A murder has been committed by one of the inhabitants of a town. Eric is on trial for the murder, because his DNA matches DNA found at the crime scene. If Eric is not guilty, the probability that his DNA matches DNA found at the crime scene is 0.00002

So the probability that Eric is not guilty is 0.00002

No! To argue like this is to commit the prosecutor fallacy.

$$p(\text{match} | \text{not guilty}) = 0.00002 \text{ and this is not the same as } p(\text{not guilty} | \text{match})$$

What the jury wants to know is  $p(\text{not guilty} | \text{match})$  This is the probability that Eric is not guilty.

For example, say the town has 250,000 inhabitants. Typically  $250,000 \times 0.00002 = 5$  people will have DNA that matches the sample found at the crime scene. So, in the absence of any other evidence, the probability that Eric is not guilty is  $4/5$

#### Example 4 False-Positive Fallacy

There is a disease but sufferers show no symptoms. At any given time, 1% of people actually have the disease. A test has been developed that can detect the disease. If a person has the disease, the test result will be positive. If a person does not have the disease, there is a 3% chance that the test result will be positive. Eric has just had the test, and the result is positive. So the probability that Eric does not have the disease is 3%

No! To argue like this is to commit the false-positive fallacy

$$p(\text{positive} \mid \text{no disease}) = 0.03 \text{ and this is not the same as } p(\text{no disease} \mid \text{positive})$$

Consider 100 people. On average, 1 person will have the disease and test positive and 99 people will not have the disease and 3 of them will test positive. So of the 4 people who test positive, only one of them has the disease. So the probability that Eric does not have the disease is  $3/4$

#### Example 5 OJ Simpson trial

OJ Simpson is on trial for the murder of his wife. The prosecution has established that he used to beat-up his wife. The defence argue that, if a man beats-up his wife, the probability that he will murder her is extremely small. True but irrelevant. The prosecution should have argued that, if a man beats-up his wife and his wife is murdered, the probability that he is the murderer is very high.

#### Example 6 Sally Clark trial

Sally Clark is on trial for the murder of her two children. The prosecution argue that, if a woman has 2 children, the probability they both die of natural causes is extremely low. True but irrelevant. The defence should have argued that, if a woman has 2 children and they both die, the probability they both died of natural causes is high.

There were other incorrect uses of probability in this trial. You should read up about it.

#### Example 7

#### LAW OF AVERAGES AND LAW OF LARGE NUMBERS

## Probability Paradoxes

### Example 1

#### Condorcet Paradox

Dice A has faces numbered 3,3,3,3,3,3

Dice B has faces numbered 1,1,5,5,5,5

Dice C has faces numbered 2,2,2,2,6,6

We each choose a dice. We each roll our dice and the highest score wins.

Being a wonderfully nice person, I will let you choose first. Which dice will you choose?

Let's work out the probabilities.

In a contest between dice A and dice B:

$$p(A \text{ wins}) = \frac{2}{6} \text{ and } p(B \text{ wins}) = \frac{4}{6}$$

In a contest between dice A and dice C:

$$p(A \text{ wins}) = \frac{4}{6} \text{ and } p(C \text{ wins}) = \frac{2}{6}$$

In a contest between dice B and dice C:

6	C	C	C	C	C	C	C
6	C	C	C	C	C	C	C
2	C	C	B	B	B	B	B
2	C	C	B	B	B	B	B
2	C	C	B	B	B	B	B
2	C	C	B	B	B	B	B
	1	1	5	5	5	5	5

$$p(B \text{ wins}) = \frac{16}{36} \text{ and } p(C \text{ wins}) = \frac{20}{36}$$

Which dice will you choose?

If you pick A then I'll pick B. If you pick B then I'll pick C. If you pick C then I'll pick A.

### Example 2

#### St. Petersburg Paradox

You spin a coin      If it is heads, I give you £1, and the game ends

                        If it is tails, you spin again.

You spin again      If it is heads, I give you £2, and the game ends.

	If it is tails, you spin again.
You spin again	If it is heads, I give you £4, and the game ends.
	If it is tails, you spin again.
You spin again	If it is heads, I give you £8, and the game ends.
	If it is tails, you spin again.

etc

Let  $X$  be your winnings. The probability distribution for  $X$  is:

$x$	$p(x)$	$xp(x)$
1	1/2	1/2
2	1/4	1/2
4	1/8	1/2
8	1/16	1/2
...	...	...

Your expected winnings are:

$$E(X) = \sum_{x=1}^{\infty} xp(x) = \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \dots \quad \text{this is infinite.}$$

So if I charge you £1,000,000 to play this game, then you should play.

### Example 3

#### Simpson's Paradox

A university offers courses in Engineering and Medicine.

Engineering:

100 women apply and 40 are accepted. 600 men apply and 150 are accepted.

So the acceptance rate is higher for women.

Medicine:

600 women apply and 72 are accepted. 100 men apply and 10 are accepted.

So the acceptance rate is higher for women.

University:

700 women apply and 112 are accepted. 700 men apply and 160 are accepted.

So the acceptance rate is higher for men.

Coins

if you know about the binomial distribution ...

If you spin a coin 20 times, what is the probability you get 10 heads and 10 tails?

Let X be the number of heads in 20 spins

X has a binomial distribution.

So:

$$p(X=10) = (20C10) \left(\frac{1}{2}\right)^{10} \left(\frac{1}{2}\right)^{10} = \frac{(20)!}{(10)!(10)!2^{20}}$$

In general:

If you spin a coin  $2n$  times, what is the probability you get  $n$  heads and  $n$  tails?

Let X be the number of heads in  $2n$  spins

X has a binomial distribution.

So:

$$p(X=n) = (2nCn) \left(\frac{1}{2}\right)^n \left(\frac{1}{2}\right)^n = \frac{(2n)!}{(n)!(n)!2^{2n}}$$

What happens if  $n$  is large?

Stirling discovered a remarkable approximation for  $m!$  when  $m$  is large:

It is:

$$m! \approx (m^m)(e^{-m})\sqrt{(2\pi m)} \quad \text{what are } e \text{ and } \pi \text{ doing?} \quad \text{See Footnote}$$

Using Stirling's approximation show that:

If  $n$  is large then:

$$p(X=n) \approx \frac{1}{\sqrt{(n\pi)}}$$

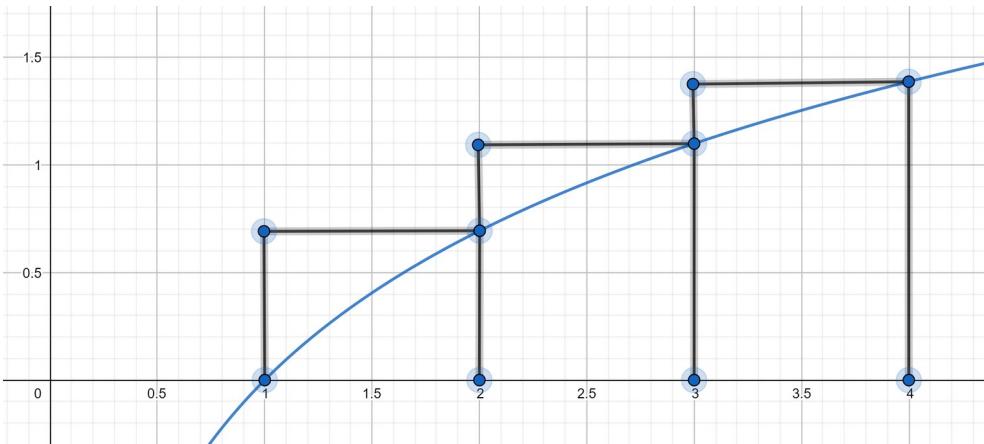
Footnote:

$$m! = 1 \times 2 \times 3 \times 4 \times \dots \times m$$

So:

$$\ln(m!) = \ln 1 + \ln 2 + \ln 3 + \ln 4 + \dots + \ln m$$

Here is the graph  $y = \ln x$



The diagram shows blocks between  $x=1$  and  $x=4$

The area of the blocks is:  $\ln 2 + \ln 3 + \ln 4$

The area under the graph is:  $\int_1^4 (\ln x) dx = [x \ln x - x]_1^4 = 4 \ln 4 - 4 + 1$

So:

$$\ln 2 + \ln 3 + \ln 4 \approx 4 \ln 4 - 4 + 1$$

In general:

The diagram shows blocks between  $x=1$  and  $x=m$

The area of the blocks is:  $\ln 2 + \ln 3 + \ln 4 + \dots + \ln m$

The area under the graph is:  $\int_1^m (\ln x) dx = [x \ln x - x]_1^m = m \ln m - m + 1$

So:

$$\ln 2 + \ln 3 + \ln 4 + \dots + \ln m \approx m \ln m - m + 1$$

So:

$$\ln(m!) \approx m \ln m - m + 1$$

Show that:

$$m! \approx (m^m)(e^{-m})e$$

This is not as good as Stirling's approximation but it's a start.

Tennis

Alice and Bill play tennis. For each point they play, the probability that Alice wins the point is  $p$   
(see Footnote 1) If they play just one game, what is the probability that Alice wins the game?

For Alice to win, game:love

Alice must win 4 points and Bill must win no points.

Probability:  $(p^4)$

For Alice to win, game:15

Alice must win 4 points and Bill must win 1 point.

But Alice must win the last point – think about it!

So Alice must win 3 of the first 4 points and then win the 5<sup>th</sup> point.

The number of different orders where Alice wins 3 of the first 4 points is  $(4C3)$

These are AAAB, AABA, ABAA, BAAA

(A denotes Alice wins the point and B denotes Bill wins the point)

Probability:  $(4C3)(p^4)(1-p)$

For Alice to win, game:30

Alice must win 4 points and Bill must win 2 points.

But Alice must win the last point - etc

Probability:  $(5C3)(p^4)(1-p)^2$

For Alice to win, game:40

This can't happen – think about it!

What is the probability the game goes to deuce?

Alice must win 3 points and Bill must win 3 points.

In any order.

Probability:  $(6C3)(p^3)(1-p)^3$

What is the probability Alice wins the game, starting from deuce?

This is a bit more difficult.

note: if Alice and Bill start at deuce and play 2 points then:

either, Alice wins both points and wins the game, with probability  $p^2$

or, Bill wins both points and wins the game, with probability  $(1-p)^2$

or, Alice and Bill each win 1 point and they are back at deuce, with probability  $2p(1-p)$

### method 1

The score is at deuce. Alice wins the game if:

Alice wins the next 2 points

OR Alice and Bill each win 1 of the next 2 points and then Alice wins 2 points

OR Alice and Bill each win 1 of the next 2 points and then Alice and Bill each win 1 of the following 2 points and then Alice wins 2 points

OR...

So Alice wins with probability:  $p^2 + 2p(1-p)p^2 + (2p(1-p))^2 p^2 + (2p(1-p))^3 p^2 + \dots$

We can sum this infinite series to get:

$$\frac{p^2}{1-2p(1-p)} = \frac{p^2}{2p^2-2p+1}$$

### method 2

The score is at deuce. Alice wins the game if:

Alice wins the next 2 points.

OR Alice and Bill each win 1 of the next 2 points and then Alice wins the game.

So if  $a$  is the probability Alice wins the game, starting from deuce then:

$$a = p^2 + 2p(1-p)a$$

This is a neat trick, writing  $a$  in terms of  $a$  (see Footnote 2)

This rearranges to:

$$a = \frac{p^2}{2p^2-2p+1}$$

So the probability Alice wins the game via deuce is:

$$(6C3)(p^3)(1-p)^3 \times \frac{p^2}{2p^2-2p+1} = (6C3) \frac{(p^5)(1-p)^3}{2p^2-2p+1}$$

So the total probability that Alice wins the game is simply:

$$p^4 + (4C3)p^4(1-p) + (5C3)p^4(1-p)^2 + (6C3) \frac{p^5(1-p)^3}{2p^2-2p+1}$$

Footnote 1:

Alice and Bill play tennis. For each point they play  $p$  is the probability that Alice wins the point. This might not be very realistic. The probability that Alice wins the point will probably depend on who is serving, etc. We have ignored such complications.

Footnote 2:

This neat trick reminds me of another problem.

Evaluate:

$$1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

Let:

$$x = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

Then:

$$x = 1 + \frac{1}{x} \text{ which we can solve.}$$

Collecting Cards

if you know about probability distributions ...

Every packet of cornflakes contains a card with a picture of a mathematician. There are 20 different mathematicians to collect. On average, how many cornflakes packets will I have to buy to get the complete set?

Let  $X_1$  be the number of cereal packets I will have to buy to get my first mathematician.

Let  $X_2$  be the number of cereal packets I will have to buy, after I have got my first mathematician, to get my second mathematician.

Let  $X_3$  be the number of cereal packets I will have to buy, after I have got my second mathematician, to get my third mathematician.

etc

Let  $X$  be the total number of cereal packets I will have to buy to get the complete set of 20 mathematicians.

So:

$$X = X_1 + X_2 + X_3 + \dots + X_{20} \text{ and we want to find } E(X)$$

We know that:

$$E(X) = E(X_1) + E(X_2) + E(X_3) + \dots + E(X_{20})$$

When I buy my first packet, I will get my first mathematician.

So:

$$X_1 = 1 \text{ and so } E(X_1) = 1$$

Now I have got my first mathematician. How many more packets will I have to buy to get my second mathematician?

Look at this table.

$x_2$	$p(x_2)$	$x_2 p(x_2)$
1	$\frac{19}{20}$	$1 \times \frac{19}{20}$
2	$\frac{1}{20} \times \frac{19}{20}$	$2 \times \frac{1}{20} \times \frac{19}{20}$
3	$\frac{1}{20} \times \frac{1}{20} \times \frac{19}{20}$	$3 \times \frac{1}{20} \times \frac{1}{20} \times \frac{19}{20}$
...	...	...

Now:

$$E(X_2) = \sum x_2 p(x_2)$$

So:

$$E(X_2) = \frac{19}{20} \left( 1 + 2\left(\frac{1}{20}\right) + 3\left(\frac{1}{20}\right)^2 + 4\left(\frac{1}{20}\right)^3 + \dots \right)$$

So:

$$E(X_2) = \frac{19}{20} \frac{1}{\left(1 - \frac{1}{20}\right)^2} = \frac{20}{19} \quad \text{see Footnote with } x = \frac{1}{20}$$

Now I have got my second mathematician. How many more packets will I have to buy to get my third mathematician?

Look at this table.

$x_3$	$p(x_3)$	$x_3 p(x_3)$
1	$\frac{18}{20}$	$1 \times \frac{19}{20}$
2	$\frac{2}{20} \times \frac{18}{20}$	$2 \times \frac{1}{20} \times \frac{19}{20}$
3	$\frac{2}{20} \times \frac{2}{20} \times \frac{18}{20}$	$3 \times \frac{1}{20} \times \frac{1}{20} \times \frac{19}{20}$
...	...	...

Repeat the above calculation and show that:

$$E(X_3) = \frac{20}{18}$$

Find:

$$E(X_4)$$

etc

Show that:

$$E(X) = 20 \left( \frac{1}{20} + \frac{1}{19} + \frac{1}{18} + \dots + \frac{1}{1} \right)$$

Footnote

We know that:

$$1 + x + x^2 + x^3 + x^4 + x^5 + \dots = \frac{1}{1-x} \quad \text{it is a geometric series}$$

Differentiate both sides and show that:

$$1+2x+3x^2+4x^3+5x^4+\ldots=\frac{1}{(1-x)^2}$$

## Party Game

Imagine a party in a big hall with lots of guests milling around. Each guest has a card. Some guests have a red card and some guests have a green card. If two guests happen to bump into each other then they show each other their cards and points are awarded.

If two reds bump into each other, they both win  $-6$  points.

If two greens bump into each other, they both win  $1$  point.

If a red bumps into a green, the red wins  $4$  points and the green wins  $0$  points.

I arrive late to the party and the host asks me if I want a red card or a green card. Assuming I want to win as many points as possible, which colour should I choose?

Say  $r$  is the proportion of guests with red cards and  $1-r$  is the proportion of guests with green cards.

If I take a red card then my expected score when I bump into another guest is:

$$r(-6)+(1-r)(4)$$

If I take a green card then my expected score when I bump into another guest is:

$$r(0)+(1-r)(1)$$

I should take a red card if:

$$r(-6)+(1-r)(4) > r(0)+(1-r)(1)$$

so  $r < 1/3$

I should take a green card if:

$$r > 1/3$$

If  $r = 1/3$  then it doesn't matter which card I take.

Now let's change the rules so that guests can ask the host for a different card during the party.

How will the proportions of red cards evolve over time?

If we wait long enough, the proportion of red cards will settle down to  $1/3$

## Proof by Contradiction

To prove a theorem is true, we assume it is false and then show that this cannot be the case as it leads to a contradiction.

### Theorem 1

$4x - 2y = 1$  has no solution where  $x$  and  $y$  are integers.

#### Proof

Assume we have found a solution where  $x$  and  $y$  are integers:

LHS is even. RHS is odd.

Contradiction.

### Theorem 2

No prime (except 3) is one less than a square.

#### Proof

Assume the prime  $p$  is one less than the square  $n^2$

So:

$$p = n^2 - 1 = (n-1)(n+1)$$

So:

the prime  $p$  can be written as the product of two integers.

Contradiction. Unless  $(n-1)=1$  So  $n=2$  so  $p=3$

### Theorem 3

$\log 5$  is irrational

#### Proof

Assume  $\log 5$  is rational

So:

$$\log 5 = \frac{p}{q} \text{ where } p \text{ and } q \text{ are positive integers.}$$

So:

$$5 = 10^{p/q} \text{ So } 5^q = 10^p$$

Now:

LHS is odd. RHS is even.

Contradiction

#### Theorem 4

$\sqrt{2}$  is irrational

#### Proof

Assume  $\sqrt{2}$  is rational

So:

$$\sqrt{2} = \frac{p}{q} \text{ where } p \text{ and } q \text{ are integers}$$

We can say  $p$  and  $q$  are not both multiples of 2 because if they had both been multiples of 2 then we would have cancelled them down before we started.

Now:

$$2q^2 = p^2$$

So:

$p^2$  is a multiple of 2. So  $p$  is a multiple of 2. Let  $p=2r$

So:

$$2q^2 = 4r^2 \text{ So } q^2 = 2r^2 \text{ So } q^2 \text{ is a multiple of 2. So } q \text{ is a multiple of 2.}$$

So:

$p$  and  $q$  are not both multiples of 2 but  $p$  is a multiple of 2 and  $q$  is a multiple of 2.

Contradiction.

## Proof By Induction

If a theorem is true when  $n=1, 2, 3, \dots$  then we might be able to prove it using proof by induction.

### Theorem 1

$$1+2+3+\dots+n=\frac{1}{2}n(n+1) \quad \text{for } n=1, 2, 3, \dots$$

#### Proof

part 1:

If  $n=1$  then  $LHS=1$  and  $RHS=1$  So the formula is true when  $n=1$

part 2:

If  $1+2+3+\dots+n=\frac{1}{2}n(n+1)$  is true when  $n=k$  then:

$$1+2+3+\dots+k=\frac{1}{2}k(k+1)$$

$$1+2+3+\dots+k+(k+1)=\frac{1}{2}k(k+1)+(k+1)$$

$$1+2+3+\dots+k+(k+1)=\frac{1}{2}(k(k+1)+2(k+1))$$

$$1+2+3+\dots+k+(k+1)=\frac{1}{2}(k+1)(k+2)$$

So  $1+2+3+\dots+n=\frac{1}{2}n(n+1)$  is true when  $n=k+1$

End of proof

So what's going on?

Part 1 shows that the theorem is true when  $n=1$

Part 2 shows that if the theorem is true when  $n=1$  then the theorem is true when  $n=2$

So the theorem is true for  $n=2$

Part 2 shows that if the theorem is true when  $n=2$  then the theorem is true when  $n=3$

So the theorem is true for  $n=3$

etc

So we have shown the theorem must be true for all values of  $n$  Brilliant!

### Theorem 2

$$9^n - 1 \text{ is a multiple of 8} \quad \text{for } n=1, 2, 3, \dots$$

#### Proof

part 1:

If  $n=1$  then  $9^n - 1 = 8$  So  $9^n - 1$  is a multiple of 8 when  $n=1$

part 2:

If  $9^n - 1$  is a multiple of 8 when  $n=k$  then:

$9^k - 1$  is a multiple of 8

$9^k - 1 = 8r$  for some integer  $r$

$$\text{Now } 9^{k+1} - 1 = 9(9^k) - 1 = 9(9^k - 1) + 8 = 9(8r) + 8 = 8(9r + 1)$$

So  $9^n - 1$  is a multiple of 8 when  $n=k+1$

End of proof

## EXERCISE

Prove the following for  $n=1, 2, 3, \dots$

$$1) 1+3+5+\dots+(2n-1)=n^2$$

$$2) 1+2^1+2^2+2^3+\dots+2^n=2^{n+1}-1$$

## SOLUTION

1) Proof

part 1:

If  $n=1$  then  $LHS=1$  and  $RHS=1$  so the formula is true when  $n=1$

part 2:

If  $1+3+5+\dots+(2n-1)=n^2$  is true when  $n=k$  then:

$$1+3+5+\dots+(2k-1)=k^2$$

$$1+3+5+\dots+(2k-1)+(2k+1)=k^2+(2k+1)$$

$$1+3+5+\dots+(2k-1)+(2k+1)=(k+1)^2$$

So  $1+3+5+\dots+(2n-1)=n^2$  is true when  $n=k+1$

2) Proof

part 1:

If  $n=1$  then  $LHS=1$  and  $RHS=1$  so the formula is true when  $n=1$

part 2:

If  $1+2^1+2^2+2^3+\dots+2^n=2^{n+1}-1$  is true when  $n=k$  then:

$$1+2^1+2^2+2^3+\dots+2^k=2^{k+1}-1$$

$$1+2^1+2^2+2^3+\dots+2^k+2^{k+1}=2^{k+1}-1+2^{k+1}$$

$$1+2^1+2^2+2^3+\dots+2^k+2^{k+1}=2(2^{k+1})-1$$

$$1+2^1+2^2+2^3+\dots+2^k+2^{k+1}=2^{k+2}-1$$

So  $1+2^1+2^2+2^3+\dots+2^n=2^{n+1}-1$  is true when  $n=k+1$

Incidently, and this has nothing to do with proof by induction, we can prove:

$$1+3+5+\dots+(2n-1)=n^2 \text{ with this diagram.}$$

E	E	E	E	E
D	D	D	D	E
C	C	C	D	E
B	B	C	D	E
A	B	C	D	E

In this diagram we have got: one A, three Bs, five Cs, seven Ds, nine Es

How many letters have we got?

$$1+3+5+7+9=5^2$$

In general:

$$1+3+5+\dots+(2n-1)=n^2$$

## Proving The Contrapositive

In the chapter: If ... Then, we showed that  $p \Rightarrow q$  is the same as  $q' \Rightarrow p'$

So:

to prove  $p \Rightarrow q$  we can prove  $q' \Rightarrow p'$  instead.

Note:

$q' \Rightarrow p'$  is called the contrapositive of  $p \Rightarrow q$

## Theorem

$n^2$  is even  $\Rightarrow$   $n$  is even

We are going to prove:

$n$  is odd  $\Rightarrow$   $n^2$  is odd

Proof

$n$  is odd  $\Rightarrow n = (2k+1)$  for some integer  $k$

So:

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

So:

$n^2$  is odd

End of proof

## Proof using Selections

### Example 1

We have 10 books and we want to select 4 of them.

Method 1:

We select 4 books and keep them.

The number of ways this can be done is:  $(10C4)$

Method 2:

We select 6 books and throw them away (keeping the remaining 4 books)

The number of ways this can be done is:  $(10C6)$

So  $(10C4) = (10C6)$

In general:

$$(mCk) = (mC(m-k))$$

### Example 2

We have 12 books and we want to select 5 of them.

Method 1:

The number of ways this can be done is:  $(12C5)$

Method 2:

One of the books is Alice's Adventures In Wonderland.

There are  $(11C4)$  selections which include Alice's Adventures In Wonderland.

There are  $(11C5)$  selections which exclude Alice's Adventures In Wonderland.

So there are  $(11C4) + (11C5)$  selections in total.

So  $(11C4) + (11C5) = (12C5)$

In general:

$$(mCk) + (mC(k+1)) = ((m+1)C(k+1))$$

### Example 3

We have 4 books and we want to select some (or none) of them.

Method 1:

There are  $(4C0)$  selections of 0 books.

There are  $(4C1)$  selections of 1 book.

There are  $(4C2)$  selections of 2 books.

There are  $(4C3)$  selections of 3 books.

There are  $(4C4)$  selections of 4 books.

So there are  $(4C0)+(4C1)+(4C2)+(4C3)+(4C4)$  selections in total.

Method 2:

For each book, there are 2 choices. Either the book is selected or the book is not selected.

So there are  $2^4$  selections in total.

So  $(4C0)+(4C1)+(4C2)+(4C3)+(4C4)=2^4$

In general:

$$(nC0)+(nC1)+(nC2)+\dots+(nCn)=2^n$$

## Recurrence Relations

### Example 1

We have a sequence of numbers  $u_1, u_2, u_3, \dots$

$u_1=3$  and  $u_{n+1}=4u_n+1$  This is a recurrence relation. If you know a number in this sequence then the recurrence relation will tell you how to calculate the next number in this sequence.

Now  $u_1=3$

put  $n=1$  into  $u_{n+1}=4u_n+1$  and we get  $u_2=4u_1+1=(4\times 3)+1=13$

put  $n=2$  into  $u_{n+1}=4u_n+1$  and we get  $u_3=4u_2+1=(4\times 13)+1=53$

put  $n=3$  into  $u_{n+1}=4u_n+1$  and we get  $u_4=4u_3+1=(4\times 53)+1=213$

etc

### Example 2

We can define factorials using a recurrence relation:

$$1!=1 \quad (n+1)!=(n+1)n!$$

Now  $1!=1$

put  $n=1$  into  $(n+1)!=(n+1)n!$  and we get  $2!=(2)1!=2\times 1=2$

put  $n=2$  into  $(n+1)!=(n+1)n!$  and we get  $3!=(3)2!=3\times 2=6$

put  $n=3$  into  $(n+1)!=(n+1)n!$  and we get  $4!=(4)3!=4\times 6=24$

etc

Many problems give rise to recurrence relations as will see in the next few sections.

### Exercise

Write down the first 5 terms of the sequence

$$u_1=2 \text{ and } u_2=3 \quad u_{n+2}=u_n \times u_{n+1}$$

### Solution

$$u_1=2$$

$$u_2=3$$

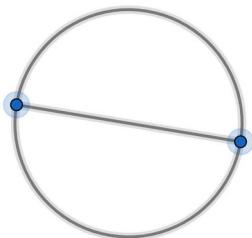
$$u_3=u_1 \times u_2=2 \times 3=6$$

$$u_4=u_2 \times u_3=3 \times 6=18$$

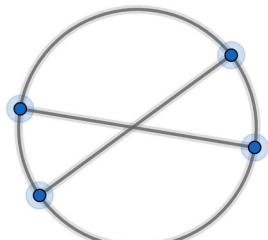
$$u_5=u_3 \times u_4=6 \times 18=108$$

## Cutting a Pizza

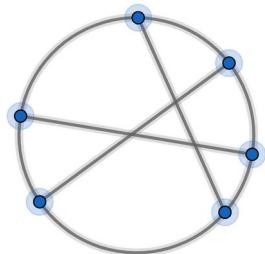
We have a pizza. We run the pizza cutter, in a straight line, across the pizza.  
With 1 cut, we get 2 pieces.



With 2 cuts, we get a maximum of 4 pieces.



With 3 cuts, we get a maximum of 7 pieces.



We want the maximum number of pieces, so we want each cut to cross over all the other cuts and we don't want three or more cuts to cross at the same point.

With 4 cuts?

The fourth cut must cross the other 3 cuts, so it must pass through 4 pieces of pizza. Each of these pieces is cut into two pieces, adding 4 more pieces.

Let  $P_4$  be the maximum number of pieces with 4 cuts.

$$\text{So } P_4 = P_3 + 4 \quad \text{So } P_4 = P_3 + 4 = 7 + 4 = 11$$

In general:

$$P_1=2 \quad \text{and} \quad P_{n+1}=P_n+(n+1)$$

We want a formula for  $P_n$ . We will use the guess and prove method.

Guess:

$$P_n=\frac{1}{2}n(n+1)+1$$

### EXERCISE

Use proof by induction to show that this guess is correct

### SOLUTION

Proof part 1:

If  $n=1$  then  $LHS=P_1=2$  and  $RHS=\frac{1}{2}(1)(2)+1=2$  So the formula is true when  $n=1$

Proof part 2:

If  $P_n=\frac{1}{2}n(n+1)+1$  is true when  $n=k$  then:

$$P_k=\frac{1}{2}k(k+1)+1 \quad \text{but} \quad P_{k+1}=P_k+(k+1)$$

$$P_{k+1}=\frac{1}{2}k(k+1)+1+(k+1)=\dots=\frac{1}{2}(k+1)(k+2)+1$$

So  $P_n=\frac{1}{2}n(n+1)+1$  is true when  $n=k+1$

So our guess is correct.

## Tower of Hanoi



We have three posts. There are some discs on one of these posts. These discs are all different sizes. The discs are in order of size with the largest disc at the bottom and the smallest disc is at the top. We want to move all the discs from this post to another post. However, we can only move one disc at at time and we cannot put a disc on top of a smaller disc.

Let's call the discs A, B, C, ... with disc A being the smallest, disc B being the next smallest ...

We start with two discs, A and B on post 1. We make these moves:

A to post 2 then B to post 3 then A to post 3. Try it.

Now the discs are all on post 3. So to move two discs we need three moves.

We start with three discs, A and B and C on post 1. We make these moves:

A to post 2 then B to post 3 then A to post 3 then C to post 2 then A to post 1 then B to post 2 then A to post 2. Try it.

Now the discs are all on post 3. So to move three discs we need seven moves.

I'm not going to write out all the moves required to transfer four discs. It's time to stop and think.

We start with four discs A and B and C and D on post 1. To move D, we first have to move A, B and C to another post. We know this takes seven moves. Then we have to move D. This takes one move.

Then we have to move A, B and C back on top of D. This takes another seven moves.

So to move four discs we need  $7+1+7=15$  moves.

Let  $M(n)$  be the number of moves to move  $n$  discs.

So  $M_4 = 2M_3 + 1$

In general:

$$M_1 = 1 \text{ and } M_{n+1} = 2M_n + 1$$

We want a formula for  $M(n)$ . We will use the guess and prove method.

Guess:

$$M_n = 2^n - 1$$

## EXERCISE

Use proof by induction to show that this guess is correct

## SOLUTIONS

Proof part 1:

If  $n=1$  then  $LHS=M_1=1$  and  $RHS=2^1-1=1$  So the formula is true when  $n=1$

Proof part 2:

If  $M_n=2^n-1$  is true when  $n=k$  then:

$$M_k=2^k-1 \text{ but } M_{k+1}=2M_k+1$$

$$M_{k+1}=2(2^k-1)+1=2^{k+1}-1$$

So  $M_n=2^n-1$  is true when  $n=k+1$

So our guess is correct.

## Derangements

There are five people A, B, C, D, E and each person has a card.

A's card has a 1 printed on it, B's card has a 2 printed on it ... etc

We collect in the cards, shuffle them up, and then give everyone a card.

How many possible derangements are there?

A derangement is where no-one ends up with their own card.

Let  $D_n$  be the number of ways of deranging  $n$  cards.

What if A swaps cards with another person?

For example, A gets card 3 and C gets card 1

We are now left with three people B, D, E and three cards 2, 4, 5

B could get card 4 or 5 but not card 2

D could get card 2 or 5 but not card 4

E could get card 2 or 4 but not card 5

This gives us  $D_3$  possible derangements.

A gets card 2 and B gets card 1                     $D_3$  derangements

A gets card 3 and C gets card 1                     $D_3$  derangements

A gets card 4 and D gets card 1                     $D_3$  derangements

A gets card 5 and E gets card 1                     $D_3$  derangements

This gives a total of  $4D_3$  derangements

What if A does not swap cards with another person?

For example, A gets card 3 but C does not get card 1.

We are now left with four people B, C, D, E and four cards 1, 2, 4, 5

B could get card 1 or 4 or 5 but not card 2

C could get card 2 or 4 or 5 but not card 1 (because this would be a swap)

D could get card 1 or 2 or 5 but not card 4

E could get card 1 or 2 or 4 but not card 5

This gives us  $D(4)$  possible derangements.

A gets card 2 but B does not get card 1             $D_4$  derangements

A gets card 3 but C does not get card 1             $D_4$  derangements

A gets card 4 but D does not get card 1             $D_4$  derangements

A gets card 5 but E does not get card 1             $D_4$  derangements

This gives a total of  $4D_4$  derangements

So  $D_5 = 4D_3 + 4D_4$

In general:

$$D_1 = 0 \text{ and } D_2 = 1 \text{ and } D_{n+2} = (n+1)D_n + (n+1)D_{n+1}$$

We want a formula for  $D_n$ . We will use the guess and prove method.

Guess:

$$D_n = n! \left( 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \dots + \frac{1}{n!} \right) \quad (\text{where did this come from?})$$

Proof:

$$D_1 = 1! \left( 1 - \frac{1}{1!} \right) = 0 \quad \text{Correct}$$

$$D_2 = 2! \left( 1 - \frac{1}{1!} + \frac{1}{2!} \right) = 1 \quad \text{Correct}$$

$$(n+1)D_n + (n+1)D_{n+1} = \dots = D_{n+2} \quad \text{Correct (you do this - it is very tedious!)}$$

Now  $\frac{1}{e} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \frac{1}{5!} + \dots$  (see chapter: e)

So if  $n$  is large  $D_n \approx n! \left( \frac{1}{e} \right)$

Instead of asking about the number of derangements, we can ask about the probability of getting a derangement.

There are  $n$  people and each person owns a card. We collect in the cards, shuffle them up, and then give everyone a card. What is the probability of getting a derangement?

There are  $D_n$  ways of getting a derangement and there are  $n!$  ways of giving out the cards.

So the probability of getting a derangement is  $\frac{D_n}{n!}$

So if  $n$  is large, the probability of getting a derangement is approximately  $1/e$

### Exercise

1) I write out my thirty Christmas cards and then I write out all the envelopes. Foolishly, I put the cards into the envelopes at random.

What is the probability that all my friends get sent the wrong card?

2) You and I each have a pack of cards. Both packs are shuffled. We then play Snap. What is the probability that we get to the end of our packs with no snaps?

Answer is approximately  $1/e$

3) Twenty students go to a party. When they arrive, each student drops their coat on the floor. When they leave, each student grabs a coat at random. What is the probability that no student gets their own coat?

Answer is approximately  $1/e$

Solutions

1) Answer is approximately  $1/e$

2) Answer is approximately  $1/e$

3) Answer is approximately  $1/e$

## Fibonacci Numbers

The Fibonacci numbers:

1, 1, 2, 3, 5, 8, 13, ... are given by the recurrence relation:

$$F_1 = 1 \quad F_2 = 1 \quad F_{n+2} = F_{n+1} + F_n$$

So:

$$F_3 = F_2 + F_1 \quad \text{and} \quad F_4 = F_3 + F_2 \quad \text{and} \quad F_5 = F_4 + F_3 \quad \text{etc}$$

We want a formula for  $F_n$ . We will use the guess and prove method.

Guess:

$$F_n = \frac{a^n - b^n}{\sqrt{5}} \quad \text{where} \quad a = \frac{1 + \sqrt{5}}{2} \quad \text{and} \quad b = \frac{1 - \sqrt{5}}{2} \quad (\text{where did that come from?})$$

Proof:

Consider the equation  $x^2 = x + 1$  (where did that come from?)

Solving with the quadratic equation formula gives:

$$x = \frac{1 \pm \sqrt{5}}{2} \quad \text{so} \quad x = a \quad \text{or} \quad x = b$$

Now:

$a$  and  $b$  satisfy  $x^2 = x + 1$

So:

$$a^2 = a^1 + 1 \quad a^3 = a^2 + a^1 \quad \dots \quad a^{n+2} = a^{n+1} + a^n$$

And:

$$b^2 = b^1 + 1 \quad b^3 = b^2 + b^1 \quad \dots \quad b^{n+2} = b^{n+1} + b^n$$

According to our guess:

$$F_1 = \frac{a^1 - b^1}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1$$

Correct

$$F_2 = \frac{a^2 - b^2}{\sqrt{5}} = \frac{(a^1 + 1) - (b^1 + 1)}{\sqrt{5}} = \frac{a^1 - b^1}{\sqrt{5}} = 1$$

Correct

$$F_{n+2} = \frac{a^{n+2} - b^{n+2}}{\sqrt{5}} = \frac{(a^{n+1} + a^n) - (b^{n+1} + b^n)}{\sqrt{5}} = \frac{(a^{n+1} - b^{n+1}) + (a^n - b^n)}{\sqrt{5}} = F_{n+1} + F_n$$

Correct

Let's look at the ratio of consecutive Fibonacci numbers:

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \dots$$

As  $n \rightarrow \infty$  these ratios tend to a limit called  $\phi$

Now:

$$F_{n+2} = F_{n+1} + F_n \text{ so } \frac{F_{n+2}}{F_{n+1}} = \frac{F_{n+1}}{F_{n+1}} + \frac{F_n}{F_{n+1}} \text{ so } \frac{F_{n+2}}{F_{n+1}} = 1 + \frac{F_n}{F_{n+1}}$$

$$\text{Letting } n \rightarrow \infty \text{ we get } \phi = 1 + \frac{1}{\phi} \text{ so } \phi^2 = \phi + 1 \text{ so } \phi = \frac{1 + \sqrt{5}}{2}$$

Note:

$\phi$  is called the golden ratio. Look it up!

Theorem:

If  $F_n$  is prime then  $n$  is prime.

The converse of this theorem is not true – for example  $F_{19}$  is not prime.

Conjecture:

There are an infinite number of Fibonacci numbers that are prime.

## EXERCISE

1) Write the Fibonacci sequence in mod 2.

Show that the 3<sup>rd</sup>, 6<sup>th</sup>, 9<sup>th</sup>, 12<sup>th</sup> ... Fibonacci numbers are all multiples of 2

2) Write the Fibonacci sequence in mod 3.

Show that the 4<sup>th</sup>, 8<sup>th</sup>, 12<sup>th</sup>, 16<sup>th</sup> ... Fibonacci numbers are all multiples of 3

3) Write the Fibonacci sequence in mod 5.

Show that the 5<sup>th</sup>, 10<sup>th</sup>, 15<sup>th</sup>, 20<sup>th</sup> ... Fibonacci numbers are all multiples of 5

4)

If  $d$  is a factor of  $F_{17}$  and  $F_{18}$  show that  $d$  is a factor of  $F_{16}$

If  $d$  is a factor of  $F_{16}$  and  $F_{17}$  show that  $d$  is a factor of  $F_{15}$

Show that consecutive Fibonacci numbers have no common factor.

5)

$$F_1 = F_3 - F_2$$

$$F_2 = F_4 - F_3$$

$$F_3 = F_5 - F_4$$

...

$$F_{n-1} = F_{n+1} - F_n$$

$$F_n = F_{n+2} - F_{n+1}$$

Show that:

$$F_1 + F_2 + F_3 + \dots + F_n = F_{n+2} - 1$$

## SOLUTIONS

1) mod 2:

1, 1, 0, 1, 1, 0, 1, 1, ...

The sequence must now repeat because we are back to 1, 1

So the 3<sup>rd</sup>, 6<sup>th</sup>, 9<sup>th</sup>, 12<sup>th</sup> ... terms are all multiples of 2

2) mod 3:

1, 1, 2, 0, 2, 2, 1, 0, 1, 1, ...

The sequence must now repeat because we are back to 1, 1

So the 4<sup>th</sup>, 8<sup>th</sup>, 12<sup>th</sup>, 16<sup>th</sup> ... terms are all multiples of 3

3) mod 5:

1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3, 2, 0, 2, 2, 4, 1, 0, 1, 1, ...

The sequence must now repeat because we are back to 1, 1

So the 5<sup>th</sup>, 10<sup>th</sup>, 15<sup>th</sup>, 20<sup>th</sup> ... terms are all multiples of 5

4)

$d$  is a factor of  $F_{16}$  because  $F_{16} = F_{18} - F_{17}$

$d$  is a factor of  $F_{15}$  because  $F_{15} = F_{17} - F_{16}$

etc

$d$  is a factor of  $F_1$

So consecutive Fibonacci numbers have no common factor

5)

add up the left-hand-sides:  $F_1 + F_2 + F_3 + \dots + F_n$

add up the right-hand -sides:  $F_{n+2} - F_2$

$$F_1 + F_2 + F_3 + \dots + F_n = F_{n+2} - F_2$$

$$F_1 + F_2 + F_3 + \dots + F_n = F_{n+2} - 1$$

## Polygonal numbers

The triangle numbers:

1,3,6,10,15,... are given by the recurrence relation:

$$T_1=1 \text{ and } T_{n+1}=T_n+n+1$$

So:

$$T_2=T_1+2 \text{ and } T_3=T_2+3 \text{ and } T_4=T_3+4 \text{ etc}$$

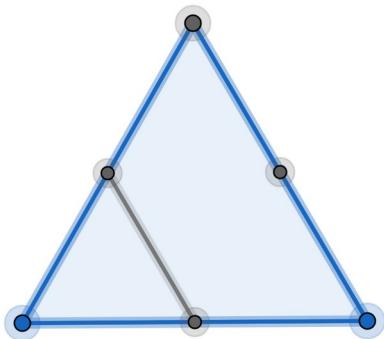
So:

$$T_4=T_3+4=(T_2+3)+4=((T_1+2)+3)+4=1+2+3+4$$

In general:

$$T_n=1+2+3+\dots+n$$

NEED BETTER DIAGRAM



Theorem:

$$T_n=\frac{1}{2}n(n+1)$$

Proof (by induction)

part 1:

If  $n=1$  then:

$$LHS=T_1=1 \text{ and } RHS=\frac{1}{2}(1)(2)=1 \text{ So the formula is true when } n=1$$

part 2:

If  $T_n=\frac{1}{2}n(n+1)$  is true when  $n=k$  then:

$$T_k=\frac{1}{2}k(k+1) \text{ but } T_{k+1}=T_k+k+1$$

So:

$$T_{k+1} = \frac{1}{2}k(k+1) + k+1 = \dots = \frac{1}{2}(k+1)(k+2)$$

So:

$$T_n = \frac{1}{2}n(n+1) \text{ is true when } n=k+1$$

The square numbers:

1, 4, 9, 16, 25, ... are given by the recurrence relation:

$$S_1 = 1 \text{ and } S_{n+1} = S_n + 2n + 1$$

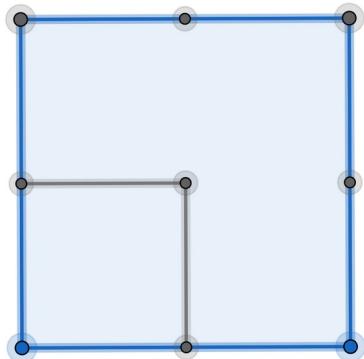
So:

$$S_2 = S_1 + 3 \text{ and } S_3 = S_2 + 5 \text{ and } S_4 = S_3 + 7 \text{ etc}$$

Show that:

$$S_n = 1 + 3 + 5 + \dots + (2n - 1)$$

NEED BETTER DIAGRAM



Theorem:

$$S_n = \frac{1}{2}n(2n) \text{ or if you prefer } S_n = n^2$$

see Exercise 1

The pentagonal numbers:

1, 5, 12, 22, 35, ... are given by the recurrence relation:

$$P_1 = 1 \text{ and } P_{n+1} = P_n + 3n + 1$$

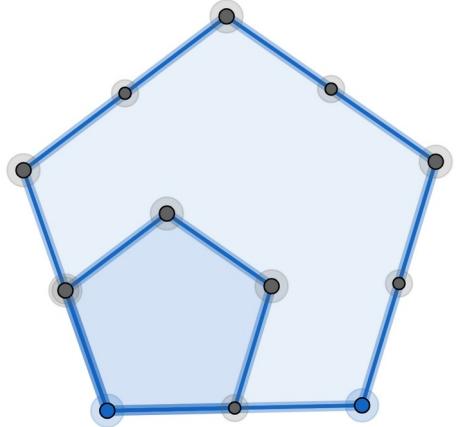
So:

$$P_2 = P_1 + 4 \text{ and } P_3 = P_2 + 7 \text{ and } P_4 = P_3 + 10 \text{ etc}$$

Show that:

$$P_n = 1 + 4 + 7 + \dots + (3n - 2)$$

NEED BETTER DIAGRAM



Theorem:

$$P_n = \frac{1}{2}n(3n - 1)$$

The hexagonal numbers:

1, 6, 15, 28, 45, ... are given by the recurrence relation:

$$H_1 = 1 \text{ and } H_{n+1} = H_n + 4n + 1$$

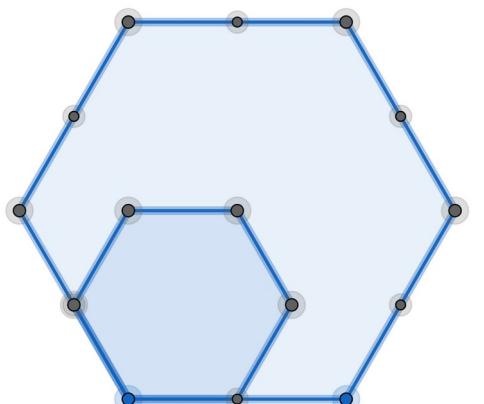
So:

$$H_2 = H_1 + 5 \text{ and } H_3 = H_2 + 9 \text{ and } H_4 = H_3 + 13 \text{ etc}$$

Show that:

$$H_n = 1 + 5 + 9 + \dots + (4n - 3)$$

NEED BETTER DIAGRAM



Theorem:

$$H_n = \frac{1}{2}n(4n-2)$$

The polygonal number theorem (difficult to prove)

Every positive integer can be written as the sum of:

- 3 (or fewer) triangle numbers
- 4 (or fewer) square numbers
- 5 (or fewer) pentagonal numbers

etc

see Exercise 2

### EXERCISE 1

Square numbers:

Show that  $S_n = \frac{1}{2}n(2n)$  Use proof by induction

### EXERCISE 2

Prove the following:

1. The sum of two consecutive triangle numbers is a square number.
2. If  $T$  is a triangle number then  $8T+1$  is a square number.
3. If  $T$  is a triangle number then  $9T+1$  is a triangle number.
4. The difference of the squares of two consecutive triangle numbers is a cube.
5.  $P_n = T_n + 2T_{n-1}$
6.  $H_n = T_n + 3T_{n-1}$
7. The last digit of a triangle number can't be 2, 4, 7 or 9

### SOLUTIONS 1

Proof (by induction)

part 1:

If  $n=1$  then  $LHS=S_1=1$  and  $RHS=\frac{1}{2}(1)(2)=1$  So the formula is true when  $n=1$

part 2:

If  $S_n = \frac{1}{2}n(2n)$  is true when  $n=k$  then:

$$S_k = \frac{1}{2}k(2k) \text{ but } S_{k+1} = S_k + 2k + 1$$

$$\text{So } S_{k+1} = \frac{1}{2}k(2k) + 2k + 1 = \dots = \frac{1}{2}(k+1)2(k+1)$$

$$\text{So } S_n = \frac{1}{2}n(2n) \text{ is true when } n=k+1$$

## SOLUTIONS 2

$$1) T_k + T_{k+1} = \frac{1}{2}k(k+1) + \frac{1}{2}(k+1)(k+2) = \dots = (k+1)^2$$

Or:

In this diagram we have got:  $T_5$  Ps and  $T_6$  Qs

How many letters have we got?

Q	Q	Q	Q	Q	Q
P	Q	Q	Q	Q	Q
P	P	Q	Q	Q	Q
P	P	P	Q	Q	Q
P	P	P	P	Q	Q
P	P	P	P	P	Q

$$T_5 + T_6 = 6^2$$

$$\text{In general } T_k + T_{k+1} = (k+1)^2$$

$$2) 8T_k + 1 = 8\frac{1}{2}k(k+1) + 1 = \dots = (2k+1)^2$$

$$3) 9T_k + 1 = 9\frac{1}{2}k(k+1) + 1 = \dots = \frac{1}{2}(3k+1)(3k+2)$$

$$4) (T_{k+1})^2 - (T_k)^2 = \left(\frac{1}{2}(k+1)(k+2)\right)^2 - \left(\frac{1}{2}k(k+1)\right)^2 = \dots = (k+1)^3$$

$$5) P_n = \frac{1}{2}n(3n-1)$$

$$T_n + 2T_{n-1} = \frac{1}{2}n(n+1) + 2\frac{1}{2}(n-1)n = \dots = \frac{1}{2}n(3n-1)$$

$$6) \quad H_n = \frac{1}{2}n(4n-2)$$

$$T_n + 3T_{n-1} = \frac{1}{2}n(n+1) + 3\frac{1}{2}(n-1)n = \dots = \frac{1}{2}n(4n-2)$$

7) mod 10:

$n$	0	1	2	3	4	5	6	7	8	9
$n+1$	1	2	3	4	5	6	7	8	9	0
$n(n+1)$	0	2	6	2	0	0	2	6	2	0

now  $T = \frac{1}{2}n(n+1)$  so  $2T = n(n+1)$  so the last digit of  $2T$  is 0, 2 or 6

mod 10:

$T$	0	1		3		5	6		8	
$2T$	0	2		6		0	2		6	

If the last digit of  $2T$  is 0, 2 or 6 then the last digit of  $T$  must be 0, 1, 3, 5, 6 or 8

A Nice Integral      if you have studied integration ...

$$I_n = \int_0^\infty x^n e^{-x} dx$$

Use integration by parts to show that:

$$I_n = n I_{n-1}$$

So:

$$I_8 = 8 \times I_7 = 8 \times 7 \times I_6 = 8 \times 7 \times 6 \times I_5 = \dots = 8!$$

In general:

$$I_n = n!$$

Now:

$$n! = 1 \times 2 \times 3 \dots \times n$$

This only makes sense if  $n$  is a positive integer.

$$I_n = \int_0^\infty x^n e^{-x} dx$$

This makes sense for any value of  $n$

So, for example:

$$(-1)! = \int_0^\infty x^{-1} e^{-x} dx$$

I might not be able to work this out but it certainly has a value.

## Magic Squares

### Example 1

Here is a  $4 \times 4$  magic square:

1	15	14	4
12	6	7	9
8	10	11	5
13	3	2	16

The numbers in each column, each row and both diagonals add up to the same total.

Now  $1+2+3+\dots+16=136$  Our sixteen numbers are arranged in four columns so the numbers in each column (and each row and both diagonals) must add up to  $136/4=34$

### Example 2

We want to arrange the numbers  $1, 2, 3, \dots, 9$  into a  $3 \times 3$  magic square.

Now  $1+2+3+4+5+6+7+8+9=45$  Our nine numbers are arranged in three columns so the numbers in each column (and each row and both diagonals) must add up to  $45/3=15$

### Theorem

5 must go in the middle cell.

### Proof

A	B	C
D	E	F
G	H	I

$$A+E+I=15 \quad C+E+G=15 \quad B+E+H=15 \quad D+E+F=15$$

$$\text{So } A+E+I+C+E+G+B+E+H+D+E+F=60$$

$$\text{But } A+B+C+D+E+F+G+H+I=45 \text{ so } E=5$$

Show that we cannot put 9 in the same column/row/diagonal as 8 or 7 or 6 or 3.

Put 9 in a corner. Now 1 must go in the opposite corner. What numbers can go in the other corners?

Show that 9 cannot go in a corner. So 9 must go in the middle of a side.

Put 3 in a corner. Show that 3 cannot go in a corner. So 3 must go in the middle of a side.

Where can we put 8?

Now complete the magic square.

I got:

8	3	4
1	5	9
6	7	2

And let's say you got:

4	3	8
9	5	1
2	7	6

We would say these are the same. Two magic squares are the same if we can change the first square into the second square by rotating the first square about its centre or by reflecting the first square about any mirror line passing through its centre.

A magic square will remain magic if:

- we add  $k$  to all the numbers in the square, for any number  $k$
- we multiply all the numbers in the square by  $k$  for any number  $k$
- we swap 2 rows that are equidistant from the centre
- we swap 2 columns that are equidistant from the centre

Try it!

Back to my  $3 \times 3$  magic square.

If we add 9 to each number in my  $3 \times 3$  magic square then we get a magic square with the numbers: 10 ... 18

17	12	13
10	14	18
15	16	11

If we add another 9 to each number then we get a magic square with the numbers: 19 ... 27

If we add another 9 to each number then we get a magic square with the numbers: 28 ... 36

...

If we add another 9 to each number then we get a magic square with the numbers: 73 ... 81

We can now assemble these nine magic squares into a  $9 \times 9$  magic square:

(look carefully to see how I've arranged the nine magic squares)

71	66	67	26	21	22	35	30	31
64	68	72	19	23	27	28	32	36
69	70	65	24	25	20	33	34	29
8	3	4	44	39	40	80	75	76
1	5	9	37	41	45	73	77	81
6	7	2	42	43	38	78	79	74
53	48	49	62	57	58	17	12	13
46	50	54	55	59	63	10	14	18
51	52	47	60	61	56	15	16	11

Here is a method to find a  $N \times N$  magic square if  $N$  is a multiple of 4.

Start with this square:

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32
33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64

Divide this square into four  $4 \times 4$  squares.

Look at the numbers on the diagonals of these  $4 \times 4$  squares:

1, 10, 19, 28 and 4, 11, 18, 25

5, 14, 23, 32 and 8, 15, 22, 29

33, 42, 51, 60 and 36, 43, 50, 57

37, 46, 55, 64 and 40, 47, 54, 61

Swap any two of these numbers that add up to 65.

swap: 1 and 64      swap: 10 and 55      swap: 19 and 46      etc

This gives us the magic square:

64	2	3	61	60	6	7	57
9	55	54	12	13	51	50	16
17	47	46	20	21	43	42	24
40	26	27	37	36	30	31	33
32	34	35	29	28	38	39	25
41	23	22	44	45	19	18	48
49	15	14	52	53	11	10	56
8	58	59	5	4	62	63	1

There are many other methods to find magic squares. Look them up.

Here is my favourite magic square:

7	53	41	27	2	52	48	30
12	58	38	24	13	63	35	17
51	1	29	47	54	8	28	42
64	14	18	36	57	11	23	37
25	43	55	5	32	46	50	4
22	40	60	10	19	33	61	15
45	31	3	49	44	26	6	56
34	20	16	62	39	21	9	59

It remains magic if all the numbers are squared!

## EXERCISE

Arrange the numbers  $1, 2, 3, \dots, 16$  into a  $4 \times 4$  magic square.

## SOLUTION

Start with the square:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

do the swaps to get:

16	2	3	13
5	11	10	8
9	7	6	12
4	14	15	1

## Latin Squares

### Example 1

Here is a  $4 \times 4$  Latin square:

A	B	C	D
B	A	D	C
C	D	A	B
D	C	B	A

There are four symbols A, B, C, D and each symbol appears once (and only once) in each row and once (and only once) in each column.

Latin squares are used in agricultural research. We are growing oats in a field and we want to compare four types of fertilizer, A, B, C, D. We divide the field into 16 plots and apply the fertilizer as in the Latin square. Conditions (drainage etc) might vary across the field, so we want to try each type of fertilizer in each row and each column of the field.

One way to make a Latin square is the diagonal method:

A	B	C	D	E	F
F	A	B	C	D	E
E	F	A	B	C	D
D	E	F	A	B	C
C	D	E	F	A	B
B	C	D	E	F	A

Look and see how each letter is arranged along diagonals.

See EXERCISE 1

## Sudoku Squares

Here is an incomplete sudoku square:

	H	I	E	G	C	D	F	B
F	G	D	I				A	E
E		C	A	F	D	H	I	
H	I				F	B	D	C
C	A	B	H	D		E		F
				E			H	
I		A			E		B	
B	E	G	D	I	A	F	C	
D				C		I	E	

There are nine symbols A, B, C, ... I. The challenge is to fill in the square to make a  $9 \times 9$  Latin square. But there is more. If you divide up the board into nine  $3 \times 3$  squares then each  $3 \times 3$  square must contain all nine symbols. So, for example, look at the top-left  $3 \times 3$  square:

	H	I
F	G	D
E		C

The two empty cells must contain A and B.

The nine symbols in a sudoku square are usually 1, 2, 3, 4, 5, 6, 7, 8, 9. I've chosen to use letters instead because this puzzle is not really about numbers.

There are just 5,524,751,496,156,892,842,531,225,600 possible  $9 \times 9$  Latin squares but only some of them are Sudoku squares.

See EXERCISE 2

### EXERCISE 1

Arrange the letters A, B, C, D, E into a  $5 \times 5$  Latin Square using the diagonal method.

## EXERCISE 2

Complete the above sudoku square

## SOLUTIONS 1

A	B	C	D	E
E	A	B	C	D
D	E	A	B	C
C	D	E	A	B
B	C	D	E	A

## SOLUTIONS 2

A	H	I	E	G	C	D	F	B
F	G	D	I	B	H	C	A	E
E	B	C	A	F	D	H	I	G
H	I	E	G	A	F	B	D	C
C	A	B	H	D	I	E	G	F
G	D	F	C	E	B	A	H	I
I	C	A	F	H	E	G	B	D
B	E	G	D	I	A	F	C	H
D	F	H	B	C	G	I	E	A

## Euler Squares

### Example 1

Here are two  $3 \times 3$  Latin squares:

A	B	C
C	A	B
B	C	A

a	b	c
b	c	a
c	a	b

We can combine them to form a  $3 \times 3$  Euler square:

A, a	B, b	C, c
C, b	A, c	B, a
B, c	C, a	A, b

Each cell contains two symbols and no two cells contain the same two symbols.

Euler squares are used in agricultural research. We are growing wheat in a field and we want to compare three types of wheat, a, b, c and three types of fertilizer, A, B, C. We want to grow each type of wheat with each type of fertilizer. We divide the field into 9 plots and plant the wheat and apply the fertilizer as in the Euler square. Conditions (drainage etc) might vary across the field, so we want to try each type of wheat and each type of fertilizer in each row and column of the field.

There are no  $2 \times 2$  Euler squares. Can you see why?

Euler tried, and failed, to find a  $6 \times 6$  Euler square.

In 1901 a proof was discovered that  $6 \times 6$  Euler squares do not exist.

In 1960 a proof was discovered that Euler squares exist for all sizes except  $2 \times 2$  and  $6 \times 6$

One way to make an Euler square is the double-diagonal method.

### Example 2

A	B	C	D	E
E	A	B	C	D
D	E	A	B	C
C	D	E	A	B
B	C	D	E	A

a	b	c	d	e
b	c	d	e	a
c	d	e	a	b
d	e	a	b	c
e	a	b	c	d

The first Latin square is diagonal from top-left to bottom-right. The other Latin square is diagonal from top-right to bottom-left.

We can combine these two Latin squares to make an Euler square:

A, a	B, b	C, c	D, d	E, e
E, b	A, c	B, d	C, e	D, a
D, c	E, d	A, e	B, a	C, b
C, d	D, e	E, a	A, b	B, c
B, e	C, a	D, b	E, c	A, d

Unfortunately, this method does not always work.

Investigation: When will the double-diagonal method work?

There are many other methods to find Euler squares. Look them up. (Euler squares are also called Graeco-Latin squares)

### EXERCISE

Take the 16 picture cards (jacks, queens, kings, aces of spades, hearts, clubs, diamonds) from a pack of cards. Arrange them in a  $4 \times 4$  Euler square:

a card of each suit must appear in each row and each column

a card of each rank must appear in each row and each column

## SOLUTIONS

There are many solutions. Here is mine. I tried the diagonal method but it did not work.

Ace, spade	King, heart	Queen, club	Jack, diamond
King, diamond	Ave club	Jack, heart	Queen, spade
Queen, heart	Jack, spade	Ace, diamond	King, club
Jack, club	Queen, diamond	King, spade	Ace, heart