From Euclid to Turing: proofs, truths and codes.

Prof. Mark Wildon

ROYAL HOLLOWAY UNIVERSITY OF LONDON

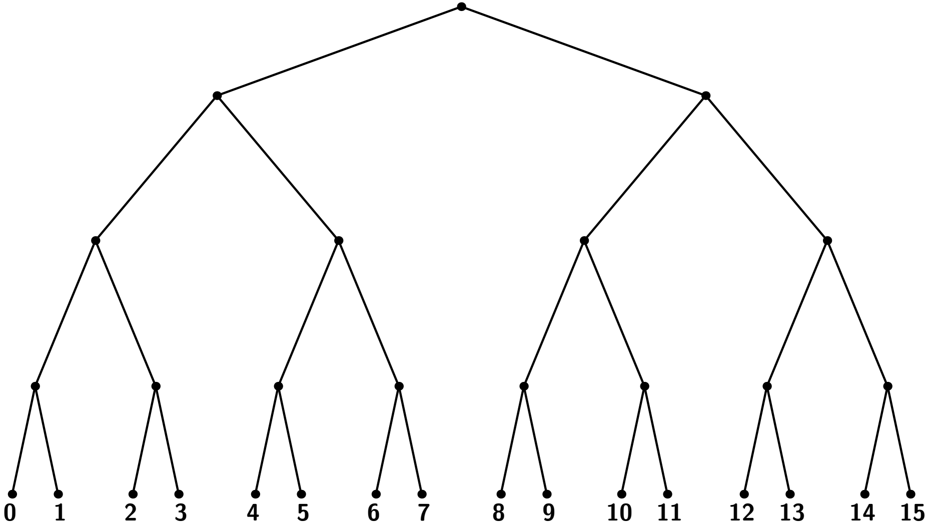
Heilbronn Institute for Mathematical Research

Guessing Games

Ask a friend to thinks of a number between 1 and 15. How many YES/NO questions do you need to ask to find out the secret number?

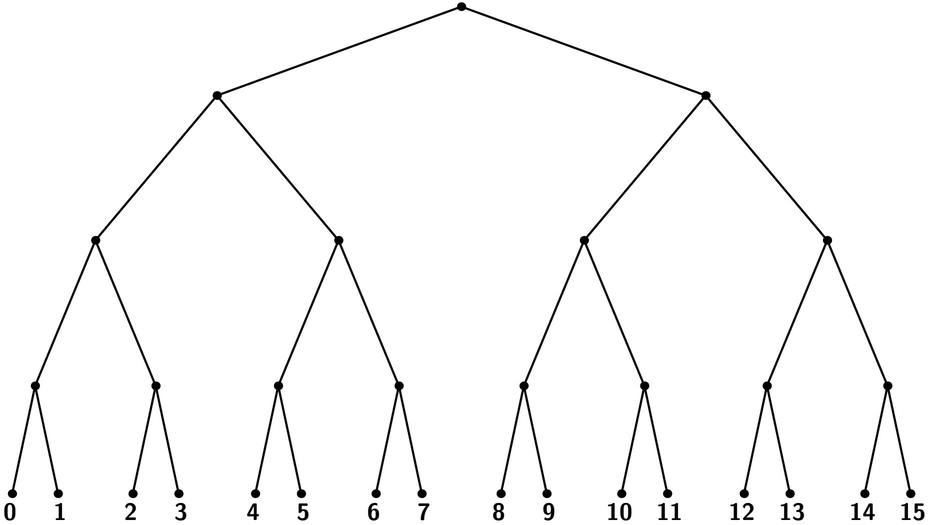
Guessing Games

Ask a friend to thinks of a number between 1 and 15. How many YES/NO questions do you need to ask to find out the secret number?



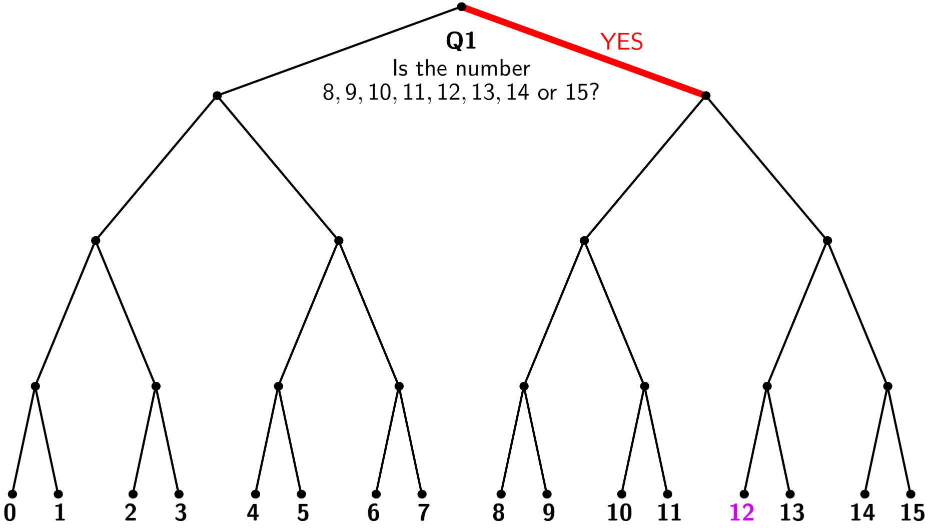
Guessing Games

Ask a friend to thinks of a number between 1 and 15. How many YES/NO questions do you need to ask to find out the secret number?



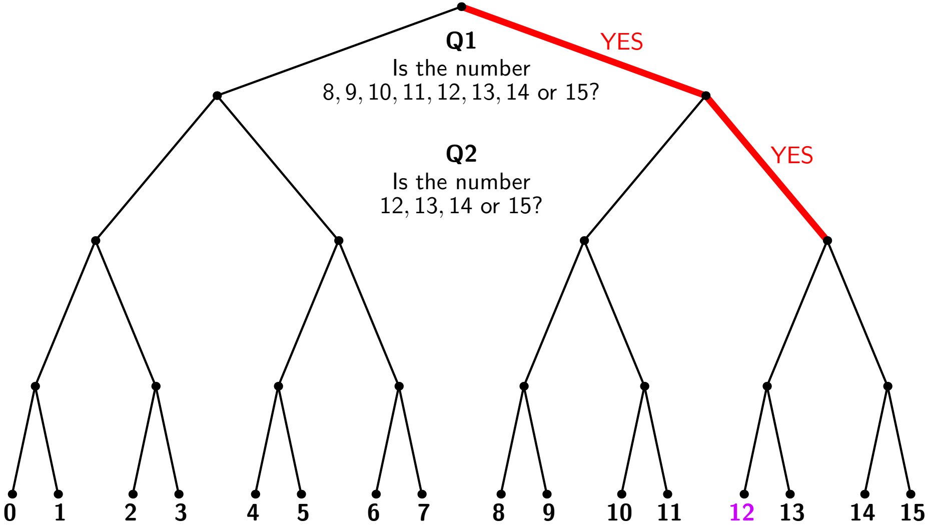
Guessing Games

Ask a friend to thinks of a number between 1 and 15. How many YES/NO questions do you need to ask to find out the secret number?



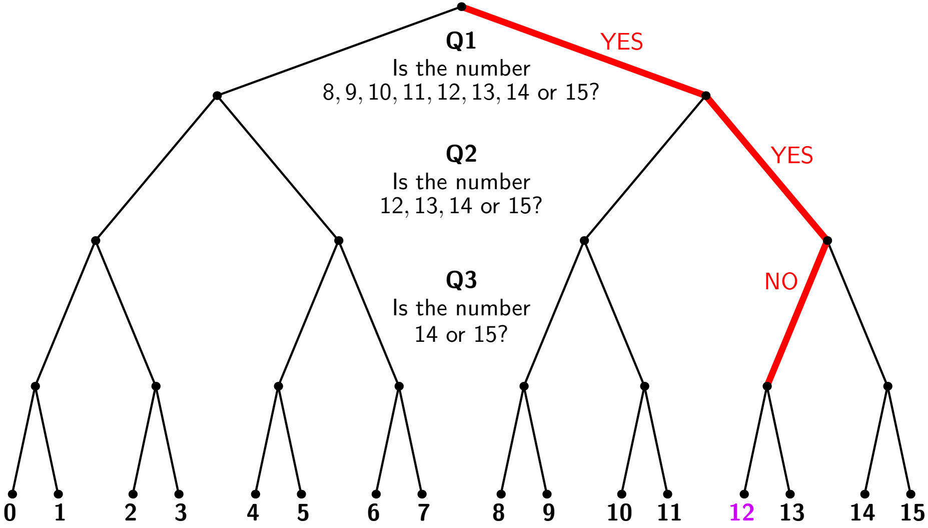
Guessing Games

Ask a friend to thinks of a number between 1 and 15. How many YES/NO questions do you need to ask to find out the secret number?



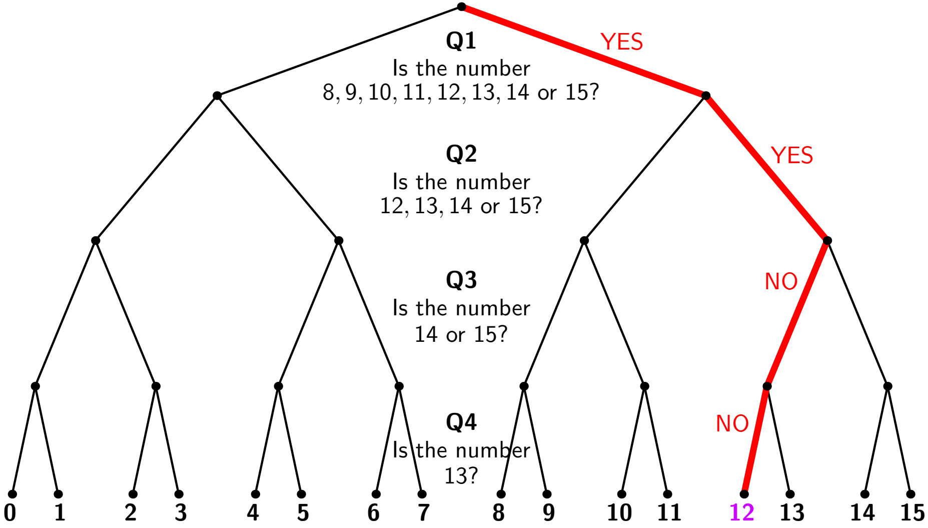
Guessing Games

Ask a friend to thinks of a number between 1 and 15. How many YES/NO questions do you need to ask to find out the secret number?



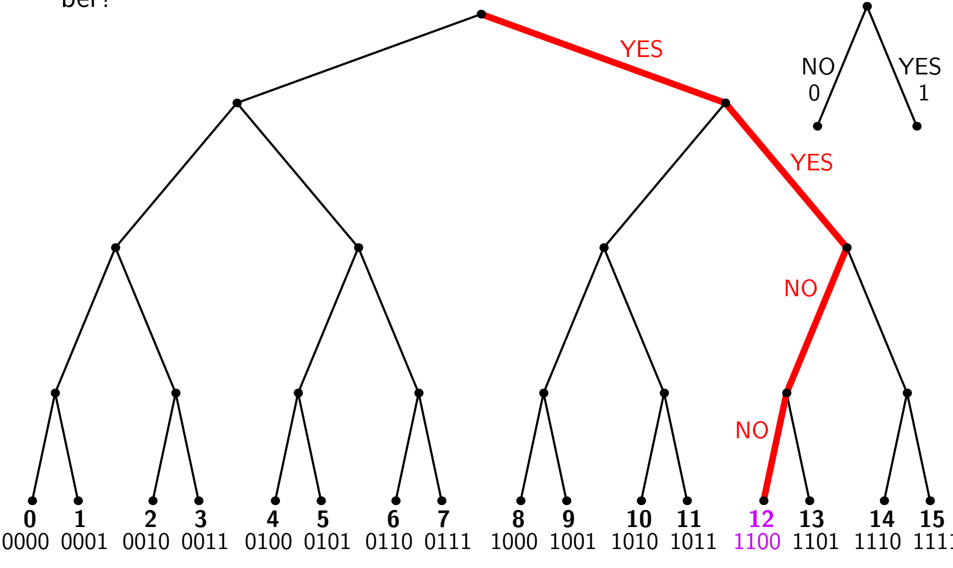
Guessing Games

Ask a friend to thinks of a number between 1 and 15. How many YES/NO questions do you need to ask to find out the secret number?



Guessing Games

Ask a friend to thinks of a number between 1 and 15. How many YES/NO questions do you need to ask to find out the secret number?



Why we need proofs

- True or false: $0.999999\ldots = 1$?
- I have equally full glasses of red wine and white wine.
  - I transfer a teaspoon of red wine to the white wine glass;
  - After stirring, I transfer a teaspoon of the mixture back to the red wine glass.

  Which glass is more contaminated with the wine from the other glass?

Spot the prime.

Spot the prime.

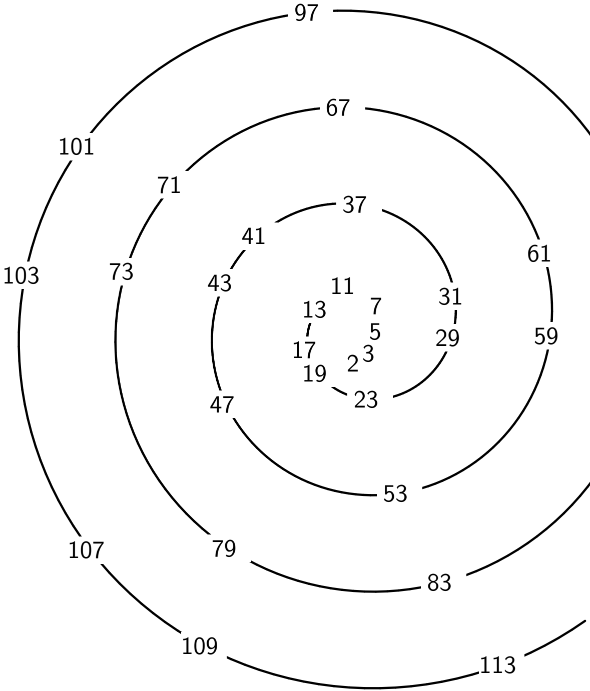
- 31 is prime

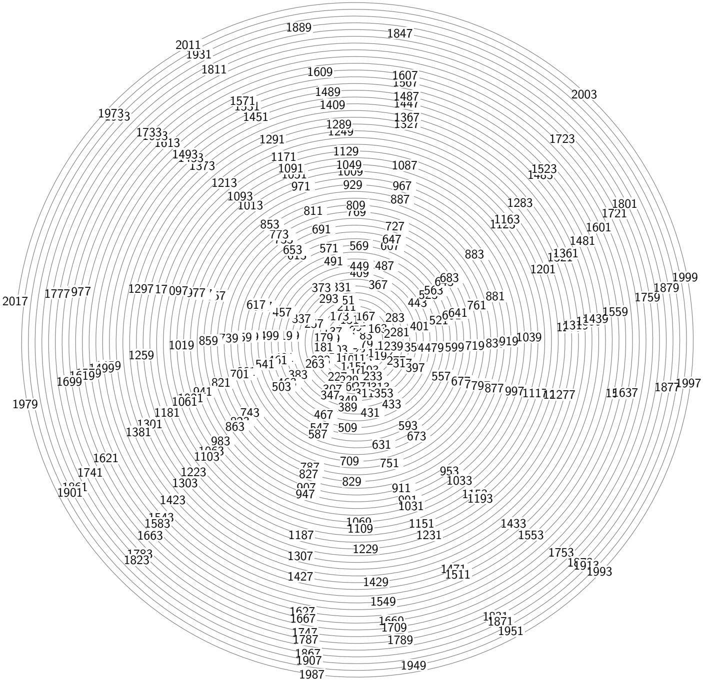
1 is not a prime

1 is not a prime — says who?

1 is not a prime — says who?

We want unique factorization, not $57 = 3 \times 19 = 1 \times 3 \times 19 = \cdots$.


2
3
5
7
11
13
17
19
23
29
31
37
41
43
47
53
59
61
67
71
73
79
83
89
97
101
103
107
109
113



1889
1847
2011
1931
1811
1609
1607
2003
1489
1487
1409
1447
1451
1367
1289
1291
1723
1129
1171
1049
1087
1091
1523
971
929
967
1213
887
1093
1013
809
1283
811
1801
1721
727
691
1163
1601
853
1481
569
647
571
653
883
1361
491
449
487
1201
1999
683
1879
367
1759
373
1297
2017
977
293
563
881
1559
617
761
457
443
641
1439
167
283
521
401
859
1019
1259
739
499
179
281
1039
599
719
919
181
479
1239
263
541
397
1979
1699
821
383
233
557
779
877
997
1277
1637
1877
1997
701
503
347
353
941
389
433
1061
1181
743
467
431
1301
1381
863
593
509
587
673
983
631
1103
1621
709
751
1741
1223
827
953
829
1033
1303
911
1901
947
1193
1423
1031
1583
1109
1151
1433
1663
1187
1231
1553
1229
1307
1753
1823
1427
1511
1993
1429
1549
1667
1871
1709
1951
1787
1789
1907
1949
1987

2, 3, 5, 7, 11, . . . , 2003, 2011, 2017, 2027, 2029, . . .

$$2, 3, 5, 7, 11, \ldots, 2003, 2011, 2017, 2027, 2029, \ldots, 1000000007, \ldots$$

2, 3, 5, 7, 11, . . . , 2003, 2011, 2017, 2027, 2029, . . . , 1000000007, . . .

- Does the sequence of primes ever stop?
- Or maybe there are infinitely many primes?

The first three primes are 2, 3, 5

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

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

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

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

30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

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

30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

- $30031 = 15015 \times 2 + 1$
- $30031 = 10010 \times 3 + 1$

  ...
- $30031 = 2310 \times 13 + 1$

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

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

30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

- $30031 = 15015 \times 2 + 1$
- $30031 = 10010 \times 3 + 1$

  ...
- $30031 = 2310 \times 13 + 1$

But 30031 is either prime or divisible by a prime

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

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

30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

- $30031 = 15015 \times 2 + 1$
- $30031 = 10010 \times 3 + 1$

  $\dots$
- $30031 = 2310 \times 13 + 1$

But 30031 is either prime or divisible by a prime ($30031 = 59 \times 209$)

The first three primes are 2, 3, 5

$2 \times 3 \times 5 = 30$

$2 \times 3 \times 5 + 1 = 31$

31 leaves remainder 1 when we divide it by 2, 3, 5

- $31 = 15 \times 2 + 1$
- $31 = 10 \times 3 + 1$
- $31 = 6 \times 5 + 1$

But 31 is either prime or divisible by a prime

So 2, 3, 5 are not all the primes

The first six primes are 2, 3, 5, 7, 11, 13

$2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$

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

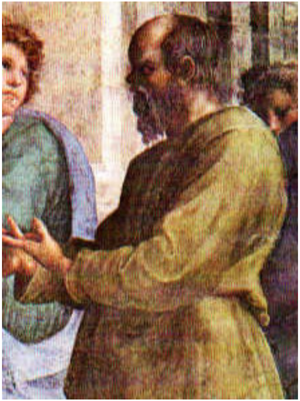
30031 leaves remainder 1 when we divide it by 2, 3, 5,7,11,13.

- $30031 = 15015 \times 2 + 1$
- $30031 = 10010 \times 3 + 1$

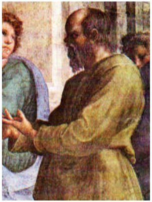
  $\dots$
- $30031 = 2310 \times 13 + 1$

But 30031 is either prime or divisible by a prime ($30031 = 59 \times 209$)

So 2, 3, 5, 7, 11, 13 are not all the primes

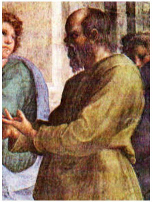


A fictional Socratic dialogue



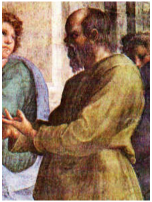
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes

A fictional Socratic dialogue



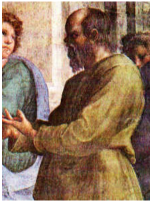
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$

A fictional Socratic dialogue



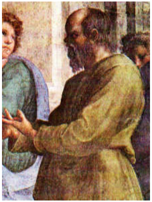
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must ...

A fictional Socratic dialogue



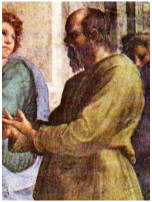
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must ...
- Euclid: N leaves remainder 1 when divided by all your primes

A fictional Socratic dialogue



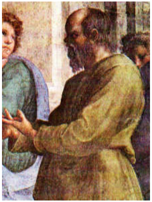
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must ...
- Euclid: N leaves remainder 1 when divided by all your primes
- Socrates: You are correct

A fictional Socratic dialogue



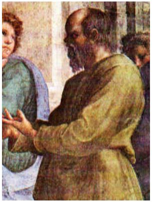
- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must ...
- Euclid: N leaves remainder 1 when divided by all your primes
- Socrates: You are correct
- Euclid: But N is divisible by some prime

A fictional Socratic dialogue



- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must ...
- Euclid: N leaves remainder 1 when divided by all your primes
- Socrates: You are correct
- Euclid: But N is divisible by some prime
- Socrates: Yes. So there is a prime not in my list

A fictional Socratic dialogue



- Socrates: I think $p_1, p_2, \ldots, p_r$ might be all the primes
- Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
- Socrates: If I must ...
- Euclid: N leaves remainder 1 when divided by all your primes
- Socrates: You are correct
- Euclid: But N is divisible by some prime
- Socrates: Yes. So there is a prime not in my list
- Euclid: Indeed. This shows there are more than any finite number of primes
- Socrates: You are correct

Binary and Computers

In a computer everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1.

Binary and Computers

In a computer everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers 'Yes', 'Yes', 'No', 'No'.

Books, music, videos, computer programs, bitcoins . . . , all become bits.

Binary and Computers

In a computer everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers ‘Yes’, ‘Yes’, ‘No’, ‘No’.

Books, music, videos, computer programs, bitcoins . . . , all become bits.

```
00001110 11101011 00100000 10101000 00101011 01100010 00100000 11101011
10101100 00100000 11101010 11101011 00101110 00100000 00101110 11101011
00100000 10101000 00101011 11100100 00100000 00101110 01101000 00101001
00101110 00100000 01101001 10101101 00100000 00101110 01101000 00101011
00100000 00101101 00101111 00101011 10101101 00101110 01101001 11101011
11101010 11100100 11000000 10001111 01101000 00101011 00101110 01101000
00101011 10101100 00100000 10100011 00101110 01101001 10101101 00100000
11101010 11101011 10101000 01101010 00101011 10101100 00100000 01101001
11101010 00100000 00101110 01101000 00101011 00100000 01101011 01101001
11101010 00101010 00100000 00101110 11101011 00100000 10101101 00101111
10101010 10101010 00101011 10101100 11000000 00001110 01101000 00101011
00100000 10101101 01101010 01101001 11101010 10101011 10101101 00100000
00101001 11101010 00101010 00100000 00101001 10101100 10101100 11101011
10101111 10101101 00100000 11101011 10101010 00100000 11101011 00101111
00101110 10101100 00101001 10101011 00101011 11101011 00101111 10101101
00100000 10101010 11101011 10101100 00101110 00101111 11101010 00101011
01100010
```

William Shakespeare (approx 1600)

Binary and Computers

In a computer everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers 'Yes', 'Yes', 'No', 'No'.

Books, music, videos, computer programs, bitcoins . . . , all become bits.

00001110 11101011 00100000 10101000 00101011 01100010 00100000 11101011
10101100 00100000 11101010 11101011 00101110 00100000 00101110 11101011
00100000 10101000 00101011 11100100 00100000 00101110 01101000 00101001
00101110 00100000 01101001 10101101 00100000 00101110 01101000 00101011
00100000 00101101 00101111 00101011 10101101 00101110 01101001 11101011
11101010 11100100 11000000 10001111 01101000 00101011 00101110 01101000
00101011 10101100 00100000 10100011 00101110 01101001 10101101 00100000
11101010 11101011 10101000 01101010 00101011 10101100 00100000 01101001
11101010 00100000 00101110 01101000 00101011 00100000 01101011 01101001
11101010 00101010 00100000 00101110 11101011 00100000 10101101 00101111
10101010 10101010 00101011 10101100 11000000 00001110 01101000 00101011
00100000 10101101 01101010 01101001 11101010 10101011 10101101 00100000
00101001 11101010 00101010 00100000 00101001 10101100 10101100 11101011
10101111 10101101 00100000 11101011 10101010 00100000 11101011 00101111
00101110 10101100 00101001 10101011 00101011 11101011 00101111 10101101
00100000 10101010 11101011 10101100 00101110 00101111 11101010 00101011
01100010

William Shakespeare (approx 1600)

To be, or not to be: that is the question:
Whether 'tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,

Binary and Computers

In a computer everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers ‘Yes’, ‘Yes’, ‘No’, ‘No’.

Books, music, videos, computer programs, bitcoins . . . , all become bits.

00001110	11101011	00100000	10101000	00101011	01100010	00100000	11101011
10101100	00100000	11101010	11101011	00101110	00100000	00101110	11101011
00100000	10101000	00101011	11100100	00100000	00101110	01101000	00101001
00101110	00100000	01101001	10101101	00100000	00101110	01101000	00101011
00100000	00101101	00101111	00101011	10101101	00101110	01101001	11101011
11101010	11100100	11000000	10001111	01101000	00101011	00101110	01101000
00101011	10101100	00100000	10100011	00101110	01101001	10101101	00100000
11101010	11101011	10101000	01101010	00101011	10101100	00100000	01101001
11101010	00100000	00101110	01101000	00101011	00100000	01101011	01101001
11101010	00101010	00100000	00101110	11101011	00100000	10101101	00101111
10101010	10101010	00101011	10101100	11000000	00001110	01101000	00101011
00100000	10101101	01101010	01101001	11101010	10101011	10101101	00100000
00101001	11101010	00101010	00100000	00101001	10101100	10101100	11101011
10101111	10101101	00100000	11101011	10101010	00100000	11101011	00101111
00101110	10101100	00101001	10101011	00101011	11101011	00101111	10101101
00100000	10101010	11101011	10101100	00101110	00101111	11101010	00101011
01100010							

William Shakespeare (approx 1600)

To be, or not to be: that is the question:
Whether ’tis nobler in the mind to suffer
The slings and arrows of outrageous fortune,

Binary and Computers

In a computer everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers 'Yes', 'Yes', 'No', 'No'.

Books, music, videos, computer programs, bitcoins . . . , all become bits.

00110000 01110111 01000110 10000000 00011000 00000001 01011101 00011110
10101100 00000000 10101110 00001011 10101100 00101011 01101011 01101001
00001110 00101110 10101100 00101001 00101110 10001101 00100100 00100101
10101100 00101011 01101011 01101001 00001110 00001111 10001000 01001011
01100100 11001010 11001100 11001111 11001111 00001000 00000101 00010100
00001100 00110000 01000000 01011010 00110000 11000010 00110000 00110000
10000000 00011010 00111010 00110000 10000110 10111101 00011010 10101100
00000000 00001011 00101110 10101001 00101011 11101000 10101000 11001011
10001001 10100111 10101001 10101010 11001011 10100101 11001010 01001001
00001110 11001100 11001111 11001111 00001000 00010100 10000001 01011010
00110000 01000101 00010001 01111010 00110000 10100101 01011010 10101100
00000000 00001011 11101010 11101011 01101001 00101110 00101100 00101011
10101001 01101100 00001011 10101111 11101011 01101010 10101010 10101100
00101011 10101110 11001011 10101100 00101011 10101011 00101011 00101110
11101010 01001001 10001001 00100111 10100100 10101001 10101010 11001011
10100101 11001010 01001001 00001110 11001100 11001111 11001111 00001000
00010100

Anonymous Microsoft Programmer (2010)

Binary and Computers

In a computer everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers ‘Yes’, ‘Yes’, ‘No’, ‘No’.

Books, music, videos, computer programs, bitcoins . . . , all become bits.

Part of the machine code for Microsoft Word 2011.

Binary and Computers

In a computer everything is stored as a lists of the **bits** (**bi**nary digi**ts**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers 'Yes', 'Yes', 'No', 'No'.

Books, music, videos, computer programs, bitcoins . . . , all become bits.

Why Coding Theory?

A bit gives a single piece of information: ‘NO’ or ‘YES’; ‘on’ or ‘off’; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000:
- Full text of *Hamlet*
- Pictures of Royal Holloway (compressed)
- Compact disc of Beethoven 9th
- Large Hadron Collider, per second

Why Coding Theory?

A bit gives a single piece of information: ‘NO’ or ‘YES’; ‘on’ or ‘off’; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000: 10 bits
- Full text of *Hamlet*
- Pictures of Royal Holloway (compressed)
- Compact disc of Beethoven 9th
- Large Hadron Collider, per second

Why Coding Theory?

A bit gives a single piece of information: ‘NO’ or ‘YES’; ‘on’ or ‘off’; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000: 10 bits
- Full text of *Hamlet* 1.5 million bits
- Pictures of Royal Holloway (compressed)
- Compact disc of Beethoven 9th
- Large Hadron Collider, per second

Why Coding Theory?

A bit gives a single piece of information: ‘NO’ or ‘YES’; ‘on’ or ‘off’; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000: 10 bits
- Full text of *Hamlet* 1.5 million bits
- Pictures of Royal Holloway (compressed) 5 million bits each
- Compact disc of Beethoven 9th
- Large Hadron Collider, per second

Why Coding Theory?

A bit gives a single piece of information: ‘NO’ or ‘YES’; ‘on’ or ‘off’; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000: 10 bits
- Full text of *Hamlet* 1.5 million bits
- Pictures of Royal Holloway 5 million bits each
- Compact disc of Beethoven 9th
- Large Hadron Collider, per second
- A quantum computer big enough to break public key cryptography

Why Coding Theory?

A bit gives a single piece of information: ‘NO’ or ‘YES’; ‘on’ or ‘off’; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000: 10 bits
- Full text of *Hamlet* 1.5 million bits
- Pictures of Royal Holloway 5 million bits each
- Compact disc of Beethoven 9th 6 billion bits
- Large Hadron Collider, per second
- A quantum computer big enough to break public key cryptography

Why Coding Theory?

A bit gives a single piece of information: ‘NO’ or ‘YES’; ‘on’ or ‘off’; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000: 10 bits
- Full text of *Hamlet* 1.5 million bits
- Pictures of Royal Holloway 5 million bits each
- Compact disc of Beethoven 9th 0.7 GB
- Large Hadron Collider, per second
- A quantum computer big enough to break public key cryptography

Why Coding Theory?

A bit gives a single piece of information: 'NO' or 'YES'; 'on' or 'off'; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000: 10 bits
- Full text of *Hamlet* 1.5 million bits
- Pictures of Royal Holloway 5 million bits each
- Compact disc of Beethoven 9th 0.7 GB
- Large Hadron Collider, per second 300 GB
- A quantum computer big enough to break public key cryptography

Why Coding Theory?

A bit gives a single piece of information: 'NO' or 'YES'; 'on' or 'off'; 0 or 1.

- A number between 0 and 15: 4 bits
- A number between 0 and 1000: 10 bits
- Full text of *Hamlet* 1.5 million bits
- Pictures of Royal Holloway 5 million bits each
- Compact disc of Beethoven 9th 0.7 GB
- Large Hadron Collider, per second 300 GB
- A quantum computer big enough to break public key cryptography 20 million qubits

Errors in reading and writing are inevitable. We can only hope to correct them when they occur.

A Simple Error Correcting Code

Number	Encoded as	Number	Encoded as
0	0000 0000 0000	8	1000 1000 1000
1	0001 0001 0001	9	1001 1001 1001
2	0010 0010 0010	10	1010 1010 1010
3	0011 0011 0011	11	1011 1011 1011
4	0100 0100 0100	12	1100 1100 1100
5	0101 0101 0101	13	1101 1101 1101
6	0110 0110 0110	14	1110 1110 1110
7	0111 0111 0111	15	1111 1111 1111

A Simple Error Correcting Code

Number	Encoded as	Number	Encoded as
0	0000 0000 0000	8	1000 1000 1000
1	0001 0001 0001	9	1001 1001 1001
2	0010 0010 0010	10	1010 1010 1010
3	0011 0011 0011	11	1011 1011 1011
4	0100 0100 0100	12	1100 1100 1100
5	0101 0101 0101	13	1101 1101 1101
6	0110 0110 0110	14	1110 1110 1110
7	0111 0111 0111	15	1111 1111 1111

Question. Suppose you receive 0011 0010 0011. What number was most likely sent?

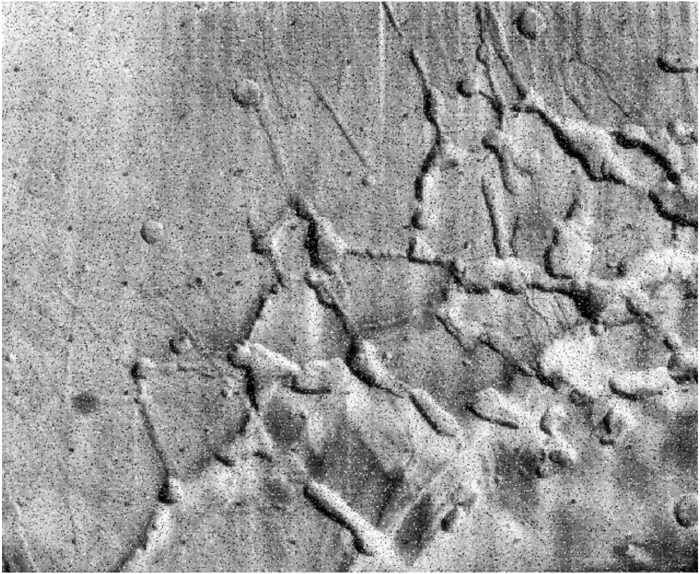
A Simple Error Correcting Code

Number	Encoded as	Number	Encoded as
0	0000 0000 0000	8	1000 1000 1000
1	0001 0001 0001	9	1001 1001 1001
2	0010 0010 0010	10	1010 1010 1010
3	0011 0011 0011	11	1011 1011 1011
4	0100 0100 0100	12	1100 1100 1100
5	0101 0101 0101	13	1101 1101 1101
6	0110 0110 0110	14	1110 1110 1110
7	0111 0111 0111	15	1111 1111 1111

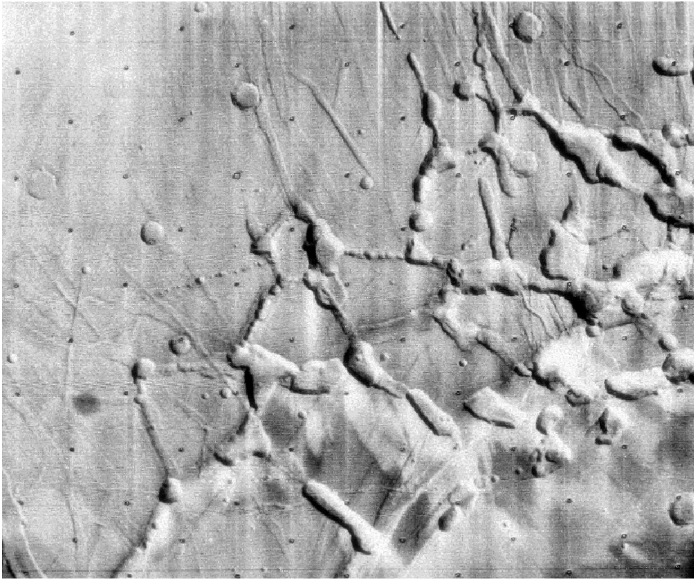
Question. Suppose you receive 0011 0010 0011. What number was most likely sent?

Answer. Since 0011 0010 0011 differs from 0011 0011 0011 in just once place, it's most likely that the number is 3.

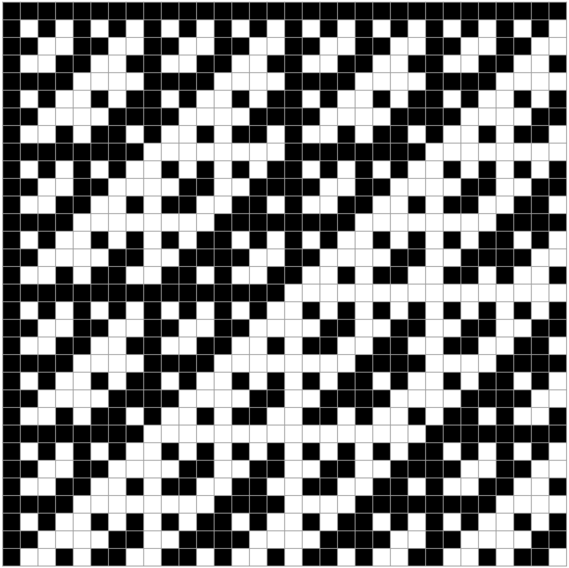
Mariner 9 Image: Improvement Due to Error Correction



Mariner 9 Image: Improvement Due to Error Correction



The Mariner 9 Code: 32 of the 64 Mariner 9 codewords: Black Squares Show 0, White Squares Show 1



The Liar Game: Dealing with Deliberate Errors

Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask, if your friend is permitted to lie at most once?

It is not compulsory to lie.

The Liar Game: Dealing with Deliberate Errors

Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask, if your friend is permitted to lie at most once?

It is not compulsory to lie.

Any interesting strategies?

The Liar Game: Dealing with Deliberate Errors

Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask, if your friend is permitted to lie at most once?

It is not compulsory to lie.

Any interesting strategies?

Question 1. Are you going to tell the truth in the next three questions?

The Liar Game: Dealing with Deliberate Errors

Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask, if your friend is permitted to lie at most once?

It is not compulsory to lie.

Any interesting strategies?

Question 1. Are you going to tell the truth in the next three questions?

- If **Yes**: You told the truth!

The Liar Game: Dealing with Deliberate Errors

Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask, if your friend is permitted to lie at most once?

It is not compulsory to lie.

Any interesting strategies?

Question 1. Are you going to tell the truth in the next three questions?

- If **Yes**: You told the truth!
- If **No**: Either you're lying now, or you'll lie in the next three questions.

The Liar Game: Dealing with Deliberate Errors

Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask, if your friend is permitted to lie at most once?

It is not compulsory to lie.

Any interesting strategies?

Question 1. Are you going to tell the truth in the next three questions?

- If **Yes**: You told the truth!
- If **No**: Either you're lying now, or you'll lie in the next three questions.

How about a proof that no strategy can guarantee to use six questions or fewer?

The Liar Game: Dealing with Deliberate Errors

Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask, if your friend is permitted to lie at most once?

It is not compulsory to lie.

Any interesting strategies?

Question 1. Are you going to tell the truth in the next three questions?

- If **Yes**: You told the truth!
- If **No**: Either you're lying now, or you'll lie in the next three questions.

How about a proof that no strategy can guarantee to use six questions or fewer?

Coding theory gives a seven question strategy. Lies correspond to errors in transmission.

The Hamming Code

Richard Hamming discovered a one-error correcting binary code of length 7 with 16 codewords. He invented it because he was fed up with the paper tape reader on his early computer misreading his programs.

It gives an optimal solution to the Liar Game using 7 questions.

Remarkably, it is possible to specify all the questions in advance.

The Hamming Code

Find the binary codeword corresponding to your secret number.

0	0000000	8	1110000
1	1101001	9	0011001
2	0101010	10	1011010
3	1000011	11	0110011
4	1001100	12	0111100
5	0100101	13	1010101
6	1100110	14	0010110
7	0001111	15	1111111

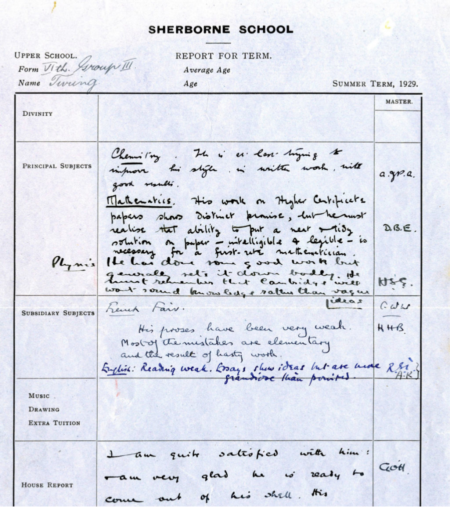
The questions are:

> 'Is there a 1 in the first position (far left) of the codeword?',
>
> 'Is there a 1 in the second position of the codeword?',

and so on. If there is one lie, then the questioner will write down one wrong bit. But because the Hamming code can correct one error, the questioner can still work out what the number is.

Turing

Alan Turing (1912 — 1952) was a polymathematic pioneer of early computing



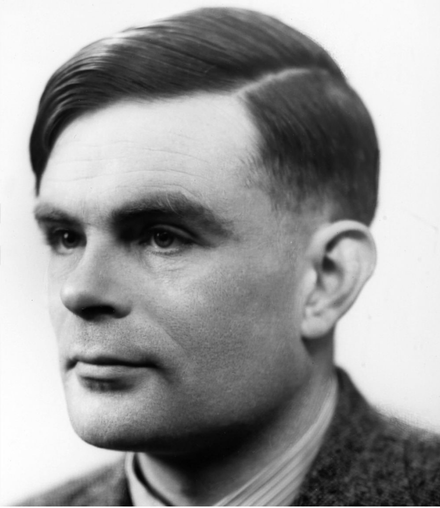
SHERBORNE SCHOOL

UPPER SCHOOL. REPORT FOR TERM.

Form VIth. Group III Average Age

Name Turing Age SUMMER TERM, 1929.

		MASTER.
DIVINITY		
PRINCIPAL SUBJECTS	Chemistry. He is at last trying to improve his style in written work, with good results. Mathematics. His work on Higher Certificate papers shows distinct promise, but he must realise that ability to put a neat & tidy solution on paper — intelligible & legible — is necessary for a first-rate mathematician. Physics: He has done some good work but generally sets it down badly. He must remember that Cambridge will want sound knowledge rather than vague ideas.	D.B.E.
SUBSIDIARY SUBJECTS	French Fair. His proses have been very weak. Most of the mistakes are elementary and the result of hasty work. English: Reading weak. Essays show ideas but are more grandiose than pointed.	H.H.B.
MUSIC DRAWING EXTRA TUITION		
HOUSE REPORT	I am quite satisfied with him: I am very glad he is ready to come out of his shell. His	



Turing's maths teacher had a fair point: mathematics papers are mostly words.

A PROOF OF LIOUVILLE'S THEOREM

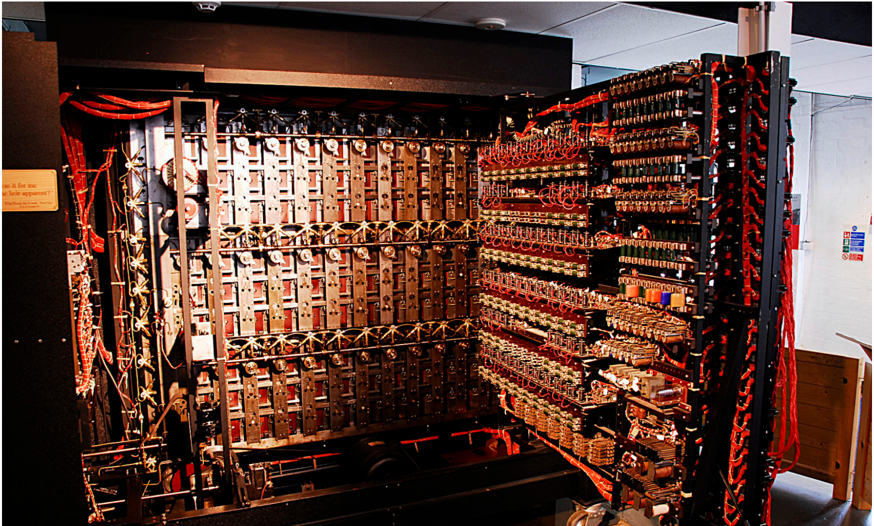
EDWARD NELSON

Consider a bounded harmonic function on Euclidean space. Since it is harmonic, its value at any point is its average over any sphere, and hence over any ball, with the point as center. Given two points, choose two balls with the given points as centers and of equal radius. If the radius is large enough, the two balls will coincide except for an arbitrarily small proportion of their volume. Since the function is bounded, the averages of it over the two balls are arbitrarily close, and so the function assumes the same value at any two points. Thus a bounded harmonic function on Euclidean space is a constant.

PRINCETON UNIVERSITY

Received by the editors June 26, 1961.

Turing and his Hut 8 team used a mixture of cryptanalysis, statistical inference and computation — the 'Bombe' — to crack the Enigma code used by the German Navy in the Second World War.



Turing's finest mathematical achievement is the following theorem.

Theorem. There is no algorithm that will decide the truth or falsity of a mathematical statement

- There are infinitely many primes — True
- There are infinitely many primes ending 1 — True
- There are infinitely many primes ending 2 — False
- $0.9999\ldots = 1$ — True
- 2^3 and 3^2 are the only consecutive integer powers — ???
- There are infinitely many twin primes such as 3, 5 or 5, 7 or 11, 13 or 17, 19 or ... or 2027, 2029 or ... — ???
- There is an efficient algorithm for factoring large numbers — ???

What Turing really proved is that there is no algorithm that decides whether an algorithm terminates: 'The Entscheidungsproblem is undecidable.'

Corollary 1 (Gödel's first incompleteness theorem)

Fix a formal proof system. There exists a true statement that has no formal proof.

For example, a formal proof from Russell–Whitehead *Principia M*

***54·43.** $\vdash :. \alpha, \beta \in 1 . \supset : \alpha \cap \beta = \Lambda . \equiv . \alpha \cup \beta \in 2$

Dem.

$\vdash . {*54{\cdot}26} . \supset \vdash :. \alpha = \iota‘x . \beta = \iota‘y . \supset : \alpha \cup \beta \in 2 . \equiv . x \neq y .$

$[{*51{\cdot}231}] \qquad \equiv . \iota‘x \cap \iota‘y = \Lambda .$

$[{*13{\cdot}12}] \qquad \equiv . \alpha \cap \beta = \Lambda \qquad (1)$

$\vdash . (1) . {*11{\cdot}11{\cdot}35} . \supset$

$\vdash :. (\exists x, y) . \alpha = \iota‘x . \beta = \iota‘y . \supset : \alpha \cup \beta \in 2 . \equiv . \alpha \cap \beta = \Lambda \qquad (2)$

$\vdash . (2) . {*11{\cdot}54} . {*52{\cdot}1} . \supset \vdash .$ Prop

From this proposition it will follow, when arithmetical addition has been defined, that $1 + 1 = 2$.

What Turing really proved is that there is no algorithm that decides whether an algorithm terminates: 'The Entscheidungsproblem is undecidable.'

Corollary 1 (Gödel's first incompleteness theorem)

Fix a formal proof system. There exists a true statement that has no formal proof.

Proof. Suppose, for a contradiction, that either P or $\neg P$ is provable for every statement P. Given a Turing machine M, let P_M be the statement 'M halts'.

- Spend week 1 looking for a formal proof of P_M,
- Spend week 2 looking for a formal proof of $\neg P_M$,
- Spend week 3 looking for a formal proof of P_M,

and so on. Since either P_M or $\neg P_M$ is provable, and formal proofs can be enumerated one-by-one, eventually we will succeed in finding a proof. Therefore we can detect when Turing machines halt. This contradicts Turing's result. Hence there are statements Q such that neither Q nor $\neg Q$ is provable. But either Q or $\neg Q$ is true. □


ALAN MATHISO
IEKYF RONSI

Thank you! Any questions?

A Hat Game Related to Coding Theory

You and two friends are on your way to a party.

At the party a black or white hat will be put on each person's head. You can see your friends' hats, but not your own.

A Hat Game Related to Coding Theory

You and two friends are on your way to a party.

At the party a black or white hat will be put on each person's head. You can see your friends' hats, but not your own.

When the host shouts 'Go!', you may either say a colour or remain silent. Everyone who speaks must speak at the same time.

If everyone who speaks gets the colour of his or her hat correct, you all win some cake. If no-one speaks, or someone gets it wrong, there is no cake.

A Hat Game Related to Coding Theory

You and two friends are on your way to a party.

At the party a black or white hat will be put on each person's head. You can see your friends' hats, but not your own.

When the host shouts 'Go!', you may either say a colour or remain silent. Everyone who speaks must speak at the same time.

If everyone who speaks gets the colour of his or her hat correct, you all win some cake. If no-one speaks, or someone gets it wrong, there is no cake.

Question: What is a good strategy?

Thank you! Any questions?

Thank you! Any questions?

- Why is maths a good subject to study?
- What do maths lecturers do all day?
- How does maths at university differ from A-level maths?
- Are women just as good as men at maths? (**Answer:** Yes!)

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.
- In the worst case, there are least **8** possible numbers after the first question.

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.
- In the worst case, there are least **8** possible numbers after the first question.
  - 'Is the number 8 or more?' $7\ (\mathrm{NO}) + 8\ (\mathrm{YES}) = 15$

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.
- In the worst case, there are least **8** possible numbers after the first question.
  - 'Is the number 8 or more?' $7\ (\mathrm{NO}) + 8\ (\mathrm{YES}) = 15$
  - 'Is the number even?' $8\ (\mathrm{NO}) + 7\ (\mathrm{YES}) = 15$

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.
- In the worst case, there are least **8** possible numbers after the first question.
  - 'Is the number 8 or more?' $7\ (\mathrm{NO}) + 8\ (\mathrm{YES}) = 15$
  - 'Is the number even?' $8\ (\mathrm{NO}) + 7\ (\mathrm{YES}) = 15$
  - 'Is the number 12? $14\ (\mathrm{NO}) + 1\ (\mathrm{YES}) = 15$

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.
- In the worst case, there are least **8** possible numbers after the first question.
  - 'Is the number 8 or more?' $7\ (\mathrm{NO}) + 8\ (\mathrm{YES}) = 15$
  - 'Is the number even?' $8\ (\mathrm{NO}) + 7\ (\mathrm{YES}) = 15$
  - 'Is the number 12? $14\ (\mathrm{NO}) + 1\ (\mathrm{YES}) = 15$
  - 'Is the number prime? $9\ (\mathrm{NO}) + 6\ (\mathrm{YES}) = 15$

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.
- In the worst case, there are least **8** possible numbers after the first question.
  - 'Is the number 8 or more?' $7\ (\mathrm{NO}) + 8\ (\mathrm{YES}) = 15$
  - 'Is the number even?' $8\ (\mathrm{NO}) + 7\ (\mathrm{YES}) = 15$
  - 'Is the number 12? $14\ (\mathrm{NO}) + 1\ (\mathrm{YES}) = 15$
  - 'Is the number prime? $9\ (\mathrm{NO}) + 6\ (\mathrm{YES}) = 15$
- In the worst case there are at least **4** possible numbers after the second question.

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.
- In the worst case, there are least **8** possible numbers after the first question.
  - 'Is the number 8 or more?' $7\ (\mathrm{NO}) + 8\ (\mathrm{YES}) = 15$
  - 'Is the number even?' $8\ (\mathrm{NO}) + 7\ (\mathrm{YES}) = 15$
  - 'Is the number 12? $14\ (\mathrm{NO}) + 1\ (\mathrm{YES}) = 15$
  - 'Is the number prime? $9\ (\mathrm{NO}) + 6\ (\mathrm{YES}) = 15$
- In the worst case there are at least **4** possible numbers after the second question.
- In the worst case there are at least **2** possible numbers after the third question.

Four Questions are Necessary

The aim is to find a number between 1 and 15.

- There are **15** possible numbers.
- In the worst case, there are least **8** possible numbers after the first question.
  - 'Is the number 8 or more?' $7\ (\mathrm{NO}) + 8\ (\mathrm{YES}) = 15$
  - 'Is the number even?' $8\ (\mathrm{NO}) + 7\ (\mathrm{YES}) = 15$
  - 'Is the number 12? $14\ (\mathrm{NO}) + 1\ (\mathrm{YES}) = 15$
  - 'Is the number prime? $9\ (\mathrm{NO}) + 6\ (\mathrm{YES}) = 15$
- In the worst case there are at least **4** possible numbers after the second question.
- In the worst case there are at least **2** possible numbers after the third question.
- So three questions are not enough.