The Liar Game
Truths and Proofs from Euclid to Turing
Mark Wildon
Which National Football League player has a prime number?

Not 10 because $10 = 2 \times 5$

Not 57 because $57 = 3 \times 19$

Not 25 because $25 = 5 \times 5$

31 is prime
Which National Football League player has a prime number?

- Not 10 because $10 = 2 \times 5$
- Not 57 because $57 = 3 \times 19$
- Not 25 because $25 = 5 \times 5$
- 31 is prime
Which National Football League player has a prime number?

- Not 10 because $10 = 2 \times 5$
- Not 57 because $57 = 3 \times 19$
- 31 is prime
Which National Football League player has a prime number?

- Not 10 because $10 = 2 \times 5$
- Not 57 because $57 = 3 \times 19$
- Not 25 because $25 = 5 \times 5$
- 31 is prime
Which National Football League player has a prime number?

- Not 10 because $10 = 2 \times 5$
- Not 57 because $57 = 3 \times 19$
- Not 25 because $25 = 5 \times 5$
- 31 is prime
1 is not a prime — says who?
1 is not a prime
1 is not a prime — says who?
2, 3, 5, 7, 11, 13, ..., 2003, 2011, 2017, 2027, 2029, ...
Does the sequence of primes ever stop?

Or maybe there are infinitely many primes?
2, 3, 5, 7, 11, 13, ..., 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

$2 \times 3 \times 5 = 30$

$30 + 1 = 31$
The first three primes are 2, 3, 5

\[ 2 \times 3 \times 5 = 30 \]
\[ 30 + 1 = 31 \]

31 has remainder 1 when we divide it by 2, 3, 5
The first three primes are 2, 3, 5

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

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

\[ 31 = 15 \times 2 + 1 \]
The first three primes are 2, 3, 5.

$2 \times 3 \times 5 = 30$

$30 + 1 = 31$

31 has 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
- \(2 \times 3 \times 5 = 30\)
- \(30 + 1 = 31\)
- 31 has 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

- $2 \times 3 \times 5 = 30$
- $30 + 1 = 31$
- 31 has 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

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

31 has 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

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

31 has 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
30 + 1 = 31
31 has remainder 1 when we divide it by 2, 3, 5
\begin{itemize}
  \item 31 = 15 \times 2 + 1
  \item 31 = 10 \times 3 + 1
  \item 31 = 6 \times 5 + 1
\end{itemize}
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
30030 + 1 = 30031
The first three primes are 2, 3, 5

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

31 has 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

\[ 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030 \]

\[ 30030 + 1 = 30031 \]

30031 has remainder 1 when we divide it by 2, 3, 5, 7, 11, 13
The first three primes are 2, 3, 5
- $2 \times 3 \times 5 = 30$
- $30 + 1 = 31$
- 31 has 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
- $2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$
- $30030 + 1 = 30031$
- 30031 has remainder 1 when we divide it by 2, 3, 5, 7, 11, 13
  - $30031 = 15015 \times 2 + 1$
The first three primes are 2, 3, 5

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

31 has 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

\[ 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030 \]

\[ 30030 + 1 = 30031 \]

30031 has remainder 1 when we divide it by 2, 3, 5, 7, 11, 13
- \[ 30031 = 15015 \times 2 + 1 \]
- \[ 30031 = 10010 \times 3 + 1 \]

\[ \ldots \]
The first three primes are $2, 3, 5$

$2 \times 3 \times 5 = 30$

$30 + 1 = 31$

31 has 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 $2, 3, 5, 7, 11, 13$

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

$30030 + 1 = 30031$

30031 has 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

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

31 has 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

\[ 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030 \]

\[ 30030 + 1 = 30031 \]

30031 has 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

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

31 has 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

\[ 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030 \]

\[ 30030 + 1 = 30031 \]

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

\[ 30031 = 15015 \times 2 + 1 \]
\[ 30031 = 10010 \times 3 + 1 \]

\[ \ldots \]
\[ 30031 = 2310 \times 13 + 1 \]

But 30031 is either prime or divisible by a prime
The first three primes are 2, 3, 5

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

31 has 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

\[ 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030 \]

\[ 30030 + 1 = 30031 \]

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

\[ 30031 = 15015 \times 2 + 1 \]
\[ 30031 = 10010 \times 3 + 1 \]

\[ \ldots \]
\[ 30031 = 2310 \times 13 + 1 \]

But 30031 is either prime or divisible by a prime (in fact \( 30031 = 59 \times 209 \))
The first three primes are 2, 3, 5

\[ 2 \times 3 \times 5 = 30 \]

\[ 30 + 1 = 31 \]

31 has 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

\[ 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030 \]

\[ 30030 + 1 = 30031 \]

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

\[ 30031 = 15015 \times 2 + 1 \]
\[ 30031 = 10010 \times 3 + 1 \]

\[ \ldots \]
\[ 30031 = 2310 \times 13 + 1 \]

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

So 2, 3, 5, 7, 11, 13 are not all the primes.
Socrates: I think $p_1, p_2, \ldots, p_r$ are all the primes.
- **Socrates:** I think $p_1, p_2, \ldots, p_r$ are all the primes
- **Euclid:** Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$
Socrates: I think $p_1, p_2, \ldots, p_r$ are all the primes

Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$

Socrates: If I must ...
Socrates: I think \( p_1, p_2, \ldots, p_r \) are all the primes

Euclid: Consider \( N = p_1 \times p_2 \times \cdots \times p_r + 1 \)

Socrates: If I must ...

Euclid: \( N \) has remainder 1 when divided by all your primes
Socrates: I think $p_1, p_2, \ldots, p_r$ are all the primes

Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$

Socrates: If I must …

Euclid: $N$ has remainder 1 when divided by all your primes

Socrates: You are correct
Socrates: I think \( p_1, p_2, \ldots, p_r \) are all the primes

Euclid: Consider \( N = p_1 \times p_2 \times \cdots \times p_r + 1 \)

Socrates: If I must ...

Euclid: \( N \) has remainder 1 when divided by all your primes

Socrates: You are correct

Euclid: But \( N \) is divisible by some prime
> Socrates: I think $p_1, p_2, \ldots, p_r$ are all the primes

> Euclid: Consider $N = p_1 \times p_2 \times \cdots \times p_r + 1$

> Socrates: If I must …

> Euclid: $N$ has 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.
Ask a friend to think of a number between 1 and 15. How many YES/NO questions do you need to ask to find the secret number?
Ask a friend to think of a number between 1 and 15. How many YES/NO questions do you need to ask to find the secret number?
In a computer everything is stored as lists of \textbf{bits (binary digits)} 0 and 1.
In a computer everything is stored as lists of **bits** (**binary digits**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers ‘Yes’, ‘Yes’, ‘No’, ‘No’.

Part of the machine code for Microsoft Word 2011.

---

Q1
Is the number 8, 9, 10, 11, 12, 13, 14 or 15?

YES 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Q1
Is the number 8, 9, 10, 11, 12, 13, 14 or 15?

YES
In a computer everything is stored as lists of **bits (binary digits)** 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers `Yes', `Yes', `No', `No'.

---

**Q1**

Is the number 8, 9, 10, 11, 12, 13, 14 or 15? **YES**

---

**Q2**

Is the number 12, 13, 14 or 15? **YES**
In a computer everything is stored as lists of **bits** (**binary digits**) 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers `Yes`, `Yes`, `No`, `No`.

```
Q1
Is the number
8, 9, 10, 11, 12, 13, 14 or 15?

YES

Q2
Is the number
12, 13, 14 or 15?

YES

Q3
Is the number
14 or 15?

NO
```
In a computer everything is stored as lists of **bits (binary digits)** 0 and 1. The number 12 is stored as 1100, corresponding to the sequence of answers ‘Yes’, ‘Yes’, ‘No’, ‘No’.

![Decision tree diagram](image-url)
In a computer everything is stored as lists of **bits** (binary digits) 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 11010110 00100000 10101000 00101011 01100010 00100000 11010100 00100000 1101010
1101011 00101110 00100000 00101110 1101011 00100000 10101000 00101011 11100100 00100000 00101011
01101000 00100010 01101100 01100000 01101100 10101001 01101000 00100000 00101011 11000000 1101000
00101111 01010010 00101011 00100000 10101000 00101011 00100000 00101011 00100000 00101011 00100000
00101000 00101011 00101011 00101011 01101000 00101110 10101000 00101011 00100000 10100011 00101110
00100000 1101010 1101010 10101000 01101000 00101011 00100000 00101011 10101000 00101011 00100000
00101111 01010000 00101011 00100000 01101100 01101001 01101000 00100000 00101011 1101010
00100000 10100001 00101011 00100000 01101000 01101001 11010100 00100000 01100010 00101011 1101010
00100000 10101011 01100001 01101000 11010010 01101000 00101011 10101000 00101011 11010010 01101000
01100000 00101011 01010001 01101000 00101011 00100000 00101011 00100000 00101011 00100000 00101011
01101000 00101011 01010100 00101000 00100000 00101111 00101110 00101011 10101110 00101011 00101011
00101011 01101100 00101011 00100000 00101011 00100000 00101011 00100000 00101011 00101011 01101010
```

William Shakespeare (approx 1600)
In a computer everything is stored as lists of **bits** (binary digits) 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 1101011 00100000 10101000 0010101 01100010 00100000 11101011 10101100 00100000 1101010
1101011 00101110 00100000 00101110 1101011 00100000 10101000 00101110 1101011 00100000 1101011 01101100
01101000 00101001 00101110 00100000 01101001 10101101 00100000 11010101 00100000 01101001 10101100 00101110
01101110 00101111 00100000 01101110 00100000 00101110 11010100 10101000 00101110 11010100 01101011 01101100
01100000 11101011 1101011 10101000 01101001 10101100 00100000 11101011 1101011 11101010 01010000 01101001 01101000
00101011 10101101 00100000 00101110 11101010 10101000 00101110 11101011 01101000 00101001 01101000 00101011
01000000 10101101 01101101 10101100 11000000 11101011 10101000 01101001 01101100 11000000 11101011 10101000 10101111
01010110 1101011 10101100 00101110 00101111 11101010 00101001 01101000 01000000 01101001 01101000 00101011
01010100 11101011 10101100 01000000 01101011 00101101 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,*
In a computer everything is stored as lists of **bits** (*binary digits*) 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.

```
01010100 01101110 00100000 01100101 01101100 00101101 00001001 00000000 00100000 01100100 01100010 01101111 01110010 01100101 01101110 01000000
00100000 01100010 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000
00100000 01100010 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000
00100000 01100010 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000
00100000 01100010 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000
00100000 01100010 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000 01100100 01101111 01110010 01100101 01101110 01000000
```

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,*
In a computer everything is stored as lists of **bits (binary digits)** 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.

---

Anonymous Microsoft Programmer (2010)
In a computer everything is stored as lists of **bits** *(binary digits)* 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.

Anonymous Microsoft Programmer (2010)

Part of the machine code for Microsoft Word 2011.
In a computer everything is stored as lists of **bits (binary digits)** 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.
Alice wants to send a message to Bob. She can communicate with him by sending him a sequence of the bits 0 and 1.

Every time 0 is sent, there is a chance that 1 is received, and every time 1 is sent, there is a chance that 0 is received.

How can Alice and Bob communicate reliably?
Alice wants to send a message to Bob. She can communicate with him by sending him a sequence of the bits 0 and 1.

Every time 0 is sent, there is a chance that 1 is received, and every time 1 is sent, there is a chance that 0 is received.

How can Alice and Bob communicate reliably?

- Alice (aside): my number is 12
Alice wants to send a message to Bob. She can communicate with him by sending him a sequence of the bits 0 and 1.

Every time 0 is sent, there is a chance that 1 is received, and every time 1 is sent, there is a chance that 0 is received.

How can Alice and Bob communicate reliably?

- Alice (aside): my number is 12
- Alice (to Bob): 1100
Alice wants to send a message to Bob. She can communicate with him by sending him a sequence of the bits 0 and 1.

Every time 0 is sent, there is a chance that 1 is received, and every time 1 is sent, there is a chance that 0 is received.

**How can Alice and Bob communicate reliably?**

- Alice (aside): my number is 12
- Alice (to Bob): 1100
- Bob: I hear 1000, which is 8
Alice wants to send a message to Bob. She can communicate with him by sending him a sequence of the bits 0 and 1.

Every time 0 is sent, there is a chance that 1 is received, and every time 1 is sent, there is a chance that 0 is received.

How can Alice and Bob communicate reliably?

- Alice (aside): my number is 12
- Alice (to Bob): 1100
- Bob: I hear 1000, which is 8
- Alice: No that's wrong
Alice wants to send a message to Bob. She can communicate with him by sending him a sequence of the bits 0 and 1.

Every time 0 is sent, there is a chance that 1 is received, and every time 1 is sent, there is a chance that 0 is received.

How can Alice and Bob communicate reliably?

- Alice (aside): my number is 12
- Alice (to Bob): 1100
- Bob: I hear 1000, which is 8
- Alice: No that's wrong
- Bob: What did you say?
Alice wants to send a message to Bob. She can communicate with him by sending him a sequence of the bits 0 and 1.

Every time 0 is sent, there is a chance that 1 is received, and every time 1 is sent, there is a chance that 0 is received.

How can Alice and Bob communicate reliably?

- Alice (aside): my number is 12
- Alice (to Bob): 1100
- Bob: I hear 1000, which is 8
- Alice: No that's wrong
- Bob: What did you say?
- Alice: 111 101 000 001
Alice wants to send a message to Bob. She can communicate with him by sending him a sequence of the bits 0 and 1.

Every time 0 is sent, there is a chance that 1 is received, and every time 1 is sent, there is a chance that 0 is received.

How can Alice and Bob communicate reliably?

- Alice (aside): my number is 12
- Alice (to Bob): 1100
- Bob: I hear 1000, which is 8
- Alice: No that's wrong
- Bob: What did you say?
- Alice: 111 101 000 001
- Bob: It sounds most like 1100, which is 12
Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask to find the secret number? Your friend may lie but only once.

It is not compulsory to lie.
Ask a friend to think of a number between 0 and 15. How many YES/NO questions do you need to ask to find the secret number? Your friend may lie but only once.

It is not compulsory to lie.

The Alice/Bob code gives a 12 question solution

<table>
<thead>
<tr>
<th>Number</th>
<th>Encoded as</th>
<th>Number</th>
<th>Encoded as</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000 0000 0000</td>
<td>8</td>
<td>1000 1000 1000</td>
</tr>
<tr>
<td>1</td>
<td>0001 0001 0001</td>
<td>9</td>
<td>1001 1001 1001</td>
</tr>
<tr>
<td>2</td>
<td>0010 0010 0010</td>
<td>10</td>
<td>1010 1010 1010</td>
</tr>
<tr>
<td>3</td>
<td>0011 0011 0011</td>
<td>11</td>
<td>1011 1011 1011</td>
</tr>
<tr>
<td>4</td>
<td>0100 0100 0100</td>
<td>12</td>
<td>1100 1100 1100</td>
</tr>
<tr>
<td>5</td>
<td>0101 0101 0101</td>
<td>13</td>
<td>1101 1101 1101</td>
</tr>
<tr>
<td>6</td>
<td>0110 0110 0110</td>
<td>14</td>
<td>1110 1110 1110</td>
</tr>
<tr>
<td>7</td>
<td>0111 0111 0111</td>
<td>15</td>
<td>1111 1111 1111</td>
</tr>
</tbody>
</table>
Richard Hamming (1915 — 1998) 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.
Find the binary codeword corresponding to your secret number.

For instance if your number is 12 then the codeword is 0111100.

<table>
<thead>
<tr>
<th></th>
<th>0000000</th>
<th>1101001</th>
<th>0101010</th>
<th>1000011</th>
<th>1001100</th>
<th>0100101</th>
<th>1100110</th>
<th>0001111</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000000</td>
<td>1101001</td>
<td>0101010</td>
<td>1000011</td>
<td>1001100</td>
<td>0100101</td>
<td>1100110</td>
<td>0001111</td>
</tr>
<tr>
<td>1</td>
<td>1101001</td>
<td>0011001</td>
<td>1011010</td>
<td>0110011</td>
<td>0111100</td>
<td>1010101</td>
<td>0010110</td>
<td>1111111</td>
</tr>
<tr>
<td>2</td>
<td>0101010</td>
<td>1011010</td>
<td>0110011</td>
<td>0111100</td>
<td>1010101</td>
<td>0010110</td>
<td>1111111</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1000011</td>
<td>1011010</td>
<td>0110011</td>
<td>0111100</td>
<td>1010101</td>
<td>0010110</td>
<td>1111111</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>1001100</td>
<td>1111100</td>
<td>1010101</td>
<td>0010110</td>
<td>1111111</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0100101</td>
<td>1010101</td>
<td>0010110</td>
<td>1111111</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>1100110</td>
<td>0010110</td>
<td>1111111</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0001111</td>
<td>1111111</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

I'll ask you:

`What is the bit in the first position (far left) of the codeword?`,
`What is the bit in the second position of the codeword?`,
and so on. The Hamming code will reveal the number, even if you lie once.
Find the binary codeword corresponding to your secret number.

For instance if your number is 12 then the codeword is 0111100.

<table>
<thead>
<tr>
<th></th>
<th>00000000</th>
<th>8</th>
<th>1110000</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1101001</td>
<td>9</td>
<td>0011001</td>
</tr>
<tr>
<td>2</td>
<td>0101010</td>
<td>10</td>
<td>1011010</td>
</tr>
<tr>
<td>3</td>
<td>1000011</td>
<td>11</td>
<td>0110011</td>
</tr>
<tr>
<td>4</td>
<td>1001100</td>
<td>12</td>
<td>0111100</td>
</tr>
<tr>
<td>5</td>
<td>0100101</td>
<td>13</td>
<td>1010101</td>
</tr>
<tr>
<td>6</td>
<td>1100110</td>
<td>14</td>
<td>0010110</td>
</tr>
<tr>
<td>7</td>
<td>0001111</td>
<td>15</td>
<td>1111111</td>
</tr>
</tbody>
</table>

I'll ask you:

'What is the bit in the first position (far left) of the codeword?'

'What is the bit in the second position of the codeword?'

and so on. The Hamming code will reveal the number, even if you lie once.

No strategy can guarantee to use fewer than 7 questions. So the Hamming code is optimal.
Ada Lovelace (1815 — 1857)
Alan Turing (1912 — 1952) was another pioneer of early computing

### Sherborne School

**Upper School**

**Form V.G. Group III**

**Name Turing**

**Average Age**

**Summer Term, 1929.**

<table>
<thead>
<tr>
<th>Divinity</th>
<th>Master</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Principal Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physics</strong></td>
</tr>
<tr>
<td>He is keen trying to retain the style of written work with good results.</td>
</tr>
<tr>
<td>Mathematics. His work on Higher Certificate papers shows distinct promise. But he must realize that ability to put a neat and tidy notation on paper - intelligible &amp; legible - is necessary for a first-rate mathematician. He has done some good work but generally not at a high standard. He has inherited the Cambridge undergraduate style rather than regular.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subsidary Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>French</td>
</tr>
<tr>
<td>His powers have been very weak. Most of the mistakes are elementary and the result of hasty work.</td>
</tr>
<tr>
<td>English Literature</td>
</tr>
<tr>
<td>Reading weak. Essay few ideas but are more developed than previous.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Music</th>
<th>Drawing</th>
<th>Extra Tuition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>House Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am quite satisfied with him; I am very glad he is ready to come out of his shell.</td>
</tr>
<tr>
<td>Coach</td>
</tr>
</tbody>
</table>

---

**Report for Term.**

**Average Age**

**Summer Term, 1929.**

<table>
<thead>
<tr>
<th>Divinity</th>
<th>Master</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Principal Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Physics</strong></td>
</tr>
<tr>
<td>He is keen trying to retain the style of written work with good results.</td>
</tr>
<tr>
<td>Mathematics. His work on Higher Certificate papers shows distinct promise. But he must realize that ability to put a neat and tidy notation on paper - intelligible &amp; legible - is necessary for a first-rate mathematician. He has done some good work but generally not at a high standard. He has inherited the Cambridge undergraduate style rather than regular.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subsidary Subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>French</td>
</tr>
<tr>
<td>His powers have been very weak. Most of the mistakes are elementary and the result of hasty work.</td>
</tr>
<tr>
<td>English Literature</td>
</tr>
<tr>
<td>Reading weak. Essay few ideas but are more developed than previous.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Music</th>
<th>Drawing</th>
<th>Extra Tuition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>House Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am quite satisfied with him; I am very glad he is ready to come out of his shell.</td>
</tr>
<tr>
<td>Coach</td>
</tr>
</tbody>
</table>
He helped crack the Enigma code used by the German navy in the Second World War.
His 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
- It takes 4 bits to store a number between 0 and 15  
  True
- There are infinitely many primes ending 1  
  True
- There is a way to win the Liar Game in 6 questions  
  False
His 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  
- It takes 4 bits to store a number between 0 and 15  
- There are infinitely many primes ending 1  
- There is a way to win the Liar Game in 6 questions  
- There are infinitely many twin primes 3, 5, or 5, 7, or 11, 13 or 17, 19 or … or 2027, 2029 or …  
- There is a fast way to factorize large numbers into primes
His 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
- It takes 4 bits to store a number between 0 and 15 — True
- There are infinitely many primes ending 1 — True
- There is a way to win the Liar Game in 6 questions — False
- There are infinitely many twin primes 3, 5, or 5, 7, or 11, 13 or 17, 19 or ... or 2027, 2029 or ... — ???
- There is a fast way to factorize large numbers into primes — ???