Computers, Codes, and Pails of Water

Dept. of Mathematical Sciences
Northern Illinois University

http://math.niu.edu/∼richard/Math230

Goal

Goal: to familiarize you with the mathematical ideas behind some of the technology used in our society.

Goal

Goal: to familiarize you with the mathematical ideas behind some of the technology used in our society.

- Computer architecture uses binary numbers in fixed sizes, called bytes.

Goal

Goal: to familiarize you with the mathematical ideas behind some of the technology used in our society.

- Computer architecture uses binary numbers in fixed sizes, called bytes.
- Megabyte of memory is (approx) one million bytes.

Goal

Goal: to familiarize you with the mathematical ideas behind some of the technology used in our society.

- Computer architecture uses binary numbers in fixed sizes, called bytes.
- Megabyte of memory is (approx) one million bytes.
- Gigabyte of memory is (approx) one billion bytes.

Encoding Information

We are particularly interested in the mathematical concepts used to encode information.

Encoding Information

We are particularly interested in the mathematical concepts used to encode information.

Two purposes for encoding information:

Encoding Information

We are particularly interested in the mathematical concepts used to encode information.

Two purposes for encoding information:
Purpose 1. Error-correcting codes

Encoding Information

We are particularly interested in the mathematical concepts used to encode information.

Two purposes for encoding information:
Purpose 1. Error-correcting codes
Purpose 2. Encryption

Error-correcting codes

In error-correcting codes, we encode information so that if an error occurs in reading the information, we can still recover the original data.

Error-correcting codes

In error-correcting codes, we encode information so that if an error occurs in reading the information, we can still recover the original data.
Compact disk technology utilizes this type of coding, where small scratches on a CD need not damage the sound reproduction.

Secret codes

A second purpose of coding information is to make it secure, so that unauthorized persons cannot read private messages.

Secret codes

A second purpose of coding information is to make it secure, so that unauthorized persons cannot read private messages.
Secret codes have obvious military, industrial, and personal applications.

Secret codes

A second purpose of coding information is to make it secure, so that unauthorized persons cannot read private messages.
Secret codes have obvious military, industrial, and personal applications.
Our simple encryption-decryption method relies on some basic facts about “clock-arithmetic” and on a method for solving what we call “the pails-of-water” problem.

Section 1. Binary Numbers

- Computers store numbers in binary form.

Section 1. Binary Numbers

- Computers store numbers in binary form.
- This means that they are stored in base 2.

Section 1. Binary Numbers

- Computers store numbers in binary form.
- This means that they are stored in base 2.
- In our familiar base 10 number system, decimal numbers are represented using the powers of 10.

Section 1. Binary Numbers

- Computers store numbers in binary form.
- This means that they are stored in base 2.
- In our familiar base 10 number system, decimal numbers are represented using the powers of 10.
- For example,

$$2047 = 2 \cdot 10^3 + 0 \cdot 10^2 + 4 \cdot 10^1 + 7.$$

Binary Representation

- In base 2 the powers of 2 are used instead of the powers of 10.

Binary Representation

- In base 2 the powers of 2 are used instead of the powers of 10.
- Also, the only digits allowed are 0 and 1.

Binary Representation

- In base 2 the powers of 2 are used instead of the powers of 10.
- Also, the only digits allowed are 0 and 1.
- This restriction is convenient for the computer, which we can think of as using switches to store these binary digits, 1 = on, 0 = off.

The Powers of Two

n	2^n
1	
2	
3	
4	
5	

n	2^n
6	
7	
8	
9	
10	

The Powers of Two

n	2^n
1	2
2	
3	
4	
5	

n	2^n
6	
7	
8	
9	
10	

The Powers of Two

n	2^n
1	2
2	4
3	
4	
5	

n	2^n
6	
7	
8	
9	
10	

The Powers of Two

n	2^n
1	2
2	4
3	8
4	
5	

n	2^n
6	
7	
8	
9	
10	

The Powers of Two

n	2^n
1	2
2	4
3	8
4	16
5	

n	2^n
6	
7	
8	
9	
10	

The Powers of Two

n	2^n
1	2
2	4
3	8
4	16
5	32

n	2^n
6	
7	
8	
9	
10	

The Powers of Two

n	2^n
1	2
2	4
3	8
4	16
5	32

n	2^n
6	64
7	
8	
9	
10	

The Powers of Two

n	2^n
1	2
2	4
3	8
4	16
5	32

n	2^n
6	64
7	128
8	
9	
10	

The Powers of Two

n	2^n
1	2
2	4
3	8
4	16
5	32

n	2^n
6	64
7	128
8	256
9	
10	

The Powers of Two

n	2^n
1	2
2	4
3	8
4	16
5	32

n	2^n
6	64
7	128
8	256
9	512
10	

The Powers of Two

n	2^n
1	2
2	4
3	8
4	16
5	32

n	2^n
6	64
7	128
8	256
9	512
10	1024

Binary Example

The binary number

Binary Example

The binary number
$(110101)_2 =$

Binary Example

The binary number

$$(110101)_2 = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1$$

Binary Example

The binary number

$$(110101)_2 = 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1$$
$$= 2^5 + 2^4 + 2^2 + 1$$

Binary Example

The binary number

$$
\begin{aligned}
(110101)_2 &= 1 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \\
&= 2^5 + 2^4 + 2^2 + 1 \\
&= 32 + 16 + 4 + 1 = 53.
\end{aligned}
$$

Binary Number Chart

Binary representation of the numbers 1 through 32:

Binary Number Chart

Binary representation of the numbers 1 through 32:

1	1	9	1001	17	10001	25	11001
2	10	10	1010	18	10010	26	11010
3	11	11	1011	19	10011	27	11011
4	100	12	1100	20	10100	28	11100
5	101	13	1101	21	10101	29	11101
6	110	14	1110	22	10110	30	11110
7	111	15	1111	23	10111	31	11111
8	1000	16	10000	24	11000	32	100000

Two Kinds of People

There are

10

kinds of people in the world–

Two Kinds of People

There are
10
kinds of people in the world–

those that can read binary
and those that can't.

Computer Lingo

- each binary digit is called a bit,

Computer Lingo

- each binary digit is called a bit,
- 8 consecutive bits are called a byte.

Computer Lingo

- each binary digit is called a bit,
- 8 consecutive bits are called a byte.
- Since computers are binary, not decimal machines,

Computer Lingo

- each binary digit is called a bit,
- 8 consecutive bits are called a byte.
- Since computers are binary, not decimal machines,
- the numbers one thousand and one million are not naturally represented.

Computer Lingo

- each binary digit is called a bit,
- 8 consecutive bits are called a byte.
- Since computers are binary, not decimal machines,
- the numbers one thousand and one million are not naturally represented.
- However, $2^{10} = 1024$ is close to a thousand and

Computer Lingo

- each binary digit is called a bit,
- 8 consecutive bits are called a byte.
- Since computers are binary, not decimal machines,
- the numbers one thousand and one million are not naturally represented.
- However, $2^{10} = 1024$ is close to a thousand and
- $2^{20} = 1,045,576$ is close to a million.

Kilo, Mega, and Giga Bytes

- One kilobyte (K) of memory is actually 1024 bytes,

Kilo, Mega, and Giga Bytes

- One kilobyte (K) of memory is actually 1024 bytes,
- although most people think of this as roughly a thousand bytes.

Kilo, Mega, and Giga Bytes

- One kilobyte (K) of memory is actually 1024 bytes,
- although most people think of this as roughly a thousand bytes.
- One megabyte (M) of memory consists of 2^{20} total bytes.

Kilo, Mega, and Giga Bytes

- One kilobyte (K) of memory is actually 1024 bytes,
- although most people think of this as roughly a thousand bytes.
- One megabyte (M) of memory consists of 2^{20} total bytes.
- A gigabyte (G) is 2^{30} bytes, roughly one billion.

Storing characters

- A byte is designed to hold one character of information.

Storing characters

- A byte is designed to hold one character of information.
- Standard keyboard characters such as letters (lower and upper case), digits, and punctuation symbols are coded by a standard convention called the ASCII code.

Storing characters

- A byte is designed to hold one character of information.
- Standard keyboard characters such as letters (lower and upper case), digits, and punctuation symbols are coded by a standard convention called the ASCII code.
- ASCII stands for American Standard for Coded Information Interchange.

Storing characters

- A byte is designed to hold one character of information.
- Standard keyboard characters such as letters (lower and upper case), digits, and punctuation symbols are coded by a standard convention called the ASCII code.
- ASCII stands for American Standard for Coded Information Interchange.
- In the ASCII code, the letter A is assigned the value 65, B is stored as 66, etc.

Storing characters

- A byte is designed to hold one character of information.
- Standard keyboard characters such as letters (lower and upper case), digits, and punctuation symbols are coded by a standard convention called the ASCII code.
- ASCII stands for American Standard for Coded Information Interchange.
- In the ASCII code, the letter A is assigned the value 65, B is stored as 66, etc.
- There are $2^8 = 256$ possible characters that can be stored in a byte, well beyond the number of characters on a typewriter keyboard.

Parity Check Bit

Many computers contain a 9th bit, which you never see, called the parity check bit, for every byte in memory.

Parity Check Bit

Many computers contain a 9th bit, which you never see, called the parity check bit, for every byte in memory.

Suppose *b* is a byte of memory.

Parity Check Bit

Many computers contain a 9th bit, which you never see, called the parity check bit, for every byte in memory.
Suppose b is a byte of memory.
This means that b consists of 8 consecutive bits.

Parity Check Bit

Many computers contain a 9th bit, which you never see, called the parity check bit, for every byte in memory.
Suppose b is a byte of memory.
This means that b consists of 8 consecutive bits.
The parity check bit is

Parity Check Bit

Many computers contain a 9th bit, which you never see, called the parity check bit, for every byte in memory.
Suppose b is a byte of memory.
This means that b consists of 8 consecutive bits.
The parity check bit is

- 0 if the number of 1's in b is even;

Parity Check Bit Examples

What is the parity check bit for $b = 10010110$?

Parity Check Bit Examples

What is the parity check bit for $b = 10010110$?
Answer: 0

Parity Check Bit Examples

What is the parity check bit for $b = 10010110$?
Answer: 0 Why?

Parity Check Bit Examples

What is the parity check bit for $b = 10010110$?
Answer: 0 since b consists of four 1's and 4 is even.

Parity Check Bit Examples

What is the parity check bit for $b = 10010110$?
Answer: 0 since b consists of four 1's and 4 is even.
What is the parity check bit for $b = 10010111$?

Parity Check Bit Examples

What is the parity check bit for $b = 10010110$?
Answer: 0 since b consists of four 1's and 4 is even.
What is the parity check bit for $b = 10010111$?
Answer: 1

Parity Check Bit Examples

What is the parity check bit for $b = 10010110$?
Answer: 0 since b consists of four 1's and 4 is even.
What is the parity check bit for $b = 10010111$?
Answer: 1 Why?

Parity Check Bit Examples

What is the parity check bit for $b = 10010110$?
Answer: 0 since b consists of four 1's and 4 is even.
What is the parity check bit for $b = 10010111$?
Answer: 1 since b consists of five 1's and 5 is odd.

Parity Check Bit and Hardware Crash

- The number of 1's in each byte plus the parity check bit is always even.

Parity Check Bit and Hardware Crash

- The number of 1's in each byte plus the parity check bit is always even.
- If the hardware of a computer detects an odd number of 1's in a byte plus its parity check bit,

Parity Check Bit and Hardware Crash

- The number of 1's in each byte plus the parity check bit is always even.
- If the hardware of a computer detects an odd number of 1's in a byte plus its parity check bit,
- the computer will crash immediately and report a hardware malfunction.

Exercises

1. Write the following numbers in binary: 21, 57, 99

Exercises

1. Write the following numbers in binary: 21, 57, 99
2. How can you tell if a binary number is even or odd?

Exercises

1. Write the following numbers in binary: 21, 57, 99
2. How can you tell if a binary number is even or odd?
3. Write the following binary numbers in decimal: 101010, 1001001, 11111111.

Exercises

1. Write the following numbers in binary: 21, 57, 99
2. How can you tell if a binary number is even or odd?
3. Write the following binary numbers in decimal: 101010, 1001001, 11111111.
4. Add the following binary numbers:

$$1101101 + 1010101$$

$$10111011 + 10001000$$

$$11111111 + 1$$

Exercises

1. Write the following numbers in binary: 21, 57, 99
2. How can you tell if a binary number is even or odd?
3. Write the following binary numbers in decimal: 101010, 1001001, 11111111.
4. Add the following binary numbers:

$$1101101 + 1010101$$

$$10111011 + 10001000$$

$$11111111 + 1$$

5. What is the parity check bit for the binary numbers in Exercise 3?

Error Correcting Codes

Suppose we wish to encode a half byte (4 bits) so that if an error occurs in transmitting this data we could detect the error.

Error Correcting Codes

Suppose we wish to encode a half byte (4 bits) so that if an error occurs in transmitting this data we could detect the error.
One simple minded way would be to just repeat the 4 bits.

Error Correcting Codes

Suppose we wish to encode a half byte (4 bits) so that if an error occurs in transmitting this data we could detect the error.
One simple minded way would be to just repeat the 4 bits.
For example, we could encode $m = 1011$ as

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix},$$

where the two rows are identical.

Finding the Error

If the message $M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$, is sent over a communications channel and the message

Finding the Error

If the message $M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$, is sent over a communications channel and the message

$$M' = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

is received, we know that en error occurred in the third bit.

Finding the Error

If the message $M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$, is sent over a communications channel and the message

$$M' = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

is received, we know that en error occurred in the third bit.
But we don't know whether the third bit was originally a 0 and the second line is wrong, or whether the third bit was originally a 1 and the first line is wrong.

Finding the Error

If the message $M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$, is sent over a communications channel and the message

$$M' = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

is received, we know that en error occurred in the third bit.
But we don't know whether the third bit was originally a 0 and the second line is wrong, or whether the third bit was originally a 1 and the first line is wrong.
You can find the error–

Finding the Error

If the message $M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$, is sent over a communications channel and the message

$$M' = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

is received, we know that en error occurred in the third bit.
But we don't know whether the third bit was originally a 0 and the second line is wrong, or whether the third bit was originally a 1 and the first line is wrong.
You can find the error– you just can't fix it.

An Error Correcting Code

Goal: Use the parity check bit

An Error Correcting Code

Goal: Use the parity check bit

- to detect errors and also

An Error Correcting Code

Goal: Use the parity check bit

- to detect errors and also
- to correct them.

An Error Correcting Code

Goal: Use the parity check bit

- to detect errors and also
- to correct them.

Our Code is called the Tic–Tac–Toe Code

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

$$M = \left[\begin{array}{cc|c} b_1 & b_2 & d_1 \\ b_3 & b_4 & d_2 \\ \hline c_1 & c_2 & c_3 \end{array}\right].$$

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

$$M = \left[\begin{array}{cc|c} b_1 & b_2 & d_1 \\ b_3 & b_4 & d_2 \\ \hline c_1 & c_2 & c_3 \end{array}\right].$$

- d_1 is the parity check bit for row 1

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

$$M = \left[\begin{array}{cc|c} b_1 & b_2 & d_1 \\ b_3 & b_4 & d_2 \\ \hline c_1 & c_2 & c_3 \end{array}\right].$$

- d_1 is the parity check bit for row 1
- d_2 is the parity check bit for row 2

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

$$M = \left[\begin{array}{cc|c} b_1 & b_2 & d_1 \\ b_3 & b_4 & d_2 \\ \hline c_1 & c_2 & c_3 \end{array}\right].$$

- d_1 is the parity check bit for row 1
- d_2 is the parity check bit for row 2
- c_1 is the parity check bit for column 1

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

$$M = \left[\begin{array}{cc|c} b_1 & b_2 & d_1 \\ b_3 & b_4 & d_2 \\ \hline c_1 & c_2 & c_3 \end{array}\right].$$

- d_1 is the parity check bit for row 1
- d_2 is the parity check bit for row 2
- c_1 is the parity check bit for column 1
- c_2 is the parity check bit for column 2

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

$$M = \left[\begin{array}{cc|c} b_1 & b_2 & d_1 \\ b_3 & b_4 & d_2 \\ \hline c_1 & c_2 & c_3 \end{array}\right].$$

- d_1 is the parity check bit for row 1
- d_2 is the parity check bit for row 2
- c_1 is the parity check bit for column 1
- c_2 is the parity check bit for column 2
- c_3 in the lower right hand corner (row 3, col 3) is the parity check bit for row 3 or for column 3.

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

$$M = \left[\begin{array}{cc|c} b_1 & b_2 & d_1 \\ b_3 & b_4 & d_2 \\ \hline c_1 & c_2 & c_3 \end{array}\right].$$

- d_1 is the parity check bit for row 1
- d_2 is the parity check bit for row 2
- c_1 is the parity check bit for column 1
- c_2 is the parity check bit for column 2
- c_3 in the lower right hand corner (row 3, col 3) is the parity check bit for row 3 or for column 3. You get the same answer either way.

The Tic–tac–toe Code

Store the original message $m = b_1 b_2 b_3 b_4$ in a 3 by 3 tic-tac-toe board:

$$M = \left[\begin{array}{cc|c} b_1 & b_2 & d_1 \\ b_3 & b_4 & d_2 \\ \hline c_1 & c_2 & c_3 \end{array}\right].$$

- d_1 is the parity check bit for row 1
- d_2 is the parity check bit for row 2
- c_1 is the parity check bit for column 1
- c_2 is the parity check bit for column 2
- c_3 in the lower right hand corner (row 3, col 3) is the parity check bit for row 3 or for column 3. You get the same answer either way. Why?

Example

The message $m = 1011$ is encoded:

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & ? \\ 1 & 1 & \\ & & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & \\ & & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & ? \\ & & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ & & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ ? & & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & ? & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & ? \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Note: the numbers of 1's in each column and each row is always even.

Example

The message $m = 1011$ is encoded:

$$M = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Note: the numbers of 1's in each column and each row is always even.
If the receiver gets a message with an odd number of 1's in a row or column, she knows an error occurred somewhere in that row or column.

Example Cont'd

Suppose she receives

$$M' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Example Cont'd

Suppose she receives

$$M' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

- Both the second row and the first column contain a single 1.

Example Cont'd

Suppose she receives

$$M' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

- Both the second row and the first column contain a single 1.
- Since the number 1 is odd, an error must have occurred in

row 2, column 1.

Example Cont'd

Suppose she receives

$$M' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

- Both the second row and the first column contain a single 1.
- Since the number 1 is odd, an error must have occurred in

  row 2, column 1.
- Not only have we detected an error,

Example Cont'd

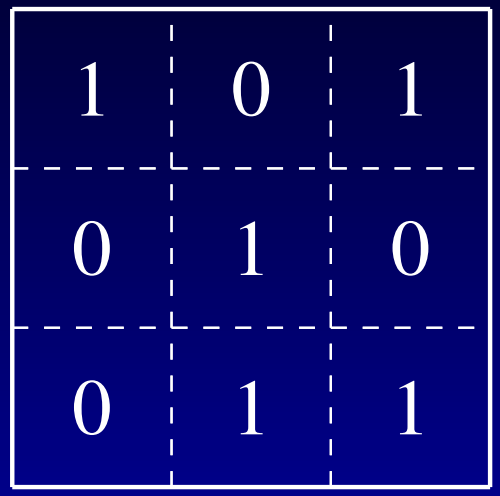
Suppose she receives

$$M' = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

- Both the second row and the first column contain a single 1.
- Since the number 1 is odd, an error must have occurred in

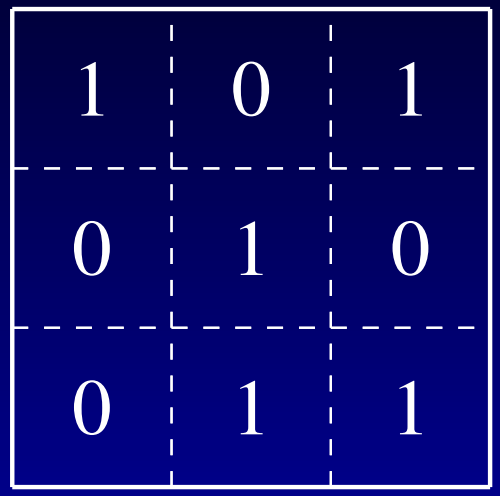
  row 2, column 1.
- Not only have we detected an error,
- but we know where it occurred!

Correcting the Error



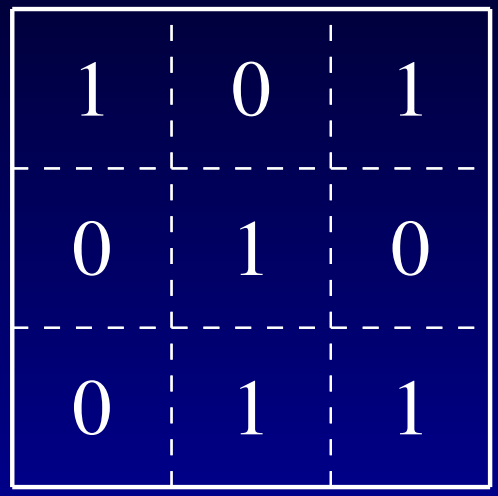
Correcting the Error

error in row 2



Correcting the Error

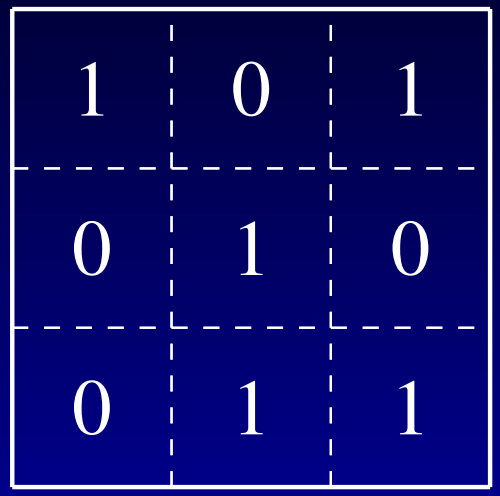
error in row 2



error in
col 1

Correcting the Error

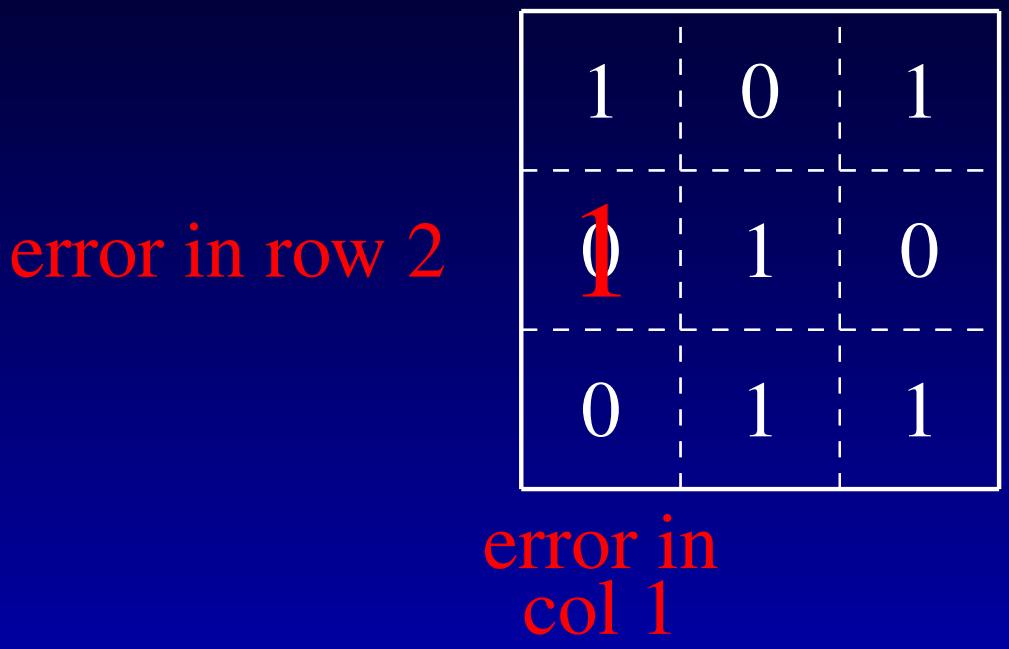
error in row 2



error in
col 1

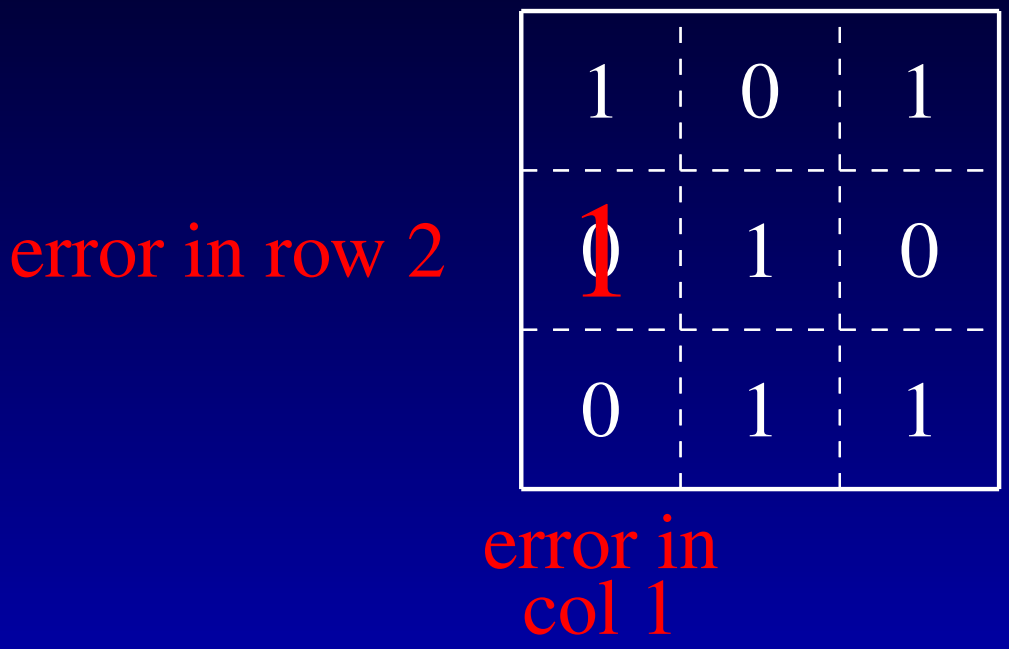
Change the 0 in row 2, column 1 to a 1.

Correcting the Error



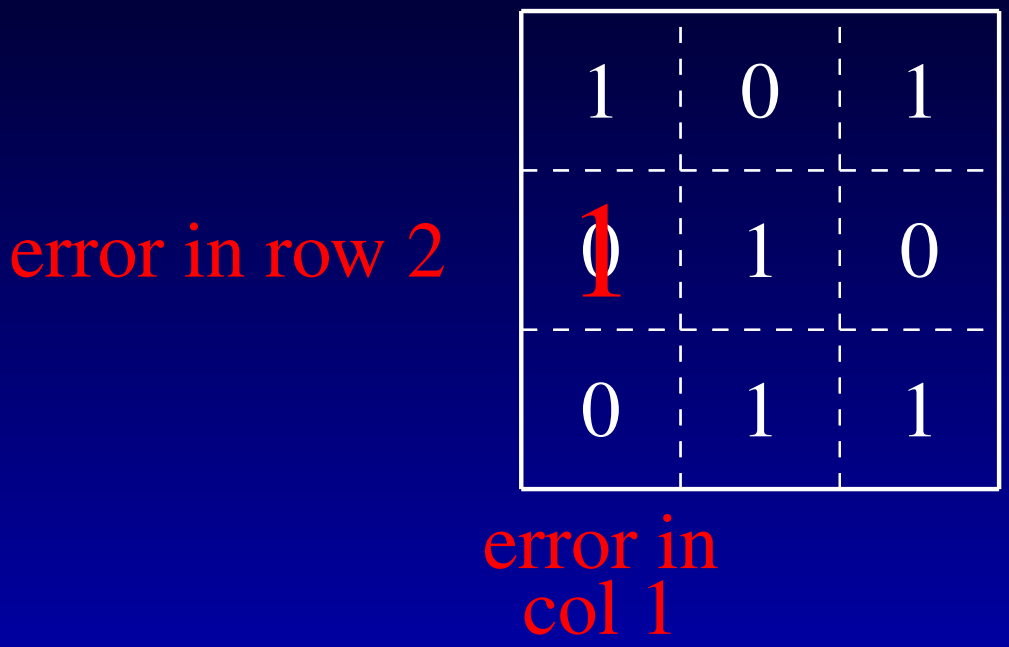
Change the 0 in row 2, column 1 to a 1.

Correcting the Error



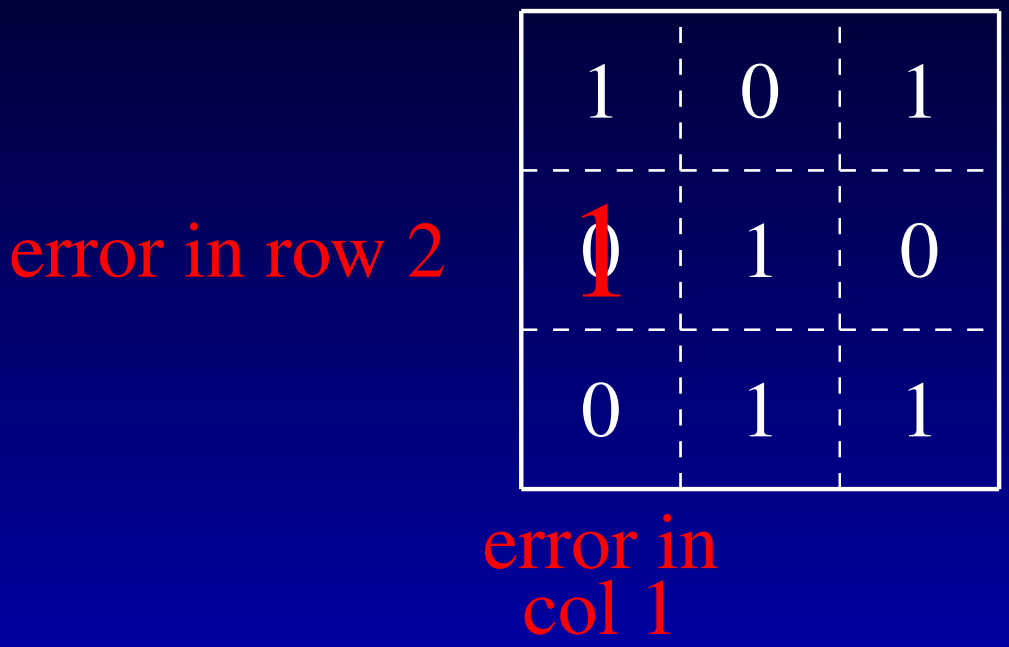
Change the 0 in row 2, column 1 to a 1.
We thus recover the correct transmitted message M.

Correcting the Error



Change the 0 in row 2, column 1 to a 1.
We thus recover the correct transmitted message M.
To obtain the original four-bit message m, simply peel off the 5 parity check bits from M.

Correcting the Error



Change the 0 in row 2, column 1 to a 1.
We thus recover the correct transmitted message M.
To obtain the original four-bit message m, simply peel off the 5 parity check bits from M.

$$m = 1\ 0\ 1\ 1$$

Exercise 1

Encode the following messages in the Tic-tac-toe code:
1011

Exercise 1

Encode the following messages in the Tic-tac-toe code:

1011

0110

Exercise 1

Encode the following messages in the Tic-tac-toe code:

1011

0110

1111.

Exercise 2

Decode the following messages using the Tic-tac-toe code:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Exercise 2

Decode the following messages using the Tic-tac-toe code:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

Exercise 2

Decode the following messages using the Tic-tac-toe code:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$$

Exercise 2

Decode the following messages using the Tic-tac-toe code:

$$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \qquad \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}$$

Exercise 3

Using the Tic-tac-toe code, can you detect two errors?

Exercise 3

Using the Tic-tac-toe code, can you detect two errors? Are you able to correct both errors?

Exercise 3

Using the Tic-tac-toe code, can you detect two errors?
Are you able to correct both errors?
Given examples to support your answers.

The Pails of Water Problem

You have a 5 and a 7 quart pail.

The Pails of Water Problem

You have a 5 and a 7 quart pail.
How can you measure exactly 1 quart of water, by pouring water back and forth between the two pails?

The Pails of Water Problem

You have a 5 and a 7 quart pail.
How can you measure exactly 1 quart of water, by pouring water back and forth between the two pails?
You are allowed to fill and empty each pail as many times as needed.

The Pails of Water Problem

You have a 5 and a 7 quart pail.
How can you measure exactly 1 quart of water, by pouring water back and forth between the two pails?
You are allowed to fill and empty each pail as many times as needed.
Split into groups and work on this problem.

The Pails of Water Problem

You have a 5 and a 7 quart pail.
How can you measure exactly 1 quart of water, by pouring water back and forth between the two pails?
You are allowed to fill and empty each pail as many times as needed.
Split into groups and work on this problem.
The first group to finish should write their solution on the whiteboard.

One solution:

5-qt	7-qt	Explanation
		fill 5-quart pail

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
		transfer 5 quarts into 7

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
		fill 5-quart pail a second time

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
		pour 2 quarts from 5 into 7

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
		empty 7-quart pail

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail
		transfer 3 quarts into 7

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail
0	3	transfer 3 quarts into 7

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail
0	3	transfer 3 quarts into 7
		fill 5-quart pail a third time

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail
0	3	transfer 3 quarts into 7
5	3	fill 5-quart pail a third time

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail
0	3	transfer 3 quarts into 7
5	3	fill 5-quart pail a third time
		transfer 4 quarts from 5 into 7

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail
0	3	transfer 3 quarts into 7
5	3	fill 5-quart pail a third time
1	7	transfer 4 quarts from 5 into 7

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail
0	3	transfer 3 quarts into 7
5	3	fill 5-quart pail a third time
1	7	transfer 4 quarts from 5 into 7
		empty 7-quart pail a second time

One solution:

5-qt	7-qt	Explanation
5	0	fill 5-quart pail
0	5	transfer 5 quarts into 7
5	5	fill 5-quart pail a second time
3	7	pour 2 quarts from 5 into 7
3	0	empty 7-quart pail
0	3	transfer 3 quarts into 7
5	3	fill 5-quart pail a third time
1	7	transfer 4 quarts from 5 into 7
1	0	empty 7-quart pail a second time

An Arithmetic Explanation

What happened?

An Arithmetic Explanation

What happened?
Notice that we filled the 5-quart pail three times

An Arithmetic Explanation

What happened?
Notice that we filled the 5-quart pail three times and emptied the 7-quart pail twice.

An Arithmetic Explanation

What happened?
Notice that we filled the 5-quart pail three times and emptied the 7-quart pail twice.
A little thought convinces us that the method given above can be written more succintly as:

An Arithmetic Explanation

What happened?
Notice that we filled the 5-quart pail three times and emptied the 7-quart pail twice.
A little thought convinces us that the method given above can be written more succintly as:

$$3 \times 5 - 2 \times 7 = 1.$$

The Pails of Water Problem

Given two positive integers a and b,

The Pails of Water Problem

Given two positive integers a and b, the "Pails of Water Problem"

The Pails of Water Problem

Given two positive integers a and b, the "Pails of Water Problem" (abbreviated as POW)

The Pails of Water Problem

Given two positive integers a and b, the "Pails of Water Problem" (abbreviated as POW) means: find two numbers m and n so that

The Pails of Water Problem

Given two positive integers a and b, the "Pails of Water Problem" (abbreviated as POW) means: find two numbers m and n so that

$$ma - nb = 1$$

POW Problem #2

Solve the POW problem if $a = 10$ and $b = 19$.

POW Problem #2

Solve the POW problem if $a = 10$ and $b = 19$. That is, find numbers m and n which satisfy the equation:

POW Problem #2

Solve the POW problem if $a = 10$ and $b = 19$. That is, find numbers m and n which satisfy the equation:

$$10m - 19n = 1$$

POW Problem #2

Solve the POW problem if $a = 10$ and $b = 19$. That is, find numbers m and n which satisfy the equation:

$$10m - 19n = 1$$

Hint: This is very easy.

POW Problem #3

Solve the POW problem if $a = 7$ and $b = 9$.

POW Problem #3

Solve the POW problem if $a = 7$ and $b = 9$.
That is, find numbers m and n which satisfy the equation:

POW Problem #3

Solve the POW problem if $a = 7$ and $b = 9$. That is, find numbers m and n which satisfy the equation:

$$7m - 9n = 1$$

POW Problem #4

Solve the POW problem if $a = 11$ and $b = 8$.

POW Problem #4

Solve the POW problem if $a = 11$ and $b = 8$. That is, find numbers m and n which satisfy the equation:

POW Problem #4

Solve the POW problem if $a = 11$ and $b = 8$. That is, find numbers m and n which satisfy the equation:

$$11m - 8n = 1$$

POW Problem #5

Solve the POW problem if $a = 6$ and $b = 10$.

POW Problem #5

Solve the POW problem if $a = 6$ and $b = 10$. That is, find numbers m and n which satisfy the equation:

POW Problem #5

Solve the POW problem if $a = 6$ and $b = 10$. That is, find numbers m and n which satisfy the equation:

$$6m - 10n = 1$$

Trouble Brewing

This last example $a = 6$ and $b = 10$ shows that not all POW problems can be solved,

Trouble Brewing

This last example $a = 6$ and $b = 10$ shows that not all POW problems can be solved, that is, you cannot always get a 1 in the equation

Trouble Brewing

This last example $a = 6$ and $b = 10$ shows that not all POW problems can be solved, that is, you cannot always get a 1 in the equation

$$ma - nb = 1$$

Trouble Brewing

This last example $a = 6$ and $b = 10$ shows that not all POW problems can be solved, that is, you cannot always get a 1 in the equation

$$ma - nb = 1$$

What has to be true about a and b so that the POW problem has a solution?

Switching a and b

When $a = 5$ and $b = 7$ a solution to the POW problem is

Switching a and b

When $a = 5$ and $b = 7$ a solution to the POW problem is

$$3 \times 5 - 2 \times 7 = 1$$

Switching a and b

When $a = 5$ and $b = 7$ a solution to the POW problem is

$$3 \times 5 - 2 \times 7 = 1$$

What if we switch the 5 and 7 and ask for an equation

$$m \times 7 - n \times 5 = 1$$

Switching a and b

When $a = 5$ and $b = 7$ a solution to the POW problem is

$$3 \times 5 - 2 \times 7 = 1$$

What if we switch the 5 and 7 and ask for an equation

$$m \times 7 - n \times 5 = 1$$

Essentially, this means that we are filling the 7-quart pail and emptying into the 5-quart pail.

Switching a and b

When $a = 5$ and $b = 7$ a solution to the POW problem is

$$3 \times 5 - 2 \times 7 = 1$$

What if we switch the 5 and 7 and ask for an equation

$$m \times 7 - n \times 5 = 1$$

Essentially, this means that we are filling the 7-quart pail and emptying into the 5-quart pail.
Can you solve this equation?

Switching a and b

In general, in seeking a solution to the POW problem, we will be content with either

Switching a and b

In general, in seeking a solution to the POW problem, we will be content with either

$$m \times a - n \times b = 1$$

Switching a and b

In general, in seeking a solution to the POW problem, we will be content with either

$$m \times a - n \times b = 1$$

or

Switching a and b

In general, in seeking a solution to the POW problem, we will be content with either

$$m \times a - n \times b = 1$$

or

$$m \times b - n \times a = 1$$

Switching a and b

In general, in seeking a solution to the POW problem, we will be content with either

$$m \times a - n \times b = 1$$

or

$$m \times b - n \times a = 1$$

Either equation solves POW.

Connecting the two solutions

Do you see any way to connect the two solutions:

Connecting the two solutions

Do you see any way to connect the two solutions:
Solution 1. $3 \times 5 - 2 \times 7 = 1$ and

Connecting the two solutions

Do you see any way to connect the two solutions:
Solution 1. $3 \times 5 - 2 \times 7 = 1$ and
Solution 2. $3 \times 7 - 4 \times 5 = 1$.

Connecting the two solutions

Do you see any way to connect the two solutions:
Solution 1. $3 \times 5 - 2 \times 7 = 1$ and
Solution 2. $3 \times 7 - 4 \times 5 = 1$.
Hint: look at the equation

$$3 \times 5 - 2 \times 7 = 3 \times 7 - 4 \times 5 = 1$$

When the numbers get big

Now suppose you wish to obtain one quart with a 7-quart and a 19-quart pail.

When the numbers get big

Now suppose you wish to obtain one quart with a 7-quart and a 19-quart pail.
That is, you want to solve the equation

When the numbers get big

Now suppose you wish to obtain one quart with a 7-quart and a 19-quart pail.
That is, you want to solve the equation

$$19m - 7n = 1$$

When the numbers get big

Now suppose you wish to obtain one quart with a 7-quart and a 19-quart pail.
That is, you want to solve the equation

$$19m - 7n = 1$$

Try it!

When the numbers get big

Here is a secret to the POW Problem (19, 7).

When the numbers get big

Here is a secret to the POW Problem (19, 7). Fill the 19-quart pail two times from the 7-quart pail,

When the numbers get big

Here is a secret to the POW Problem (19, 7). Fill the 19-quart pail two times from the 7-quart pail, thereby effectively converting the 19-quart pail into a 5-quart pail.

When the numbers get big

Here is a secret to the POW Problem (19, 7). Fill the 19-quart pail two times from the 7-quart pail, thereby effectively converting the 19-quart pail into a 5-quart pail. The associated equation is

$$5 = 19 - 2 \times 7$$

When the numbers get big

Here is a secret to the POW Problem (19, 7). Fill the 19-quart pail two times from the 7-quart pail, thereby effectively converting the 19-quart pail into a 5-quart pail. The associated equation is

$$5 = 19 - 2 \times 7$$

But we know how to solve the POW problem with the numbers of 7 and 5.

Arithmetic Magic

Here's how it works:

Explanation

Arithmetic Magic

Here's how it works:

Equation	Explanation

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	subst $5 = 19 - 2 \times 7$

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	subst $5 = 19 - 2 \times 7$
$= 3 \times 19 - 6 \times 7 - 2 \times 7$	

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	subst $5 = 19 - 2 \times 7$
$= 3 \times 19 - 6 \times 7 - 2 \times 7$	expand the parentheses

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	subst $5 = 19 - 2 \times 7$
$= 3 \times 19 - 6 \times 7 - 2 \times 7$	expand the parentheses
$= 3 \times 19 - 8 \times 7$	

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	subst $5 = 19 - 2 \times 7$
$= 3 \times 19 - 6 \times 7 - 2 \times 7$	expand the parentheses
$= 3 \times 19 - 8 \times 7$	gather the 7's together.

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	subst $5 = 19 - 2 \times 7$
$= 3 \times 19 - 6 \times 7 - 2 \times 7$	expand the parentheses
$= 3 \times 19 - 8 \times 7$	gather the 7's together.

The solution is to fill the 19-quart pair three times, a total of 57 quarts,

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	subst $5 = 19 - 2 \times 7$
$= 3 \times 19 - 6 \times 7 - 2 \times 7$	expand the parentheses
$= 3 \times 19 - 8 \times 7$	gather the 7's together.

The solution is to fill the 19-quart pair three times, a total of 57 quarts, and empty into the 7-quart pail eight times, a total loss of 56 quarts.

Arithmetic Magic

Here's how it works:

Equation	Explanation
$1 = 3 \times 5 - 2 \times 7$	solution for 5 and 7
$= 3 \times (19 - 2 \times 7) - 2 \times 7$	subst $5 = 19 - 2 \times 7$
$= 3 \times 19 - 6 \times 7 - 2 \times 7$	expand the parentheses
$= 3 \times 19 - 8 \times 7$	gather the 7's together.

The solution is to fill the 19-quart pair three times, a total of 57 quarts, and empty into the 7-quart pail eight times, a total loss of 56 quarts. The difference is precisely 1 quart.

Are you ready?

Use this Super Secret Way to solve the POW Problem with the numbers 100 and 77.

POW(100,77)

Equation

POW(100,77)

Equation

Explanation

POW(100,77)

Equation

$1 = 3 \times 8 - 23$

Explanation

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23

POW(100,77)

Equation

$1 = 3 \times 8 - 23$

$= 3 \times (77 - 3 \times 23) - 23$

Explanation

solution for 8 and 23

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together
$= 3 \times 77 - 10 \times (100 - 77)$	

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together
$= 3 \times 77 - 10 \times (100 - 77)$	subst $23 = 100 - 77$

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together
$= 3 \times 77 - 10 \times (100 - 77)$	subst $23 = 100 - 77$
$= 3 \times 77 - 10 \times 100 + 10 \times 77$	

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together
$= 3 \times 77 - 10 \times (100 - 77)$	subst $23 = 100 - 77$
$= 3 \times 77 - 10 \times 100 + 10 \times 77$	expand the parentheses

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together
$= 3 \times 77 - 10 \times (100 - 77)$	subst $23 = 100 - 77$
$= 3 \times 77 - 10 \times 100 + 10 \times 77$	expand the parentheses
$= 13 \times 77 - 10 \times 100$	

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together
$= 3 \times 77 - 10 \times (100 - 77)$	subst $23 = 100 - 77$
$= 3 \times 77 - 10 \times 100 + 10 \times 77$	expand the parentheses
$= 13 \times 77 - 10 \times 100$	gather the 77's together

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together
$= 3 \times 77 - 10 \times (100 - 77)$	subst $23 = 100 - 77$
$= 3 \times 77 - 10 \times 100 + 10 \times 77$	expand the parentheses
$= 13 \times 77 - 10 \times 100$	gather the 77's together

Do these numbers check out?

POW(100,77)

Equation	Explanation
$1 = 3 \times 8 - 23$	solution for 8 and 23
$= 3 \times (77 - 3 \times 23) - 23$	subst $8 = 77 - 3 \times 23$
$= 3 \times 77 - 9 \times 23 - 23$	expand the parentheses
$= 3 \times 77 - 10 \times 23$	gather the 23's together
$= 3 \times 77 - 10 \times (100 - 77)$	subst $23 = 100 - 77$
$= 3 \times 77 - 10 \times 100 + 10 \times 77$	expand the parentheses
$= 13 \times 77 - 10 \times 100$	gather the 77's together

Do these numbers check out? What's 13×77 and 10×100.

Today's Pop Quiz

Solve the POW Problem with the numbers 31 and 9.

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b.

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b. Let's say that a is smaller than b.

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b. Let's say that a is smaller than b. If you can't think of the solution right away because the numbers are too large,

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b. Let's say that a is smaller than b. If you can't think of the solution right away because the numbers are too large, reduce the problem to two smaller numbers,

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b. Let's say that a is smaller than b. If you can't think of the solution right away because the numbers are too large, reduce the problem to two smaller numbers, by dividing the smaller number a into b,

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b. Let's say that a is smaller than b. If you can't think of the solution right away because the numbers are too large, reduce the problem to two smaller numbers, by dividing the smaller number a into b, getting a quotient q and a remainder r.

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b. Let's say that a is smaller than b. If you can't think of the solution right away because the numbers are too large, reduce the problem to two smaller numbers, by dividing the smaller number a into b, getting a quotient q and a remainder r.

Write this as

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b. Let's say that a is smaller than b. If you can't think of the solution right away because the numbers are too large, reduce the problem to two smaller numbers, by dividing the smaller number a into b, getting a quotient q and a remainder r.

Write this as

$$r = b - q \times a.$$

Quotient and Remainder Method

In general, suppose you want to solve the POW problem with two numbers, a and b. Let's say that a is smaller than b. If you can't think of the solution right away because the numbers are too large, reduce the problem to two smaller numbers, by dividing the smaller number a into b, getting a quotient q and a remainder r.
Write this as

$$r = b - q \times a.$$

Record this equation as you will need it later.

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a.

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a. You can write this reduction as

$$(a, b) \rightarrow (r, a).$$

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a. You can write this reduction as

$$(a, b) \rightarrow (r, a).$$

If the numbers r and a are still too big, reduce again,

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a. You can write this reduction as

$$(a, b) \rightarrow (r, a).$$

If the numbers r and a are still too big, reduce again, by dividing r into a.

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a. You can write this reduction as

$$(a, b) \rightarrow (r, a).$$

If the numbers r and a are still too big, reduce again, by dividing r into a.
Eventually you will reach two numbers that you can do in your head.

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a. You can write this reduction as

$$(a, b) \rightarrow (r, a).$$

If the numbers r and a are still too big, reduce again, by dividing r into a.
Eventually you will reach two numbers that you can do in your head. Starting with this "easy" solution,

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a. You can write this reduction as

$$(a, b) \rightarrow (r, a).$$

If the numbers r and a are still too big, reduce again, by dividing r into a.
Eventually you will reach two numbers that you can do in your head. Starting with this "easy" solution, carefully work backwards,

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a. You can write this reduction as

$$(a, b) \rightarrow (r, a).$$

If the numbers r and a are still too big, reduce again, by dividing r into a.
Eventually you will reach two numbers that you can do in your head. Starting with this "easy" solution, carefully work backwards, substituting the "remainder" equations you previously recorded,

Working backwards

The original POW problem a and b *reduces* to solving POW with the smaller numbers r and a. You can write this reduction as

$$(a, b) \rightarrow (r, a).$$

If the numbers r and a are still too big, reduce again, by dividing r into a.
Eventually you will reach two numbers that you can do in your head. Starting with this "easy" solution, carefully work backwards, substituting the "remainder" equations you previously recorded, until you reach a solution using the original numbers a and b.

Giving credit to Euclid

This method for solving the pails of water problem is called the *Euclidean algorithm*.

Giving credit to Euclid

This method for solving the pails of water problem is called the *Euclidean algorithm*. An algorithm is a set of steps for completing some task.

Giving credit to Euclid

This method for solving the pails of water problem is called the *Euclidean algorithm*. An algorithm is a set of steps for completing some task. (No, the word is not named after Bill Clinton's vice president.)

Giving credit to Euclid

This method for solving the pails of water problem is called the *Euclidean algorithm*. An algorithm is a set of steps for completing some task. (No, the word is not named after Bill Clinton's vice president.) Who was that?

Giving credit to Euclid

This method for solving the pails of water problem is called the *Euclidean algorithm*. An algorithm is a set of steps for completing some task. (No, the word is not named after Bill Clinton's vice president.) A recipe from a cookbook is a good example of an algorithm.

Giving credit to Euclid

This method for solving the pails of water problem is called the *Euclidean algorithm*. An algorithm is a set of steps for completing some task. (No, the word is not named after Bill Clinton's vice president.) A recipe from a cookbook is a good example of an algorithm.

This particular procedure dates back over two thousand years ago to the African mathematician Euclid, who also founded plane geometry.

Giving credit to Euclid

This method for solving the pails of water problem is called the *Euclidean algorithm*. An algorithm is a set of steps for completing some task. (No, the word is not named after Bill Clinton's vice president.) A recipe from a cookbook is a good example of an algorithm.

This particular procedure dates back over two thousand years ago to the African mathematician Euclid, who also founded plane geometry.

Ten minute activity: Google search "Euclid" and write down 3 interesting facts about him.

Ten Minute Activity

Google search “Euclid”

Ten Minute Activity

Google search “Euclid”
Write down 3 interesting facts about him.

Clock Arithmetic

It’s 6 o’clock at night.

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour,

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours,

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours, study for 4 hours.

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours, study for 4 hours.
What time are you done studying?

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours, study for 4 hours.
What time are you done studying?
If we add the time intervals,

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours, study for 4 hours.
What time are you done studying?
If we add the time intervals, we get
$6 + 1 + 2 + 4 = 13$.

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours, study for 4 hours.
What time are you done studying?
If we add the time intervals, we get
$6 + 1 + 2 + 4 = 13$.
But 13 o'clock is not a valid time

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours, study for 4 hours.
What time are you done studying?
If we add the time intervals, we get
$6 + 1 + 2 + 4 = 13$.
But 13 o'clock is not a valid time (except in the army).

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours, study for 4 hours.
What time are you done studying?
If we add the time intervals, we get
$6 + 1 + 2 + 4 = 13$.
But 13 o'clock is not a valid time (except in the army). The time will be 1 in the morning,

Clock Arithmetic

It's 6 o'clock at night. You eat supper for one hour, watch TV for 2 hours, study for 4 hours.
What time are you done studying?
If we add the time intervals, we get
$6 + 1 + 2 + 4 = 13$.
But 13 o'clock is not a valid time (except in the army). The time will be 1 in the morning, which we get by subtracting 12 from 13.

Standard 12–Clock

In mathematics we write this as:

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12,

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12, the time resets to 0.

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12, the time resets to 0.
Similarly, 25 mod 12 = 1 and

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12, the time resets to 0.
Similarly, 25 mod 12 = 1 and
$-2 \bmod 12 = 10$, that is,

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12, the time resets to 0.
Similarly, 25 mod 12 = 1 and
$-2 \bmod 12 = 10$, that is,
2 hours *before* 12 is 10 o'clock.

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12, the time resets to 0.
Similarly, 25 mod 12 = 1 and
$-2 \bmod 12 = 10$, that is,
2 hours *before* 12 is 10 o'clock.

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12, the time resets to 0.
Similarly, 25 mod 12 = 1 and
$-2 \bmod 12 = 10$, that is,
2 hours *before* 12 is 10 o'clock.

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12, the time resets to 0.
Similarly, 25 mod 12 = 1 and
$-2 \bmod 12 = 10$, that is,
2 hours *before* 12 is 10 o'clock.

Standard 12–Clock

In mathematics we write this as:

$$13 \bmod 12 = 1.$$

On a standard 12-clock, once you reach the number 12, the time resets to 0.
Similarly, 25 mod 12 = 1 and
$-2 \bmod 12 = 10$, that is,
2 hours *before* 12 is 10 o'clock.

Other Clocks

We are familiar with different clocks besides the 12-clock.

Other Clocks

We are familiar with different clocks besides the 12-clock.

Other Clocks

We are familiar with different clocks besides the 12-clock.

Other Clocks

We are familiar with different clocks besides the 12-clock.

Other Clocks

We are familiar with different clocks besides the 12-clock.

Other Clocks

We are familiar with different clocks besides the 12-clock.

Other Clocks

We are familiar with different clocks besides the 12-clock.
For example, we can think of the days of the week as lying on a 7-clock.
It is convenient to assign the days the values:
Sun $= 0$, Mon $= 1$, Tues $= 2, \cdots,$ Sat $= 6$.
Suppose you begin a trip for Florida on Wednesday. You spend 2 days driving. You stay in a hotel in Orlando for 6 days, and a hotel in Miami for 5 days. It takes 2 days to drive home. On what day do you return home?

Other Clocks

We are familiar with different clocks besides the 12-clock.
For example, we can think of the days of the week as lying on a 7-clock.
It is convenient to assign the days the values:
Sun $= 0$, Mon $= 1$, Tues $= 2, \cdots,$ Sat $= 6$.
Suppose you begin a trip for Florida on Wednesday. You spend 2 days driving. You stay in a hotel in Orlando for 6 days, and a hotel in Miami for 5 days. It takes 2 days to drive home. On what day do you return home?
Since Wednesday is day number 3, we can add up all the days to get:

Other Clocks

We are familiar with different clocks besides the 12-clock.
For example, we can think of the days of the week as lying on a 7-clock.
It is convenient to assign the days the values:
Sun $= 0$, Mon $= 1$, Tues $= 2, \cdots,$ Sat $= 6$.
Suppose you begin a trip for Florida on Wednesday. You spend 2 days driving. You stay in a hotel in Orlando for 6 days, and a hotel in Miami for 5 days. It takes 2 days to drive home. On what day do you return home?
Since Wednesday is day number 3, we can add up all the days to get:

$$3 + 2 + 6 + 5 + 2 = 18.$$

Other Clocks

We are familiar with different clocks besides the 12-clock.
For example, we can think of the days of the week as lying on a 7-clock.
It is convenient to assign the days the values:
Sun $= 0$, Mon $= 1$, Tues $= 2, \cdots,$ Sat $= 6$.
Suppose you begin a trip for Florida on Wednesday. You spend 2 days driving. You stay in a hotel in Orlando for 6 days, and a hotel in Miami for 5 days. It takes 2 days to drive home. On what day do you return home?
Since Wednesday is day number 3, we can add up all the days to get:

$$3 + 2 + 6 + 5 + 2 = 18.$$

Other Clocks

We are familiar with different clocks besides the 12-clock.
For example, we can think of the days of the week as lying on a 7-clock.
It is convenient to assign the days the values:
Sun $= 0$, Mon $= 1$, Tues $= 2, \cdots,$ Sat $= 6$.
Suppose you begin a trip for Florida on Wednesday. You spend 2 days driving. You stay in a hotel in Orlando for 6 days, and a hotel in Miami for 5 days. It takes 2 days to drive home. On what day do you return home?
Since Wednesday is day number 3, we can add up all the days to get:

$$3 + 2 + 6 + 5 + 2 = 18.$$

Pennies

The number of pennies needed in the exact change for a purchase can be computed using a 5-clock.

Pennies

The number of pennies needed in the exact change for a purchase can be computed using a 5-clock.
For example, suppose you buy a $1.99 sandwich, a $.89 drink, and the tax is 26 cents.

Pennies

The number of pennies needed in the exact change for a purchase can be computed using a 5-clock.
For example, suppose you buy a $1.99 sandwich, a $.89 drink, and the tax is 26 cents.
How many pennies do you need to pay the bill with exact change?

Pennies

The number of pennies needed in the exact change for a purchase can be computed using a 5-clock.
For example, suppose you buy a $1.99 sandwich, a $.89 drink, and the tax is 26 cents.
How many pennies do you need to pay the bill with exact change?
Adding the three numbers as cents, we have

Pennies

The number of pennies needed in the exact change for a purchase can be computed using a 5-clock.
For example, suppose you buy a \$1.99 sandwich, a \$.89 drink, and the tax is 26 cents.
How many pennies do you need to pay the bill with exact change?
Adding the three numbers as cents, we have

$$(199 + 89 + 26) \bmod 5 = 314 \bmod 5 = 4.$$

Pennies

The number of pennies needed in the exact change for a purchase can be computed using a 5-clock.
For example, suppose you buy a \$1.99 sandwich, a \$.89 drink, and the tax is 26 cents.
How many pennies do you need to pay the bill with exact change?
Adding the three numbers as cents, we have

$$(199 + 89 + 26) \bmod 5 = 314 \bmod 5 = 4.$$

You need 4 pennies (plus a dime and 3 dollars).

General n-clock

In general, on an n-clock we write

$$a \bmod n = r$$

General n-clock

In general, on an n-clock we write

$$a \bmod n = r$$

if r is the remainder when you divide a by n.

General n-clock

In general, on an n-clock we write

$$a \bmod n = r$$

if r is the remainder when you divide a by n.
We also say "a reduces to r, mod n."

Addition Table mod 5

$+$	0	1	2	3	4
0					
1					
2					
3					
4					

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1					
2					
3					
4					

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1				
2	2				
3	3				
4	4				

Addition Table mod 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2			
2	2				
3	3				
4	4				

Addition Table mod 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3		
2	2				
3	3				
4	4				

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	
2	2				
3	3				
4	4				

Addition Table mod 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2				
3	3				
4	4				

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3			
3	3	4			
4	4	0			

Addition Table mod 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4		
3	3	4			
4	4	0			

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	
3	3	4			
4	4	0			

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4			
4	4	0			

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0		
4	4	0	1		

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	
4	4	0	1		

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1		

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	

Addition Table mod 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Multiplication Table mod 5

$\times$	0	1	2	3	4
0					
0					
2					
3					
4					

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0					
2					
3					
4					

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0				
2	0				
3	0				
4	0				

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0				
3	0				
4	0				

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2			
3	0	3			
4	0	4			

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4		
3	0	3			
4	0	4			

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	
3	0	3			
4	0	4			

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3			
4	0	4			

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1		
4	0	4	3		

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	
4	0	4	3		

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3		

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The zero row and zero column consists of all 0's.

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The zero row and zero column consists of all 0's.
What did we expect?

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The zero row and zero column consists of all 0's.
What did we expect? Zero times anything is zero.

Multiplication Table mod 5

$\times$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The zero row and zero column consists of all 0's.
What did we expect? Zero times anything is zero.
If we ignore the 0 row and column, find 3 interesting facts about the rest of the times table.

Multiplication Table mod 5

Notice that the numbers 1, 2, 3, and 4 are scrambled when we multiply by 2, 3, or 4.

Multiplication Table mod 5

Notice that the numbers 1, 2, 3, and 4 are scrambled when we multiply by 2, 3, or 4.
That is, each of the rows list the numbers 1, 2, 3, 4 in some order.

Multiplication Table mod 5

Notice that the numbers 1, 2, 3, and 4 are scrambled when we multiply by 2, 3, or 4.
That is, each of the rows list the numbers 1, 2, 3, 4 in some order.
Second row: 2, 4, 1, 3;

Multiplication Table mod 5

Notice that the numbers 1, 2, 3, and 4 are scrambled when we multiply by 2, 3, or 4.
That is, each of the rows list the numbers 1, 2, 3, 4 in some order.
Second row: 2, 4, 1, 3;
Third row: 3, 1, 4, 2;

Multiplication Table mod 5

Notice that the numbers 1, 2, 3, and 4 are scrambled when we multiply by 2, 3, or 4.
That is, each of the rows list the numbers 1, 2, 3, 4 in some order.
Second row: 2, 4, 1, 3;
Third row: 3, 1, 4, 2;
Last row: the numbers are backwards 4, 3, 2, 1.

Multiplication Table mod 5

Notice that the numbers 1, 2, 3, and 4 are scrambled when we multiply by 2, 3, or 4.
That is, each of the rows list the numbers 1, 2, 3, 4 in some order.
Second row: 2, 4, 1, 3;
Third row: 3, 1, 4, 2;
Last row: the numbers are backwards 4, 3, 2, 1.
This scrambing phenomenon is the key idea in constructing the secret codes discussed in the next section.

Birthdays

Your birthday is on Monday this year.

Birthdays

Your birthday is on Monday this year.
On what day will your birthday occur next year?

Birthdays

Your birthday is on Monday this year.
On what day will your birthday occur next year?
Note that the answer depends on whether there is a leap year (giving an additional calendar day February 29) in the upcoming year.

Exercises

Compute (a) $(11 + 23 - 5) \bmod 7$

Exercises

Compute (a) $(11 + 23 - 5) \bmod 7$
(b) $1000 \bmod 7$

Exercises

Compute (a) $(11 + 23 - 5) \bmod 7$
(b) $1000 \bmod 7$
(c) $250 \bmod 31$.

7–clock

Construct the $\times$ table for the 7-clock.

7–clock

Construct the $\times$ table for the 7-clock.
Do the rows scramble the numbers 1 — 6?

6–clock

Construct the $\times$ table for the 6-clock.

6–clock

Construct the $\times$ table for the 6-clock.
Do the rows scramble the numbers 1 — 5?

Secret Codes

We will use the fact that the multiplication on a 31-clock scrambles the numbers 1–30 to give a simple way to encode and decode messages.

- Assign each letter of the alphabet a number:

Secret Codes

We will use the fact that the multiplication on a 31-clock scrambles the numbers 1–30 to give a simple way to encode and decode messages.

- Assign each letter of the alphabet a number:
- $A = 1$, $B = 2$, $\ldots$, $Z = 26$.

Secret Codes

We will use the fact that the multiplication on a 31-clock scrambles the numbers 1–30 to give a simple way to encode and decode messages.

- Assign each letter of the alphabet a number:
- $A = 1$, $B = 2$, $\ldots$, $Z = 26$.
- We'll need some punctuation:

Secret Codes

We will use the fact that the multiplication on a 31-clock scrambles the numbers 1–30 to give a simple way to encode and decode messages.

- Assign each letter of the alphabet a number:
- $A = 1$, $B = 2$, $\ldots$, $Z = 26$.
- We'll need some punctuation:
  - period $= 27$

Secret Codes

We will use the fact that the multiplication on a 31-clock scrambles the numbers 1–30 to give a simple way to encode and decode messages.

- Assign each letter of the alphabet a number:
- $A = 1$, $B = 2$, $\ldots$, $Z = 26$.
- We'll need some punctuation:
  - period $= 27$
  - comma $= 28$

Secret Codes

We will use the fact that the multiplication on a 31-clock scrambles the numbers 1–30 to give a simple way to encode and decode messages.

- Assign each letter of the alphabet a number:
- $A = 1$, $B = 2$, $\ldots$, $Z = 26$.
- We'll need some punctuation:
  - period $= 27$
  - comma $= 28$
  - ? $= 29$ and

Secret Codes

We will use the fact that the multiplication on a 31-clock scrambles the numbers 1–30 to give a simple way to encode and decode messages.

- Assign each letter of the alphabet a number:
- $A = 1$, $B = 2$, $\ldots$, $Z = 26$.
- We'll need some punctuation:
  - period $= 27$
  - comma $= 28$
  - ? $= 29$ and
  - blank $= 30$.

$p = 31$ Secret Code Cont'd

- This is a rather crude code.

$p = 31$ Secret Code Cont'd

- This is a rather crude code.
- It doesn't allow for

$p = 31$ Secret Code Cont'd

- This is a rather crude code.
- It doesn't allow for
  - lower case letter

$p = 31$ Secret Code Cont'd

- This is a rather crude code.
- It doesn't allow for
  - lower case letter
  - the digits 0, 1, 2, . . . , 9

$p = 31$ Secret Code Cont'd

- This is a rather crude code.
- It doesn't allow for
  - lower case letter
  - the digits 0, 1, 2, . . . , 9
  - or many other punctuation symbols.

$p = 31$ Secret Code Cont'd

- This is a rather crude code.
- It doesn't allow for
  - lower case letter
  - the digits 0, 1, 2, . . . , 9
  - or many other punctuation symbols.
- But it will serve our purpose and the calculations are not too long.

$p = 31$ Secret Code Cont'd

- This is a rather crude code.
- It doesn't allow for
  - lower case letter
  - the digits 0, 1, 2, . . . , 9
  - or many other punctuation symbols.
- But it will serve our purpose and the calculations are not too long.
- Our modulus (clock number) is $p = 31$.

$p = 31$ Secret Code Cont'd

- This is a rather crude code.
- It doesn't allow for
  - lower case letter
  - the digits 0, 1, 2, . . . , 9
  - or many other punctuation symbols.
- But it will serve our purpose and the calculations are not too long.
- Our modulus (clock number) is $p = 31$.
- It is convenient to put our conversion values in a table, for easy referral.

31–Code Table

A	1	K	11	U	21
B	2	L	12	V	22
C	3	M	13	W	23
D	4	N	14	X	24
E	5	O	15	Y	25
F	6	P	16	Z	26
G	7	Q	17	.	27
H	8	R	18	,	28
I	9	S	19	?	29
J	10	T	20	bl	30

31–Code Table

A	1	K	11	U	21
B	2	L	12	V	22
C	3	M	13	W	23
D	4	N	14	X	24
E	5	O	15	Y	25
F	6	P	16	Z	26
G	7	Q	17	.	27
H	8	R	18	,	28
I	9	S	19	?	29
J	10	T	20	bl	30

31–Code Table

A	1	K	11	U	21
B	2	L	12	V	22
C	3	M	13	W	23
D	4	N	14	X	24
E	5	O	15	Y	25
F	6	P	16	Z	26
G	7	Q	17	.	27
H	8	R	18	,	28
I	9	S	19	?	29
J	10	T	20	bl	30

Encoding Messages

- In using the 31-code, we need an encoding number e between 2 and 30.

Encoding Messages

- In using the 31-code, we need an encoding number e between 2 and 30.
- Let's use the encoding number $e = 7$.

Encoding Messages

- In using the 31-code, we need an encoding number e between 2 and 30.
- Let's use the encoding number $e = 7$.
- Now suppose we wish to encode the message $H\ E\ L\ P$.

Encoding Messages

- In using the 31-code, we need an encoding number e between 2 and 30.
- Let's use the encoding number $e = 7$.
- Now suppose we wish to encode the message $H\ E\ L\ P$.
- We first convert each of the four letters H, E, L, P into its numerical equivalent, using the above table.

Encoding Messages Cont'd

- Since $H \to 8$, $E \to 5$, etc., our message becomes

$$8, \quad 5, \quad 12, \quad 16.$$

Encoding Messages Cont'd

- Since $H \to 8$, $E \to 5$, etc., our message becomes

$$8, \quad 5, \quad 12, \quad 16.$$

- Multiply each of these four numbers by the encoding number $e = 7$ to get

$$56, \quad 35, \quad 84, \quad 112.$$

Encoding Messages Cont'd

- Since $H \to 8$, $E \to 5$, etc., our message becomes

$$8, \quad 5, \quad 12, \quad 16.$$

- Multiply each of these four numbers by the encoding number $e = 7$ to get

$$56, \quad 35, \quad 84, \quad 112.$$

- Now reduce each number using the 31-clock:

$56 \bmod 31 = 25 \quad 35 \bmod 31 = 4$

$84 \bmod 31 = 22 \quad 112 \bmod 31 = 19$

to get the remainders

$$25, \quad 4, \quad 22, \quad 19.$$

Encoding Messages Cont'd

- Since $H \to 8$, $E \to 5$, etc., our message becomes

$$8, \quad 5, \quad 12, \quad 16.$$

- Multiply each of these four numbers by the encoding number $e = 7$ to get

$$56, \quad 35, \quad 84, \quad 112.$$

- Now reduce each number using the 31-clock:

$$56 \bmod 31 = 25 \quad 35 \bmod 31 = 4$$
$$84 \bmod 31 = 22 \quad 112 \bmod 31 = 19$$

to get the remainders

$$25, \quad 4, \quad 22, \quad 19.$$

- Convert these four numbers back to letters and you have the encoded message $Y\ D\ V\ S$.

Decoding Messages

- Now suppose you receive the scrambled message

$$Y\ D\ V\ S.$$

Decoding Messages

- Now suppose you receive the scrambled message

$$Y\ D\ V\ S.$$

- How can you decode this message to get the original message?

Decoding Messages

- Now suppose you receive the scrambled message

$$Y\ D\ V\ S.$$

- How can you decode this message to get the original message?
- The answer is surprisingly simple:

Decoding Messages

- Now suppose you receive the scrambled message

$$Y\ D\ V\ S.$$

- How can you decode this message to get the original message?
- The answer is surprisingly simple:
  - apply the same procedure as when encoding

Decoding Messages

- Now suppose you receive the scrambled message

$$Y\ D\ V\ S.$$

- How can you decode this message to get the original message?
- The answer is surprisingly simple:
  - apply the same procedure as when encoding
  - except you must use the decoding number d

Decoding Messages

- Now suppose you receive the scrambled message

$$Y\ D\ V\ S.$$

- How can you decode this message to get the original message?
- The answer is surprisingly simple:
  - apply the same procedure as when encoding
  - except you must use the decoding number d
  - that corresponds to the number e

Decoding Messages

- Now suppose you receive the scrambled message

$$Y\ D\ V\ S.$$

- How can you decode this message to get the original message?
- The answer is surprisingly simple:
  - apply the same procedure as when encoding
  - except you must use the decoding number d
  - that corresponds to the number e
  - used to encode the original message.

Decoding Messages

- Now suppose you receive the scrambled message

$$Y\ D\ V\ S.$$

- How can you decode this message to get the original message?
- The answer is surprisingly simple:
  - apply the same procedure as when encoding
  - except you must use the decoding number d
  - that corresponds to the number e
  - used to encode the original message.
- It turns out that the number $d = 9$ corresponds to the encoding number $e = 7$.

Decoding Messages

- To decode $Y\ D\ V\ S$, first convert the letters to numbers:

$$(Y, D, V, S) \rightarrow (25, 4, 22, 19).$$

Decoding Messages

- To decode $Y\ D\ V\ S$, first convert the letters to numbers:

$$(Y, D, V, S) \to (25, 4, 22, 19).$$

- Multiply each number by $d = 9$:

$$(225, 36, 198, 171).$$

Decoding Messages

- To decode $Y\ D\ V\ S$, first convert the letters to numbers:

$$(Y, D, V, S) \to (25, 4, 22, 19).$$

- Multiply each number by $d = 9$:

$$(225, 36, 198, 171).$$

- Reduce these four number on a 31-clock, using $225 \bmod 31 = 8$, etc., to obtain

$$(8, 5, 12, 16).$$

Decoding Messages

- To decode $Y\ D\ V\ S$, first convert the letters to numbers:

$$(Y, D, V, S) \to (25, 4, 22, 19).$$

- Multiply each number by $d = 9$:

$$(225, 36, 198, 171).$$

- Reduce these four number on a 31-clock, using $225 \bmod 31 = 8$, etc., to obtain

$$(8, 5, 12, 16).$$

- So our original message was

$$H\ E\ L\ P.$$

Two questions

(1) How do we find the decoding number d if we know the encoding number e?

Two questions

(1) How do we find the decoding number d if we know the encoding number e?

(2) Why does this work?

Two questions

(1) How do we find the decoding number d if we know the encoding number e?

(2) Why does this work?

Two questions

(1) How do we find the decoding number d if we know the encoding number e?

(2) Why does this work?

Finding d given e

- Solve the POW problem with the numbers

Finding d given e

- Solve the POW problem with the numbers
- $e = 7$ and $p = 31$.

Finding d given e

- Solve the POW problem with the numbers
- $e = 7$ and $p = 31$.
- Since $31 = 4 \times 7 + 3$, we have the reduction

Finding d given e

- Solve the POW problem with the numbers
- $e = 7$ and $p = 31$.
- Since $31 = 4 \times 7 + 3$, we have the reduction
- $(7, 31) \rightarrow (3, 7)$

Finding d given e

- Solve the POW problem with the numbers
- $e = 7$ and $p = 31$.
- Since $31 = 4 \times 7 + 3$, we have the reduction
- $(7, 31) \to (3, 7)$
- and we can easily solve POW with 3 and 7:

Finding d given e

- Solve the POW problem with the numbers
- $e = 7$ and $p = 31$.
- Since $31 = 4 \times 7 + 3$, we have the reduction
- $(7, 31) \rightarrow (3, 7)$
- and we can easily solve POW with 3 and 7:
- $7 - 2 \times 3 = 1$

Solving POW(7,31)

Working backwards, we have

$$1 = 7 - 2 \times 3$$

Solving POW(7,31)

Working backwards, we have

$1 = 7 - 2 \times 3$ solution for 3 and 7

Solving POW(7,31)

Working backwards, we have

$$1 = 7 - 2 \times 3 \qquad \text{solution for 3 and 7}$$
$$= 7 - 2 \times (31 - 4 \times 7)$$

Solving POW(7,31)

Working backwards, we have

$$1 = 7 - 2 \times 3 \qquad \text{solution for 3 and 7}$$

$$= 7 - 2 \times (31 - 4 \times 7) \qquad \text{sub } 3 = 31 - 4 \times 7$$

Solving POW(7,31)

Working backwards, we have

$$
\begin{aligned}
1 &= 7 - 2 \times 3 && \text{solution for 3 and 7} \\
&= 7 - 2 \times (31 - 4 \times 7) && \text{sub } 3 = 31 - 4 \times 7 \\
&= 7 - 2 \times 31 + 8 \times 7
\end{aligned}
$$

Solving POW(7,31)

Working backwards, we have

$$
\begin{aligned}
1 &= 7 - 2 \times 3 && \text{solution for 3 and 7} \\
&= 7 - 2 \times (31 - 4 \times 7) && \text{sub } 3 = 31 - 4 \times 7 \\
&= 7 - 2 \times 31 + 8 \times 7 && \text{expand the parentheses}
\end{aligned}
$$

Solving POW(7,31)

Working backwards, we have

$$
\begin{aligned}
1 &= 7 - 2 \times 3 && \text{solution for 3 and 7} \\
&= 7 - 2 \times (31 - 4 \times 7) && \text{sub } 3 = 31 - 4 \times 7 \\
&= 7 - 2 \times 31 + 8 \times 7 && \text{expand the parentheses} \\
&= 9 \times 7 - 2 \times 31
\end{aligned}
$$

Solving POW(7,31)

Working backwards, we have

$1 = 7 - 2 \times 3$	solution for 3 and 7
$= 7 - 2 \times (31 - 4 \times 7)$	sub $3 = 31 - 4 \times 7$
$= 7 - 2 \times 31 + 8 \times 7$	expand the parentheses
$= 9 \times 7 - 2 \times 31$	gather the 7's together

Solving POW(7,31)

Working backwards, we have

$$
\begin{aligned}
1 &= 7 - 2 \times 3 && \text{solution for 3 and 7} \\
&= 7 - 2 \times (31 - 4 \times 7) && \text{sub } 3 = 31 - 4 \times 7 \\
&= 7 - 2 \times 31 + 8 \times 7 && \text{expand the parentheses} \\
&= 9 \times 7 - 2 \times 31 && \text{gather the 7's together}
\end{aligned}
$$

The decoding number d is the 9 in this last equation.

Why does this work?

- The key equation is

$$1 = 9 \times 7 - 2 \times 31,$$

Why does this work?

- The key equation is

$$1 = 9 \times 7 - 2 \times 31,$$

- or equivalently,

$$de = 9 \times 7 = 1 + 2 \times 31.$$

Why does this work?

- The key equation is

$$1 = 9 \times 7 - 2 \times 31,$$

- or equivalently,

$$de = 9 \times 7 = 1 + 2 \times 31.$$

- Suppose we start with the letter ‘H’,

Why does this work?

- The key equation is

$$1 = 9 \times 7 - 2 \times 31,$$

- or equivalently,

$$de = 9 \times 7 = 1 + 2 \times 31.$$

- Suppose we start with the letter ‘H’,
- the first letter of our message.

Why does this work?

- The key equation is

$$1 = 9 \times 7 - 2 \times 31,$$

- or equivalently,

$$de = 9 \times 7 = 1 + 2 \times 31.$$

- Suppose we start with the letter ‘H’,
- the first letter of our message.
- Since the ‘H’ has value 8,

Why does this work?

- The key equation is

$$1 = 9 \times 7 - 2 \times 31,$$

- or equivalently,

$$de = 9 \times 7 = 1 + 2 \times 31.$$

- Suppose we start with the letter ‘H’,
- the first letter of our message.
- Since the ‘H’ has value 8,
- the encoding process multiplies 8 by e.

Why this works cont'd

The decoding process multiplies the result by d, giving

Why this works cont'd

The decoding process multiplies the result by d, giving

$$d(e8) =$$

Why this works cont'd

The decoding process multiplies the result by d, giving

$$d(e8) = (de)8 =$$

Why this works cont'd

The decoding process multiplies the result by d, giving

$$d(e8) = (de)8 = (1 + 2 \times 31)8 =$$

Why this works cont'd

The decoding process multiplies the result by d, giving

$$d(e8) = (de)8 = (1 + 2 \times 31)8 = 8 + 16 \times 31.$$

Why this works cont'd

The decoding process multiplies the result by d, giving

$$d(e8) = (de)8 = (1 + 2 \times 31)8 = 8 + 16 \times 31.$$

It is clear that this last number reduces to 8 mod 31.

Negative Catch

Question: What do you do if the value of d is negative?

- For example, if the encoding number is $e = 4$,

Negative Catch

Question: What do you do if the value of d is negative?

- For example, if the encoding number is $e = 4$,
- one solution to POW(4,31) is

$$3 \times 31 - 23 \times 4 = 1$$

Negative Catch

Question: What do you do if the value of d is negative?

- For example, if the encoding number is $e = 4$,
- one solution to POW(4,31) is

$$3 \times 31 - 23 \times 4 = 1$$

- Here the decoding number is $d = -23$

Negative Catch

Question: What do you do if the value of d is negative?

- For example, if the encoding number is $e = 4$,
- one solution to POW(4,31) is

$$3 \times 31 - 23 \times 4 = 1$$

- Here the decoding number is $d = -23$
- To make our decoding number be positive

Negative Catch

Question: What do you do if the value of d is negative?

- For example, if the encoding number is $e = 4$,
- one solution to POW(4,31) is

$$3 \times 31 - 23 \times 4 = 1$$

- Here the decoding number is $d = -23$
- To make our decoding number be positive
- simply convert $d = -23 \bmod 31$

Negative Catch

Question: What do you do if the value of d is negative?

- For example, if the encoding number is $e = 4$,
- one solution to POW(4,31) is

$$3 \times 31 - 23 \times 4 = 1$$

- Here the decoding number is $d = -23$
- To make our decoding number be positive
- simply convert $d = -23 \bmod 31 = 8$

Negative Catch

Question: What do you do if the value of d is negative?

- For example, if the encoding number is $e = 4$,
- one solution to POW(4,31) is

$$3 \times 31 - 23 \times 4 = 1$$

- Here the decoding number is $d = -23$
- To make our decoding number be positive
- simply convert $d = -23 \bmod 31 = 8$
- Note: We could have avoided this problem if we used as a solution to POW(4,31):

$$8 \times 4 - 1 \times 31 = 1$$

RSA

The state of the art encryption method, called RSA, uses a much larger clock size consisting of hundred of digits and uses exponentiation rather than multiplication.

RSA

The state of the art encryption method, called RSA, uses a much larger clock size consisting of hundred of digits and uses exponentiation rather than multiplication.

But the basic principle of RSA encryption is much the same as the code described here.