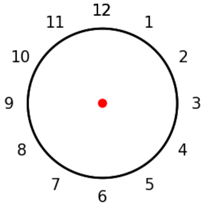
A Taste of Pi: Clocks, Set, and the Secret Math of Spies

Katherine E. Stange
SFU / PIMS-UBC

October 16, 2010

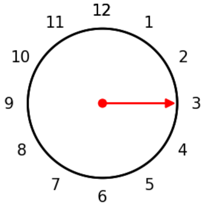
The Math of Clocks

Here is a picture of a clock.



The Math of Clocks

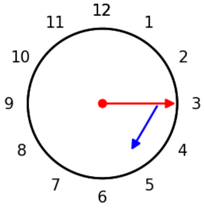
Here is a picture of a clock.



3 pm

The Math of Clocks

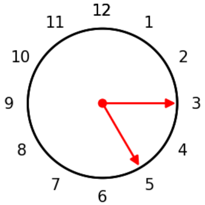
Here is a picture of a clock.



$$3\,\text{pm} + 2\,\text{hours} \quad =$$

The Math of Clocks

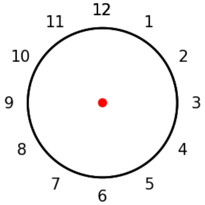
Here is a picture of a clock.



$$3\,\text{pm} + 2\,\text{hours} \quad = \quad 5\,\text{pm}$$

The Math of Clocks

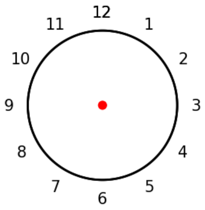
Here is a picture of a clock.



$$
\begin{aligned}
3\,\text{pm} + 2\,\text{hours} &= 5\,\text{pm} \\
3 + 2 &\equiv 5 \mod 12
\end{aligned}
$$

The Math of Clocks

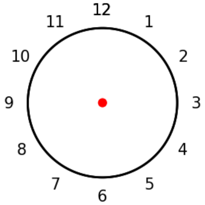
Here is a picture of a clock.



$$\begin{aligned} 3\,\text{pm} + 2\,\text{hours} &= 5\,\text{pm} \\ 3 + 2 &\equiv 5 \mod 12 \\ 2\,\text{pm} + 11\,\text{hours} &= \end{aligned}$$

The Math of Clocks

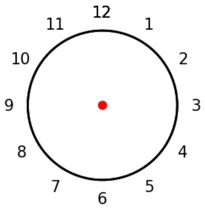
Here is a picture of a clock.



$$\begin{aligned} 3\,\text{pm} + 2\,\text{hours} &= 5\,\text{pm} \\ 3+2 &\equiv 5 \mod 12 \\ 2\,\text{pm} + 11\,\text{hours} &= 1\,\text{am} \end{aligned}$$

The Math of Clocks

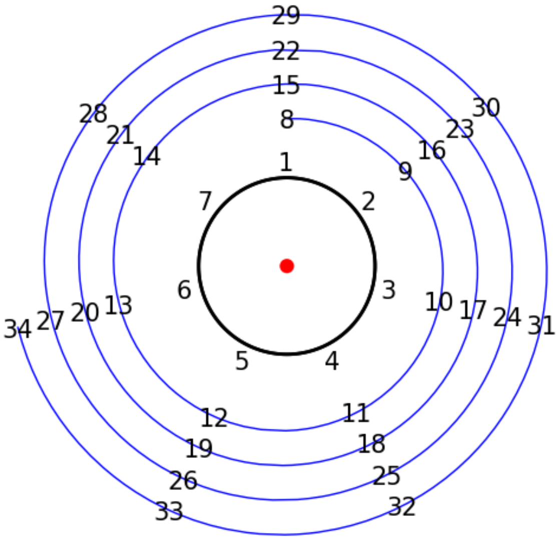
Here is a picture of a clock.



$$
\begin{aligned}
3\,\text{pm} + 2\,\text{hours} &= 5\,\text{pm} \\
3 + 2 &\equiv 5 \mod 12 \\
2\,\text{pm} + 11\,\text{hours} &= 1\,\text{am} \\
2 + 11 &\equiv 1 \mod 12
\end{aligned}
$$

The Math of Clocks

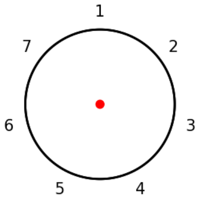
It's a little like rolling up a long line of the integers into a circle:



The Math of Clocks

We could have a clock with any number of hours on it.

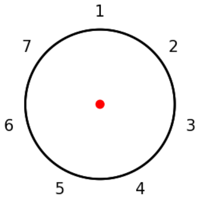
Here is a picture of a clock with
7 hours.



The Math of Clocks

We could have a clock with any number of hours on it.

Here is a picture of a clock with 7 hours.



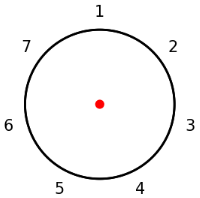
$$2 \text{ o'clock} + 11 \text{ hours} \quad =$$

The Math of Clocks

We could have a clock with any number of hours on it.

Here is a picture of a clock with 7 hours.

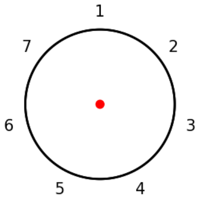
$$2\text{ o'clock} + 11\text{ hours} \quad = \quad 6\text{ o'clock}$$



The Math of Clocks

We could have a clock with any number of hours on it.

Here is a picture of a clock with 7 hours.

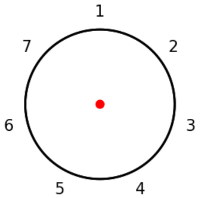


$$\begin{aligned} 2\text{ o'clock} + 11\text{ hours} &= 6\text{ o'clock} \\ 2 + 11 &\equiv 6 \mod 7 \end{aligned}$$

The Math of Clocks

We could have a clock with any number of hours on it.

Here is a picture of a clock with 7 hours.

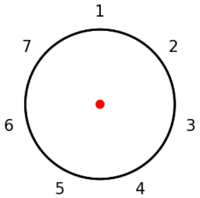


$$\begin{aligned} 2\,\text{o'clock} + 11\,\text{hours} &= 6\,\text{o'clock} \\ 2 + 11 &\equiv 6 \mod 7 \\ 1\,\text{o'clock} - 24\,\text{hours} &= \end{aligned}$$

The Math of Clocks

We could have a clock with any number of hours on it.

Here is a picture of a clock with 7 hours.

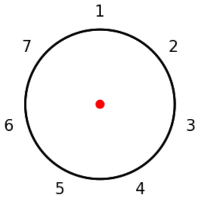


$$\begin{aligned} 2\text{ o'clock} + 11\text{ hours} &= 6\text{ o'clock} \\ 2 + 11 &\equiv 6 \mod 7 \\ 1\text{ o'clock} - 24\text{ hours} &= 5\text{ o'clock} \end{aligned}$$

The Math of Clocks

We could have a clock with any number of hours on it.

Here is a picture of a clock with 7 hours.

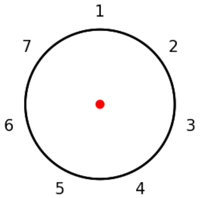


$$\begin{aligned} 2\text{ o'clock} + 11\text{ hours} &= 6\text{ o'clock} \\ 2 + 11 &\equiv 6 \mod 7 \\ 1\text{ o'clock} - 24\text{ hours} &= 5\text{ o'clock} \\ 1 - 24 &\equiv 5 \mod 7 \end{aligned}$$

The Math of Clocks

We could have a clock with any number of hours on it.

Here is a picture of a clock with 7 hours.

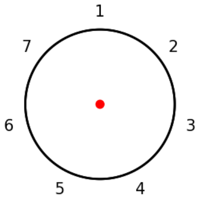


$$\begin{aligned}
2\,\text{o'clock} + 11\,\text{hours} &= 6\,\text{o'clock} \\
2 + 11 &\equiv 6 \mod 7 \\
1\,\text{o'clock} - 24\,\text{hours} &= 5\,\text{o'clock} \\
1 - 24 &\equiv 5 \mod 7 \\
2\,\text{o'clock} \times 4 &=
\end{aligned}$$

The Math of Clocks

We could have a clock with any number of hours on it.

Here is a picture of a clock with 7 hours.

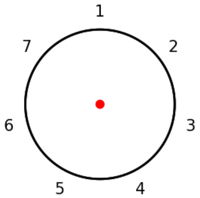


$$\begin{aligned}
2\,\text{o'clock} + 11\,\text{hours} &= 6\,\text{o'clock}\\
2 + 11 &\equiv 6 \mod 7\\
1\,\text{o'clock} - 24\,\text{hours} &= 5\,\text{o'clock}\\
1 - 24 &\equiv 5 \mod 7\\
2\,\text{o'clock} \times 4 &= 1\,\text{o'clock}
\end{aligned}$$

The Math of Clocks

We could have a clock with any number of hours on it.

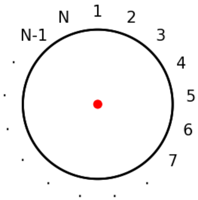
Here is a picture of a clock with 7 hours.



$$\begin{aligned}
2\text{ o'clock} + 11\text{ hours} &= 6\text{ o'clock} \\
2 + 11 &\equiv 6 \mod 7 \\
1\text{ o'clock} - 24\text{ hours} &= 5\text{ o'clock} \\
1 - 24 &\equiv 5 \mod 7 \\
2\text{ o'clock} \times 4 &= 1\text{ o'clock} \\
2 \times 4 &\equiv 1 \mod 7
\end{aligned}$$

We could label these with days of the week...

The Math of Clocks



We call the N-hour clock $\mathbb{Z}_N$, and it has N elements:

$$\mathbb{Z}_N = \{0, 1, 2, 3, \ldots, N-1\}$$

We can add, subtract and multiply elements of $\mathbb{Z}_N$ (and get back elements of $\mathbb{Z}_N$).

The Math of Clocks

- The math of clocks is called *Modular Arithmetic* and N is called the *modulus*.
- Two numbers A and B are the same “modulo N” if A and B differ by adding N some number of times.

The Math of Clocks

- The math of clocks is called *Modular Arithmetic* and N is called the *modulus*.
- Two numbers A and B are the same "modulo N" if A and B differ by adding N some number of times.
- We could say that a hamburger and a cheeseburger are the same modulo cheese.

The Math of Clocks

- The math of clocks is called *Modular Arithmetic* and N is called the *modulus*.
- Two numbers A and B are the same “modulo N” if A and B differ by adding N some number of times.
- We could say that a hamburger and a cheeseburger are the same modulo cheese.
- Some people say Gauss invented modular arithmetic, but humans have used it as long as we’ve had...
  - clocks
  - weeks
  - gears
  - money
  - ...
- It’s the beginning of the study of Number Theory.

The Math of Clocks

Let the festivities begin!

The Math of Clocks - Multiplication Tables

$\mathbb{Z}_2$	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

The Math of Clocks - Multiplication Tables

$\mathbb{Z}_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

The Math of Clocks - Multiplication Tables

$\mathbb{Z}_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The Math of Clocks - Multiplication Tables

$\mathbb{Z}_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

The Math of Clocks - Multiplication Tables

$\mathbb{Z}_8$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

The Math of Clocks - Multiplication Tables

$\mathbb{Z}_9$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

The Math of Clocks - Multiplication Tables

$\mathbb{Z}_{11}$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

The Math of Clocks

The Math of Clocks

1. When N is a prime number, then you can divide in $\mathbb{Z}_N$.

The Math of Clocks

1. When N is a prime number, then you can divide in $\mathbb{Z}_N$.
2. This makes $\mathbb{Z}_N$ a really great number system: it has $+$, $-$, $\times$ and $\div$.

The Math of Clocks

1. When N is a prime number, then you can divide in $\mathbb{Z}_N$.
2. This makes $\mathbb{Z}_N$ a really great number system: it has $+$, $-$, $\times$ and $\div$.
3. It's even better than the integers (there's no $1/2$ in the integers!).

The Math of Set

The graph of the line $y = x + 2$ in $\mathbb{Z}_5$:

2			X		
1		X			
0	X				
4					X
3				X	
	3	4	0	1	2

The Math of Set

The graph of the line $y = x + 2$ in $\mathbb{Z}_5$:

2			X		
1		X			
0	X				
4					X
3				X	
	3	4	0	1	2

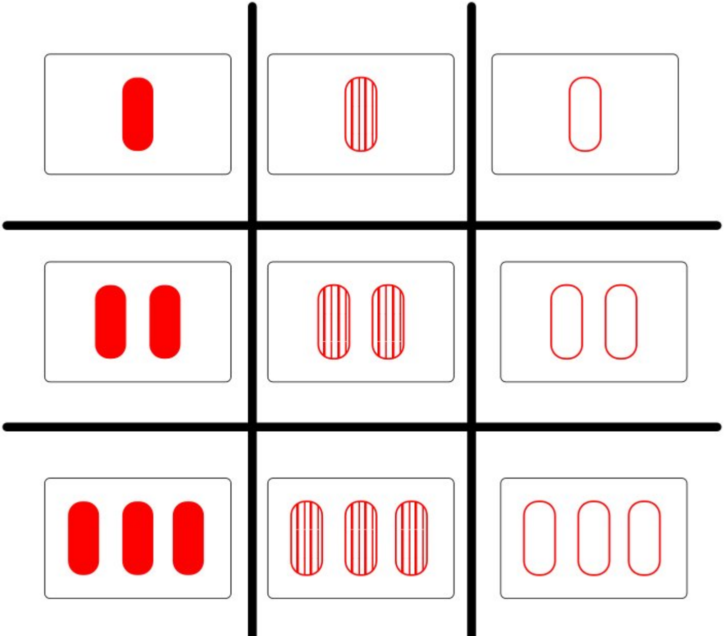
The graph is a little like Asteroids!

The Math of Set

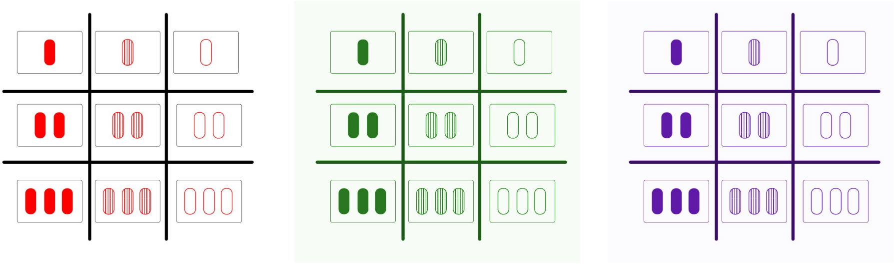
The graph of the line $y = 3x + 4$ in $\mathbb{Z}_5$:

2				X	
1		X			
0					X
4			X		
3	X				
	3	4	0	1	2

The Math of Set



The Math of Set



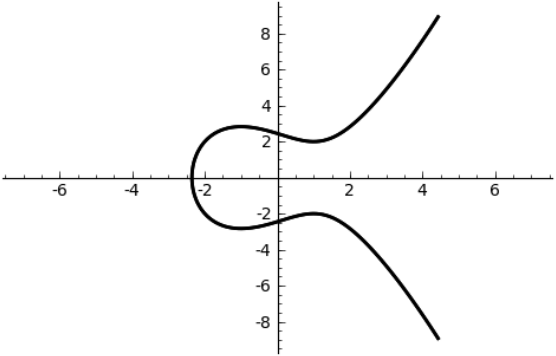
Set images due to Diane Maclagan and Ben Davis

The Math of Set

http://www.setgame.com/

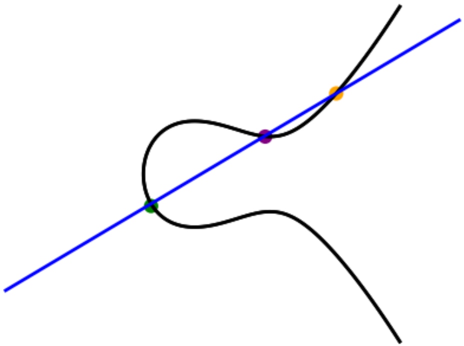
The Math of Spies

Here's the graph of $y^2 = x^3 - 3x + 6$ in the usual world (real numbers):



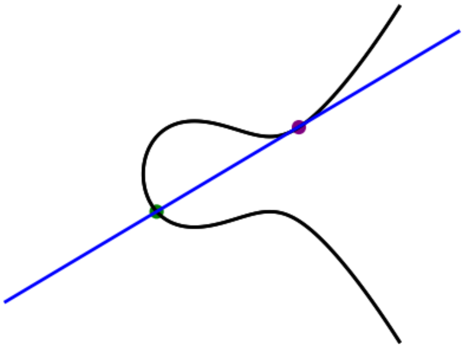
The Math of Spies

Adding two points to get another: $P + Q + R = O$.



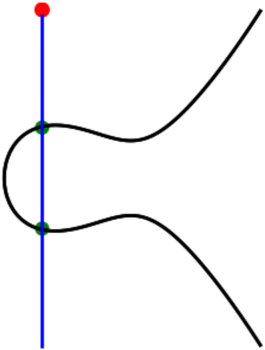
The Math of Spies

Adding a point and its negative: $P + Q + Q = O$.



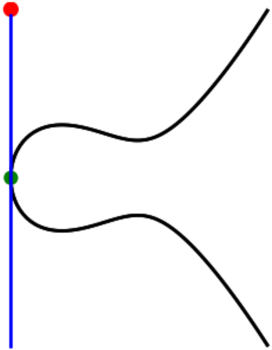
The Math of Spies

Adding a point and its negative: $P + -P = O$.



The Math of Spies

A point which adds with itself to zero: $P + P = O$.



The Math of Spies

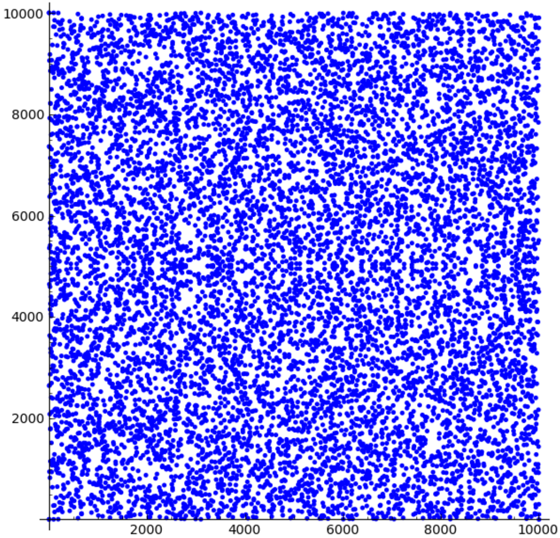
The graph of $y^2 = x^3 + 2x + 1$ in $\mathbb{Z}_5$:

2	X			X	
1			X		
0					
4			X		
3	X			X	
	3	4	0	1	2

This is called an "Elliptic Curve"

The Math of Spies

Here's an elliptic curve in $\mathbb{Z}_{10007}$.



The Math of Spies

2	A			C	
1			B		
0					
4			-B		
3	-A			-C	
	3	4	0	1	2

The Math of Spies

2	A			C	
1		X	B		
0					X
4			-B		
3	-A			-C	
	3	4	0	1	2

The Math of Spies

2	A			C	
1		X	B		
0					X
4			-B		
3	-A			-C	
	3	4	0	1	2

$$-A + -B + C = 0$$

The Math of Spies

2	A			C	
1		X	B		
0					X
4			-B		
3	-A			-C	
	3	4	0	1	2

$$-A + -B + C = 0$$
$$A + B = C$$

The Math of Spies

2	A			C	
1			B		
0					
4			-B		
3	-A			-C	
	3	4	0	1	2

The Math of Spies

2	A			C	
1			B		X
0				X	
4			-B		
3	-A	X		-C	
	3	4	0	1	2

The Math of Spies

2	A			C	
1			B		X
0				X	
4			-B		
3	-A	X		-C	
	3	4	0	1	2

$$A + A + -B = 0$$

The Math of Spies

2	A			C	
1			B		X
0				X	
4			-B		
3	-A	X		-C	
	3	4	0	1	2

$$A + A + -B = 0$$
$$A + A = B$$

The Math of Spies

2	A			C	
1			2A		
0					
4			-2A		
3	-A			-C	
	3	4	0	1	2

$A + A + -B = 0$
$A + A = B$
So $B = 2A$

The Math of Spies

2	A			C	
1			2A		
0					
4			-2A		
3	-A			-C	
	3	4	0	1	2

$A + A + -B = 0$
$A + A = B$
So $B = 2A$
From last slide:
$C = A + B =$
$A + 2A = 3A$

The Math of Spies

2	A			3A	
1			2A		
0					
4			-2A		
3	-A			-3A	
	3	4	0	1	2

$A + A + -B = 0$
$A + A = B$
So $B = 2A$
From last slide:
$C = A + B =$
$A + 2A = 3A$
So $C = 3A$

The Math of Spies

2	A			3A	
1			2A		
0					
4			5A		
3	6A			4A	
	3	4	0	1	2

With a little more work, we find out that $-3A = 4A$, $-2A = 5A$ and $-A = 6A$, and finally that $7A = O$.

The Math of Spies - Elliptic Curve Addition Table

E	O	A	2A	3A	4A	5A	6A
O	O	A	2A	3A	4A	5A	6A
A	A	2A	3A	4A	5A	6A	O
2A	2A	3A	4A	5A	6A	O	A
3A	3A	4A	5A	6A	O	A	2A
4A	4A	5A	6A	O	A	2A	3A
5A	5A	6A	O	A	2A	3A	4A
6A	6A	O	A	2A	3A	4A	5A

The Math of Spies - Modular Arithmetic Addition Table

$\mathbb{Z}_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

The Math of Spies

- Suppose I gave you two numbers, $P = 9$ and $Q = 45$ and I said,

The Math of Spies

- Suppose I gave you two numbers, $P = 9$ and $Q = 45$ and I said,

“How many times need I add P to itself to get Q?”

The Math of Spies

- Suppose I gave you two numbers, $P = 9$ and $Q = 45$ and I said,

  "How many times need I add P to itself to get Q?"

- You would divide 45 by 9 and get the answer: 5. Division is fairly easy for integers!

The Math of Spies

- Suppose I gave you two numbers, $P = 9$ and $Q = 45$ and I said,

"How many times need I add P to itself to get Q?"

- You would divide 45 by 9 and get the answer: 5. Division is fairly easy for integers!
- It takes more time as the numbers get bigger, but the time it takes grows with the number of digits of the numbers.

The Math of Spies

- Suppose I gave you two numbers modulo 5, $P = 2$ and $Q = 3$ and I said,

The Math of Spies

- Suppose I gave you two numbers modulo 5, $P = 2$ and $Q = 3$ and I said,

  "How many times need I add P to itself to get Q?"

The Math of Spies

- Suppose I gave you two numbers modulo 5, $P = 2$ and $Q = 3$ and I said,

  "How many times need I add P to itself to get Q?"

- This is trickier. You could complete a multiplication table and look in it to search for the answer. It turns out there are faster ways.

The Math of Spies

- Suppose I gave you two numbers modulo 5, $P = 2$ and $Q = 3$ and I said,

  "How many times need I add P to itself to get Q?"

- This is trickier. You could complete a multiplication table and look in it to search for the answer. It turns out there are faster ways.
- The smartest algorithms (can you come up with one?), are about as fast as division for the integers. The time it takes grows with the number of digits of the modulus.

The Math of Spies

2	P			X	
1			X		
0					
4			Q		
3	X			X	
	3	4	0	1	2

- Suppose I gave you the points P and Q and I said

  "How many times need I add P to itself to get Q?"

The Math of Spies

2	P			X	
1			X		
0					
4			Q		
3	X			X	
	3	4	0	1	2

- Suppose I gave you the points P and Q and I said

  "How many times need I add P to itself to get Q?"

- You might remember that we found $Q = 5P$ from our multiplication table.

The Math of Spies

2	P			X	
1			X		
0					
4			Q		
3	X			X	
	3	4	0	1	2

- Suppose I gave you the points P and Q and I said

  "How many times need I add P to itself to get Q?"

- You might remember that we found $Q = 5P$ from our multiplication table.
- But it was a lot of work! Is there an easy way to do this?

The Math of Spies

No one knows any efficient way to solve this problem!!

The Math of Spies

No one knows any efficient way to solve this problem!!

The time taken by good algorithms grows with about the square root of the size of the modulus.

The Math of Spies

Modern cryptography is based on mathematical operations that are easy to do and hard to undo.

Example:

The Math of Spies

Modern cryptography is based on mathematical operations that are easy to do and hard to undo.
Example:

- Getting pregnant.

The Math of Spies

Modern cryptography is based on mathematical operations that are easy to do and hard to undo.
Example:

- Getting pregnant.
- Multiplying numbers is easy, but factoring them is hard.

The Math of Spies

Modern cryptography is based on mathematical operations that are easy to do and hard to undo.
Example:

- Getting pregnant.
- Multiplying numbers is easy, but factoring them is hard.
- On an elliptic curve, adding a point P to itself many times is easy. Figuring out how many times it was added (if you weren't watching) is hard. This is the elliptic curve discrete logarithm problem.

The Math of Spies

Alice and Bob want to share a secret.

The Math of Spies

Alice and Bob want to share a secret.

A point P on an elliptic curve is general knowledge.

	Alice	Bob

The Math of Spies

Alice and Bob want to share a secret.

A point P on an elliptic curve is general knowledge.

	Alice	Bob
secret	a	b

The Math of Spies

Alice and Bob want to share a secret.

A point P on an elliptic curve is general knowledge.

	Alice	Bob
secret	a	b
public	aP	bP

The Math of Spies

Alice and Bob want to share a secret.

A point P on an elliptic curve is general knowledge.

	Alice	Bob
secret	a	b
public	aP	bP

Alice and Bob can both compute abP.

The Math of Spies

Alice and Bob want to share a secret.

A point P on an elliptic curve is general knowledge.

	Alice	Bob
secret	a	b
public	aP	bP

Alice and Bob can both compute abP.

No one else can compute it!

The Math of Spies

Here the size of the modulus N we use for this algorithm in your web browser, when you log onto a secure site:

$N = 686479766013060971498190079908139321726943530014330540939446345918554318339765605212255964066145455497729631139148085803712198799971664381257402829111505715 1$

001433054093944634591855431833976560521225596406 6
145455497729631139148085803712198799971664381257 4
028291115057151

The Math of Spies

- The hard problem of factoring is used for cryptography called RSA.

The Math of Spies

- The hard problem of factoring is used for cryptography called RSA.
- The elliptic curve discrete logarithm problem is used for elliptic curve cryptography (ECC).

The Math of Spies

- The hard problem of factoring is used for cryptography called RSA.
- The elliptic curve discrete logarithm problem is used for elliptic curve cryptography (ECC).
- Together, these two hard problems are used for pretty nearly all the cryptography in the modern world: your bank, your cell phone, your computer.

The Math of Spies

- The hard problem of factoring is used for cryptography called RSA.
- The elliptic curve discrete logarithm problem is used for elliptic curve cryptography (ECC).
- Together, these two hard problems are used for pretty nearly all the cryptography in the modern world: your bank, your cell phone, your computer.
- (No one has come up with a security method based on pregnancy.)

The Math of Spies

- The hard problem of factoring is used for cryptography called RSA.
- The elliptic curve discrete logarithm problem is used for elliptic curve cryptography (ECC).
- Together, these two hard problems are used for pretty nearly all the cryptography in the modern world: your bank, your cell phone, your computer.
- (No one has come up with a security method based on pregnancy.)
- If you can come up with a fast algorithm for these hard problems,

The Math of Spies

- The hard problem of factoring is used for cryptography called RSA.
- The elliptic curve discrete logarithm problem is used for elliptic curve cryptography (ECC).
- Together, these two hard problems are used for pretty nearly all the cryptography in the modern world: your bank, your cell phone, your computer.
- (No one has come up with a security method based on pregnancy.)
- If you can come up with a fast algorithm for these hard problems, you would immediately become hugely famous,

The Math of Spies

- The hard problem of factoring is used for cryptography called RSA.
- The elliptic curve discrete logarithm problem is used for elliptic curve cryptography (ECC).
- Together, these two hard problems are used for pretty nearly all the cryptography in the modern world: your bank, your cell phone, your computer.
- (No one has come up with a security method based on pregnancy.)
- If you can come up with a fast algorithm for these hard problems, you would immediately become hugely famous, you would get job offers from every government in the world,

The Math of Spies

- The hard problem of factoring is used for cryptography called RSA.
- The elliptic curve discrete logarithm problem is used for elliptic curve cryptography (ECC).
- Together, these two hard problems are used for pretty nearly all the cryptography in the modern world: your bank, your cell phone, your computer.
- (No one has come up with a security method based on pregnancy.)
- If you can come up with a fast algorithm for these hard problems, you would immediately become hugely famous, you would get job offers from every government in the world, and would get invited on Oprah.

Thank you!

- Thanks to SFU, Veselin Jungic, Malgorzata Dubiel and Nadia Nosrati, and Jonathan Wise.
- And to you! Feel free to email me anytime (email on my website).