BILL
RECORD THIS
LECTURE

Affine and Quadratic Ciphers

The Affine Ciphers

Affine Cipher

Recall: Shift cipher with shift $s \in \{0, \ldots, 25\}$.

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions.

Def The Affine cipher with $a, b \in \{0, \ldots, 25\}$:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$.

Affine Cipher

Recall: Shift cipher with shift $s \in \{0, \dots, 25\}$.

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions.

Def The Affine cipher with $a, b \in \{0, \dots, 25\}$:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$.

Does this work? Vote YES or NO or OTHER.

Affine Cipher

Recall: Shift cipher with shift $s \in \{0, \ldots, 25\}$.

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions.

Def The Affine cipher with $a, b \in \{0, \ldots, 25\}$:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$.

Does this work? Vote YES or NO or OTHER. Answer: OTHER

Affine Cipher

Recall: Shift cipher with shift $s \in \{0, \ldots, 25\}$.

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions.

Def The Affine cipher with $a, b \in \{0, \ldots, 25\}$:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$.

Does this work? Vote YES or NO or OTHER. Answer: OTHER
$2x + 1$ does not work: 0 and 13 both map to 1.

Affine Cipher

Recall: Shift cipher with shift $s \in \{0, \ldots, 25\}$.

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions.

Def The Affine cipher with $a, b \in \{0, \ldots, 25\}$:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$.

Does this work? Vote YES or NO or OTHER. Answer: OTHER
$2x + 1$ does not work: 0 and 13 both map to 1.
Need the map to be a bijection so it will have an inverse.

Affine Cipher

Recall: Shift cipher with shift $s \in \{0, \ldots, 25\}$.

1. Encrypt via $x \rightarrow x + s \pmod{26}$.
2. Decrypt via $x \rightarrow x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions.

Def The Affine cipher with $a, b \in \{0, \ldots, 25\}$:

1. Encrypt via $x \rightarrow ax + b \pmod{26}$.
2. Decrypt via $x \rightarrow a^{-1}(x - b) \pmod{26}$.

Does this work? Vote YES or NO or OTHER. Answer: OTHER
$2x + 1$ does not work: 0 and 13 both map to 1.
Need the map to be a bijection so it will have an inverse.

Condition on a, b so that $x \rightarrow ax + b$ is a bij: a rel prime to 26.
Condition on a, b so that a has an inv mod 26: a rel prime to 26.

Affine Cipher

Recall: Shift cipher with shift $s \in \{0, \ldots, 25\}$.

1. Encrypt via $x \to x + s \pmod{26}$.
2. Decrypt via $x \to x - s \pmod{26}$.

We replace $x + s$ with more elaborate functions.

Def The Affine cipher with $a, b \in \{0, \ldots, 25\}$:

1. Encrypt via $x \to ax + b \pmod{26}$.
2. Decrypt via $x \to a^{-1}(x - b) \pmod{26}$.

Does this work? Vote YES or NO or OTHER. Answer: OTHER
$2x + 1$ does not work: 0 and 13 both map to 1.
Need the map to be a bijection so it will have an inverse.

Condition on a, b so that $x \to ax + b$ is a bij: a rel prime to 26.
Condition on a, b so that a has an inv mod 26: a rel prime to 26.
This is achieved by making a **relatively prime** to 26.
Note Also $a \in \{1, \ldots, 25\}$ and $b \in \{0, \ldots, 25\}$. We will not mention this again.

Shift vs Affine

Shift: Key space is size 26.

Affine: Key space is $\{1,3,5,7,9,11,15,17,19,21,23,25\} \times \{0,\ldots,25\}$ which has $12 \times 26 = 312$ elements.

In an Earlier Era Affine would be harder to crack than Shift.

Shift vs Affine

Shift: Key space is size 26.

Affine: Key space is $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \times \{0, \ldots, 25\}$ which has $12 \times 26 = 312$ elements.

In an Earlier Era Affine would be harder to crack than Shift.

Today They are both easy to crack.

Shift vs Affine

Shift: Key space is size 26.

Affine: Key space is $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \times \{0, \ldots, 25\}$ which has $12 \times 26 = 312$ elements.

In an Earlier Era Affine would be harder to crack than Shift.

Today They are both easy to crack.

Both Need: The **Is-English** algorithm. Reading through 312 transcripts to see which one **looks like English** would take A LOT of time!

Key Length of Shift and Affine Ciphers

Let's look at the **keys** for Shift and Affine.

1. Shift cipher key in $\{0, \ldots, 25\}$. 5 bits.
2. Affine cipher Key in $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \times \{0, \ldots, 25\}$. 312 keys, need 9 bits.

Affine Cipher: Need to Know Inverses Mod m

If Alice and Bob use the Affine Cipher with alphabet of size m:

Affine Cipher: Need to Know Inverses Mod m

If Alice and Bob use the Affine Cipher with alphabet of size m:

1. Alice picks a, b and must make sure that a is rel prime to m.

Affine Cipher: Need to Know Inverses Mod m

If Alice and Bob use the Affine Cipher with alphabet of size m:

1. Alice picks a, b and must make sure that a is rel prime to m.
2. Bob must compute the inverse of a mod m in order to decode.

Affine Cipher: Need to Know Inverses Mod m

If Alice and Bob use the Affine Cipher with alphabet of size m:

1. Alice picks a, b and must make sure that a is rel prime to m.
2. Bob must compute the inverse of a mod m in order to decode.
3. If Alice wants to also get messages and decode them, she also has to compute the inverse of a mod m in order to decode.

Examples of Numbers Rel Prime to $|\Sigma|$

If $\Sigma = \{a, \ldots, z\}$ (size 26) then, as we saw, the set is

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \text{ 12 possibilities}$$

Examples of Numbers Rel Prime to $|\Sigma|$

If $\Sigma = \{a, \ldots, z\}$ (size 26) then, as we saw, the set is

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \text{ 12 possibilities}$$

If $\Sigma = \{a, \ldots, z, 0, \ldots, 9\}$ (size 36) then, as we saw, the set is

$$\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} \text{ 12 possibilities}$$

Examples of Numbers Rel Prime to $|\Sigma|$

If $\Sigma = \{a, \ldots, z\}$ (size 26) then, as we saw, the set is

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \text{ 12 possibilities}$$

If $\Sigma = \{a, \ldots, z, 0, \ldots, 9\}$ (size 36) then, as we saw, the set is

$$\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} \text{ 12 possibilities}$$

If $\Sigma = \{a, \ldots, z, 0, \ldots, 9, \#\}$ (size 37) then, as we saw, the set is

$$\{1, \ldots, 36\} \text{ 36 possibilities}$$

Examples of Numbers Rel Prime to $|\Sigma|$

If $\Sigma = \{a, \ldots, z\}$ (size 26) then, as we saw, the set is

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \text{ 12 possibilities}$$

If $\Sigma = \{a, \ldots, z, 0, \ldots, 9\}$ (size 36) then, as we saw, the set is

$$\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} \text{ 12 possibilities}$$

If $\Sigma = \{a, \ldots, z, 0, \ldots, 9, \#\}$ (size 37) then, as we saw, the set is

$$\{1, \ldots, 36\} \text{ 36 possibilities}$$

If given m, want to know how many elements in $\{1, \ldots, m-1\}$ are relatively prime to m.

Examples of Numbers Rel Prime to $|\Sigma|$

If $\Sigma = \{a, \ldots, z\}$ (size 26) then, as we saw, the set is

$$\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\} \text{ 12 possibilities}$$

If $\Sigma = \{a, \ldots, z, 0, \ldots, 9\}$ (size 36) then, as we saw, the set is

$$\{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\} \text{ 12 possibilities}$$

If $\Sigma = \{a, \ldots, z, 0, \ldots, 9, \#\}$ (size 37) then, as we saw, the set is

$$\{1, \ldots, 36\} \text{ 36 possibilities}$$

If given m, want to know how many elements in $\{1, \ldots, m-1\}$ are relatively prime to m.
Will be on HW.

Finding Inverse Mod n

The Most Used Algorithm In Crypto!

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.
There is a fast algorithm for this problem.

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.
There is a fast algorithm for this problem.
This algorithm is used a lot:

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.
There is a fast algorithm for this problem.
This algorithm is used a lot:

1. Affine cipher over alphabet of size n, need to know if a has an inverse, and if so, what it is.

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.
There is a fast algorithm for this problem.
This algorithm is used a lot:

1. Affine cipher over alphabet of size n, need to know if a has an inverse, and if so, what it is.
2. (Later) Cracking psuedo-random ciphers.

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.
There is a fast algorithm for this problem.
This algorithm is used a lot:

1. Affine cipher over alphabet of size n, need to know if a has an inverse, and if so, what it is.
2. (Later) Cracking psuedo-random ciphers.
3. (Later) Implementing RSA.

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.
There is a fast algorithm for this problem.
This algorithm is used a lot:

1. Affine cipher over alphabet of size n, need to know if a has an inverse, and if so, what it is.
2. (Later) Cracking psuedo-random ciphers.
3. (Later) Implementing RSA.
4. (Later) Cracking RSA.

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.
There is a fast algorithm for this problem.
This algorithm is used a lot:

1. Affine cipher over alphabet of size n, need to know if a has an inverse, and if so, what it is.
2. (Later) Cracking psuedo-random ciphers.
3. (Later) Implementing RSA.
4. (Later) Cracking RSA.
5. (Later) Factoring Algorithms.

The Most Used Algorithm In Crypto!

Finding Inverses Given a, find $a^{-1} \pmod{n}$.
There is a fast algorithm for this problem.
This algorithm is used a lot:

1. Affine cipher over alphabet of size n, need to know if a has an inverse, and if so, what it is.
2. (Later) Cracking psuedo-random ciphers.
3. (Later) Implementing RSA.
4. (Later) Cracking RSA.
5. (Later) Factoring Algorithms.
6. Many Many Others!

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.
Examples
$\mathrm{GCD}(10, 15) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.
Examples
$\mathrm{GCD}(10, 15) =$5

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m,n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10,15) =$5
$\mathrm{GCD}(11,15) =$1
$\mathrm{GCD}(12,15) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) = 5$
$\mathrm{GCD}(11, 15) = 1$
$\mathrm{GCD}(12, 15) = 3$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1
$\mathrm{GCD}(12, 15) =$3
$\mathrm{GCD}(13, 15) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.

$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) = 5$

$\mathrm{GCD}(11, 15) = 1$

$\mathrm{GCD}(12, 15) = 3$

$\mathrm{GCD}(13, 15) = 1$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1
$\mathrm{GCD}(12, 15) =$3
$\mathrm{GCD}(13, 15) =$1
$\mathrm{GCD}(14, 15) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) = 5$
$\mathrm{GCD}(11, 15) = 1$
$\mathrm{GCD}(12, 15) = 3$
$\mathrm{GCD}(13, 15) = 1$
$\mathrm{GCD}(14, 15) = 1$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1
$\mathrm{GCD}(12, 15) =$3
$\mathrm{GCD}(13, 15) =$1
$\mathrm{GCD}(14, 15) =$1
$\mathrm{GCD}(15, 15) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1
$\mathrm{GCD}(12, 15) =$3
$\mathrm{GCD}(13, 15) =$1
$\mathrm{GCD}(14, 15) =$1
$\mathrm{GCD}(15, 15) =$15

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1
$\mathrm{GCD}(12, 15) =$3
$\mathrm{GCD}(13, 15) =$1
$\mathrm{GCD}(14, 15) =$1
$\mathrm{GCD}(15, 15) =$15
$\mathrm{GCD}(15, 24) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.
Examples
$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1
$\mathrm{GCD}(12, 15) =$3
$\mathrm{GCD}(13, 15) =$1
$\mathrm{GCD}(14, 15) =$1
$\mathrm{GCD}(15, 15) =$15
$\mathrm{GCD}(15, 24) =$3

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1
$\mathrm{GCD}(12, 15) =$3
$\mathrm{GCD}(13, 15) =$1
$\mathrm{GCD}(14, 15) =$1
$\mathrm{GCD}(15, 15) =$15
$\mathrm{GCD}(15, 24) =$3
$\mathrm{GCD}(15, 25) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) = 5$
$\mathrm{GCD}(11, 15) = 1$
$\mathrm{GCD}(12, 15) = 3$
$\mathrm{GCD}(13, 15) = 1$
$\mathrm{GCD}(14, 15) = 1$
$\mathrm{GCD}(15, 15) = 15$
$\mathrm{GCD}(15, 24) = 3$
$\mathrm{GCD}(15, 25) = 5$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) = 5$
$\mathrm{GCD}(11, 15) = 1$
$\mathrm{GCD}(12, 15) = 3$
$\mathrm{GCD}(13, 15) = 1$
$\mathrm{GCD}(14, 15) = 1$
$\mathrm{GCD}(15, 15) = 15$
$\mathrm{GCD}(15, 24) = 3$
$\mathrm{GCD}(15, 25) = 5$
$\mathrm{GCD}(15, 30) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) = 5$
$\mathrm{GCD}(11, 15) = 1$
$\mathrm{GCD}(12, 15) = 3$
$\mathrm{GCD}(13, 15) = 1$
$\mathrm{GCD}(14, 15) = 1$
$\mathrm{GCD}(15, 15) = 15$
$\mathrm{GCD}(15, 24) = 3$
$\mathrm{GCD}(15, 25) = 5$
$\mathrm{GCD}(15, 30) = 15$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) =$5
$\mathrm{GCD}(11, 15) =$1
$\mathrm{GCD}(12, 15) =$3
$\mathrm{GCD}(13, 15) =$1
$\mathrm{GCD}(14, 15) =$1
$\mathrm{GCD}(15, 15) =$15
$\mathrm{GCD}(15, 24) =$3
$\mathrm{GCD}(15, 25) =$5
$\mathrm{GCD}(15, 30) =$15
$\mathrm{GCD}(15, 0) =$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) = 5$
$\mathrm{GCD}(11, 15) = 1$
$\mathrm{GCD}(12, 15) = 3$
$\mathrm{GCD}(13, 15) = 1$
$\mathrm{GCD}(14, 15) = 1$
$\mathrm{GCD}(15, 15) = 15$
$\mathrm{GCD}(15, 24) = 3$
$\mathrm{GCD}(15, 25) = 5$
$\mathrm{GCD}(15, 30) = 15$
$\mathrm{GCD}(15, 0) = 15$

Greatest Common Divisor (GCD)

We first need to look at GCD.
$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.

Examples

$\mathrm{GCD}(10, 15) = 5$
$\mathrm{GCD}(11, 15) = 1$
$\mathrm{GCD}(12, 15) = 3$
$\mathrm{GCD}(13, 15) = 1$
$\mathrm{GCD}(14, 15) = 1$
$\mathrm{GCD}(15, 15) = 15$
$\mathrm{GCD}(15, 24) = 3$
$\mathrm{GCD}(15, 25) = 5$
$\mathrm{GCD}(15, 30) = 15$
$\mathrm{GCD}(15, 0) = 15$ (we will discuss $\mathrm{GCD}(a, 0) = a$ later)

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192

IFF

d is largest divisor of 192 and $404 - 192 = 212$.

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) =$

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192, 192) =$

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192, 192) = \mathrm{GCD}(212, 192)$
$=$

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192, 192) = \mathrm{GCD}(212, 192)$
$= \mathrm{GCD}(212 - 192, 192) =$

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192, 192) = \mathrm{GCD}(212, 192)$
$= \mathrm{GCD}(212 - 192, 192) = \mathrm{GCD}(20, 192)$.

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192, 192) = \mathrm{GCD}(212, 192)$
$= \mathrm{GCD}(212 - 192, 192) = \mathrm{GCD}(20, 192)$.
Could keep going, but will be subtracting 20's for a while.

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192, 192) = \mathrm{GCD}(212, 192)$
$= \mathrm{GCD}(212 - 192, 192) = \mathrm{GCD}(20, 192)$.
Could keep going, but will be subtracting 20's for a while.

Idea: Subtract LOTS of 20's.

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192, 192) = \mathrm{GCD}(212, 192)$
$= \mathrm{GCD}(212 - 192, 192) = \mathrm{GCD}(20, 192)$.
Could keep going, but will be subtracting 20's for a while.

Idea: Subtract LOTS of 20's. Largest $x : 192 - 20x \geq 0$, $x = 9$.

GCD(404,192) The Long Way

d is largest divisor of **both** 404 and 192
IFF
d is largest divisor of 192 and $404 - 192 = 212$.
Hence GCD(404,192)=GCD(192,404-192)=GCD(192,212).

d is largest divisor of **both** 212 and 192
IFF
d is largest divisor of 212 and $212 - 192 = 20$.
Hence GCD(212,192)=GCD(212-192,192)=GCD(20,192).

Idea: Keep subtracting smaller from larger:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192, 192) = \mathrm{GCD}(212, 192)$
$= \mathrm{GCD}(212 - 192, 192) = \mathrm{GCD}(20, 192)$.
Could keep going, but will be subtracting 20's for a while.

Idea: Subtract LOTS of 20's. Largest $x : 192 - 20x \geq 0$, $x = 9$.
$= \mathrm{GCD}(20, 192 - 20 \times 9 = 12) = \mathrm{GCD}(20 - 12, 12) = \mathrm{GCD}(8, 12)$
$= \mathrm{GCD}(8, 12 - 8 = 4) = \mathrm{GCD}(8 - 2 \times 4, 4) = \mathrm{GCD}(0, 4) = 4$.

GCD(404,192) The Short Way and More Info

$$404 = 2 \times 192 + 20$$

GCD(404,192) The Short Way and More Info

$$404 = 2 \times 192 + 20$$
$$192 = 9 \times 20 + 12$$

GCD(404,192) The Short Way and More Info

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$

GCD(404,192) The Short Way and More Info

$$404 = 2 \times 192 + 20$$
$$192 = 9 \times 20 + 12$$
$$20 = 1 \times 12 + 8$$
$$12 = 1 \times 8 + 4$$

GCD(404,192) The Short Way and More Info

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + 0$ STOP HERE and go back one: 4 is the GCD.

GCD(404,192) The Short Way and More Info

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + 0$ STOP HERE and go back one: 4 is the GCD.

Can use this to write 4 as a combination of 404 and 192

GCD(404,192) The Short Way and More Info

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + 0$ STOP HERE and go back one: 4 is the GCD.
Can use this to write 4 as a combination of 404 and 192
Write 4 as a combo of 12's and 8's:
$4 = 12 - 1 \times 8$

GCD(404,192) The Short Way and More Info

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + 0$ STOP HERE and go back one: 4 is the GCD.
Can use this to write 4 as a combination of 404 and 192
Write 4 as a combo of 12's and 8's:
$4 = 12 - 1 \times 8$
Write 8 as a combo of 20's and 12's:
$4 = 12 - 1 \times (20 - 12) = 2 \times 12 - 1 \times 20$

GCD(404,192) The Short Way and More Info

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + 0$ STOP HERE and go back one: 4 is the GCD.

Can use this to write 4 as a combination of 404 and 192

Write 4 as a combo of 12's and 8's:
$4 = 12 - 1 \times 8$
Write 8 as a combo of 20's and 12's:
$4 = 12 - 1 \times (20 - 12) = 2 \times 12 - 1 \times 20$
Write 12 as combo of 192's and 20's:
$4 = 2 \times (192 - 9 \times 20) - 1 \times 20 = 2 \times 192 - 19 \times 20$

GCD(404,192) The Short Way and More Info

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + 0$ STOP HERE and go back one: 4 is the GCD.

Can use this to write 4 as a combination of 404 and 192

Write 4 as a combo of 12's and 8's:
$4 = 12 - 1 \times 8$
Write 8 as a combo of 20's and 12's:
$4 = 12 - 1 \times (20 - 12) = 2 \times 12 - 1 \times 20$
Write 12 as combo of 192's and 20's:
$4 = 2 \times (192 - 9 \times 20) - 1 \times 20 = 2 \times 192 - 19 \times 20$
Write 20 as a combo of 404 and 192:
$4 = 2 \times 192 - 19 \times (404 - 2 \times 192) = 40 \times 192 - 19 \times 404$

Upshot: $\mathrm{GCD}(m, n)$ is a combo of m and n

A More Interesting Case: GCD(38,101)

$101 = 2 \times 38 + 25$

A More Interesting Case: GCD(38,101)

$$101 = 2 \times 38 + 25$$
$$38 = 1 \times 25 + 13$$

A More Interesting Case: GCD(38,101)

$$101 = 2 \times 38 + 25$$
$$38 = 1 \times 25 + 13$$
$$25 = 1 \times 13 + 12$$

A More Interesting Case: GCD(38,101)

$$101 = 2 \times 38 + 25$$
$$38 = 1 \times 25 + 13$$
$$25 = 1 \times 13 + 12$$
$$13 = 12 + 1$$

A More Interesting Case: GCD(38,101)

$$101 = 2 \times 38 + 25$$
$$38 = 1 \times 25 + 13$$
$$25 = 1 \times 13 + 12$$
$$13 = 12 + 1$$
$12 = 12 \times 1 + 0$. Go back one: 1 is the GCD.

A More Interesting Case: GCD(38,101)

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$
$12 = 12 \times 1 + 0$. Go back one: 1 is the GCD.

$1 = 13 - 12 = 13 - (25 - 13) = 2 \times 13 - 25$

A More Interesting Case: GCD(38,101)

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$
$12 = 12 \times 1 + 0$. Go back one: 1 is the GCD.

$1 = 13 - 12 = 13 - (25 - 13) = 2 \times 13 - 25$
$1 = 2(38 - 25) - 25 = 2 \times 38 - 3 \times 25$

A More Interesting Case: GCD(38,101)

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$
$12 = 12 \times 1 + 0$. Go back one: 1 is the GCD.

$1 = 13 - 12 = 13 - (25 - 13) = 2 \times 13 - 25$
$1 = 2(38 - 25) - 25 = 2 \times 38 - 3 \times 25$
$1 = 2 \times 38 - 3 \times (101 - 2 \times 38) = 8 \times 38 - 3 \times 101$

A More Interesting Case: GCD(38,101)

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$
$12 = 12 \times 1 + 0$. Go back one: 1 is the GCD.

$1 = 13 - 12 = 13 - (25 - 13) = 2 \times 13 - 25$
$1 = 2(38 - 25) - 25 = 2 \times 38 - 3 \times 25$
$1 = 2 \times 38 - 3 \times (101 - 2 \times 38) = 8 \times 38 - 3 \times 101$
$1 = 8 \times 38 - 3 \times 101$
Why is this interesting? **Hint:** What was our original goal?

A More Interesting Case: GCD(38,101)

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$
$12 = 12 \times 1 + 0$. Go back one: 1 is the GCD.

$1 = 13 - 12 = 13 - (25 - 13) = 2 \times 13 - 25$
$1 = 2(38 - 25) - 25 = 2 \times 38 - 3 \times 25$
$1 = 2 \times 38 - 3 \times (101 - 2 \times 38) = 8 \times 38 - 3 \times 101$
$1 = 8 \times 38 - 3 \times 101$
Why is this interesting? **Hint:** What was our original goal?
Take both sides $\mod 101$
$1 \equiv 8 \times 38 \pmod{101}$

A More Interesting Case: GCD(38,101)

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$
$12 = 12 \times 1 + 0$. Go back one: 1 is the GCD.

$1 = 13 - 12 = 13 - (25 - 13) = 2 \times 13 - 25$
$1 = 2(38 - 25) - 25 = 2 \times 38 - 3 \times 25$
$1 = 2 \times 38 - 3 \times (101 - 2 \times 38) = 8 \times 38 - 3 \times 101$
$1 = 8 \times 38 - 3 \times 101$
Why is this interesting? **Hint:** What was our original goal?
Take both sides $\mod 101$
$1 \equiv 8 \times 38 \pmod{101}$
8 is the inverse of 38 mod 101

$\mathrm{GCD}(x, 0)$

Two things about GCD I want to clarify.

- Why is $\mathrm{GCD}(x, 0) = x$ for $x \geq 1$?
- When does the algorithm stop?

GCD(404, 192): I Now Supply Last Step

$404 = 2 \times 192 + 20$

GCD(404, 192): I Now Supply Last Step

$$404 = 2 \times 192 + 20$$
$$192 = 9 \times 20 + 12$$

GCD(404, 192): I Now Supply Last Step

$$404 = 2 \times 192 + 20$$
$$192 = 9 \times 20 + 12$$
$$20 = 1 \times 12 + 8$$

$\mathrm{GCD}(404, 192)$: I Now Supply Last Step

$$404 = 2 \times 192 + 20$$
$$192 = 9 \times 20 + 12$$
$$20 = 1 \times 12 + 8$$
$$12 = 1 \times 8 + 4$$

GCD(404, 192): I Now Supply Last Step

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + \mathbf{0}$ STOP WHEN GET 0. Go back one: 4 is GCD.

GCD(404, 192): I Now Supply Last Step

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + \mathbf{0}$ STOP WHEN GET 0. Go back one: 4 is GCD.

Lets look at what the algorithm actually does:

$\mathrm{GCD}(404, 192)$: I Now Supply Last Step

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + \mathbf{0}$ STOP WHEN GET 0. Go back one: 4 is GCD.

Lets look at what the algorithm actually does:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 2 \times 192, 192) = \mathrm{GCD}(20, 192) =$

$\mathrm{GCD}(404, 192)$: I Now Supply Last Step

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + \mathbf{0}$ STOP WHEN GET 0. Go back one: 4 is GCD.

Lets look at what the algorithm actually does:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 2 \times 192, 192) = \mathrm{GCD}(20, 192) =$
$\mathrm{GCD}(20, 192 - 9 \times 20) = \mathrm{GCD}(20, 12) = \mathrm{GCD}(20 - 1 \times 12, 12) =$

GCD(404, 192): I Now Supply Last Step

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + \mathbf{0}$ STOP WHEN GET 0. Go back one: 4 is GCD.

Lets look at what the algorithm actually does:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 2 \times 192, 192) = \mathrm{GCD}(20, 192) =$
$\mathrm{GCD}(20, 192 - 9 \times 20) = \mathrm{GCD}(20, 12) = \mathrm{GCD}(20 - 1 \times 12, 12) =$
$\mathrm{GCD}(8, 12) = \mathrm{GCD}(8, 12 - 8) = \mathrm{GCD}(8, 4) =$

GCD(404, 192): I Now Supply Last Step

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + \mathbf{0}$ STOP WHEN GET 0. Go back one: 4 is GCD.

Lets look at what the algorithm actually does:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 2 \times 192, 192) = \mathrm{GCD}(20, 192) =$
$\mathrm{GCD}(20, 192 - 9 \times 20) = \mathrm{GCD}(20, 12) = \mathrm{GCD}(20 - 1 \times 12, 12) =$
$\mathrm{GCD}(8, 12) = \mathrm{GCD}(8, 12 - 8) = \mathrm{GCD}(8, 4) =$
$\mathrm{GCD}(8 - 2 \times 4, 4) = \mathrm{GCD}(0, 4)$

$\mathrm{GCD}(404, 192)$: I Now Supply Last Step

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$
$8 = 4 \times 2 + \mathbf{0}$ STOP WHEN GET 0. Go back one: 4 is GCD.

Lets look at what the algorithm actually does:
$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 2 \times 192, 192) = \mathrm{GCD}(20, 192) =$
$\mathrm{GCD}(20, 192 - 9 \times 20) = \mathrm{GCD}(20, 12) = \mathrm{GCD}(20 - 1 \times 12, 12) =$
$\mathrm{GCD}(8, 12) = \mathrm{GCD}(8, 12 - 8) = \mathrm{GCD}(8, 4) =$
$\mathrm{GCD}(8 - 2 \times 4, 4) = \mathrm{GCD}(0, 4)$

To make our formula $\mathrm{GCD}(x, y) = \mathrm{GCD}(x - ky, x)$ work all the way to 0, we **define** $\mathrm{GCD}(0, x) = x$.

Why is $\mathrm{GCD}(\mathbf{0}, x) = x$?

Why is $\mathbf{GCD}(\mathbf{0}, \boldsymbol{x}) = \boldsymbol{x}$?

Why is $\mathrm{GCD}(0, x) = x$?

Why is $\mathbf{GCD}(\mathbf{0}, \boldsymbol{x}) = \boldsymbol{x}$?
This is a more interesting question than it appears.

Why is $\mathrm{GCD}(0, x) = x$?

Why is $\mathbf{GCD(0, x) = x}$?
This is a more interesting question than it appears.

Or I am going to make a point about math inspired by the question.

Why is $\mathrm{GCD}(0, x) = x$?

Why is $\mathbf{GCD(0,}\ \boldsymbol{x}\mathbf{)} = \boldsymbol{x}$?
This is a more interesting question than it appears.

Or I am going to make a point about math inspired by the question.

First a short detour: why is $5^{1/2} = \sqrt{5}$?

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time?

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss.

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss. **No**.

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss. **No**.

For $a, b \in \mathbb{N}$ we have

$$5^a \times 5^b = 5^{a+b}.$$

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss. **No**.

For $a, b \in \mathbb{N}$ we have

$$5^a \times 5^b = 5^{a+b}.$$

We want this rule to still apply when $a, b \in \mathbb{Q}$.

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss. **No**.

For $a, b \in \mathbb{N}$ we have

$$5^a \times 5^b = 5^{a+b}.$$

We want this rule to still apply when $a, b \in \mathbb{Q}$. So we want

$$5^{1/2} \times 5^{1/2} = 5^{1/2+1/2} = 5$$

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss. **No**.

For $a, b \in \mathbb{N}$ we have

$$5^a \times 5^b = 5^{a+b}.$$

We want this rule to still apply when $a, b \in \mathbb{Q}$. So we want

$$5^{1/2} \times 5^{1/2} = 5^{1/2+1/2} = 5$$

Hence we **define** $5^{1/2} = \sqrt{5}$ to make that rule work out.

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss. **No**.

For $a, b \in \mathbb{N}$ we have

$$5^a \times 5^b = 5^{a+b}.$$

We want this rule to still apply when $a, b \in \mathbb{Q}$. So we want

$$5^{1/2} \times 5^{1/2} = 5^{1/2+1/2} = 5$$

Hence we **define** $5^{1/2} = \sqrt{5}$ to make that rule work out.

Similar for 5^0 and 5^{-a}.

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss. **No**.

For $a, b \in \mathbb{N}$ we have

$$5^a \times 5^b = 5^{a+b}.$$

We want this rule to still apply when $a, b \in \mathbb{Q}$. So we want

$$5^{1/2} \times 5^{1/2} = 5^{1/2+1/2} = 5$$

Hence we **define** $5^{1/2} = \sqrt{5}$ to make that rule work out.

Similar for 5^0 and 5^{-a}.

How is 5^π defined?

Why is $5^{1/2} = \sqrt{5}$?

Why is

$$5^{1/2} = \sqrt{5}?$$

Are we multiplying a number by itself half a time? Discuss. **No**.

For $a, b \in \mathbb{N}$ we have

$$5^a \times 5^b = 5^{a+b}.$$

We want this rule to still apply when $a, b \in \mathbb{Q}$. So we want

$$5^{1/2} \times 5^{1/2} = 5^{1/2+1/2} = 5$$

Hence we **define** $5^{1/2} = \sqrt{5}$ to make that rule work out.

Similar for 5^0 and 5^{-a}.

How is 5^π defined? Discuss.

What is 5^π?

We want

$$5^{3.14159} < 5^\pi < 5^{3.141593}.$$

What is 5^π?

We want

$$5^{3.14159} < 5^\pi < 5^{3.141593}.$$

We can approximate π better and better.

What is 5^π?

We want

$$5^{3.14159} < 5^\pi < 5^{3.141593}.$$

We can approximate π better and better.

So, with this in mind, how do we define 5^π?

What is 5^π?

We want

$$5^{3.14159} < 5^\pi < 5^{3.141593}.$$

We can approximate π better and better.

So, with this in mind, how do we define 5^π?

Let $\alpha_1, \alpha_2, \ldots,$ be an infinite sequence of rationals that cvg to π.

What is 5^π?

We want

$$5^{3.14159} < 5^{\pi} < 5^{3.141593}.$$

We can approximate π better and better.

So, with this in mind, how do we define 5^π?

Let $\alpha_1, \alpha_2, \ldots,$ be an infinite sequence of rationals that cvg to π.
5^π is **defined** to be $\lim_{i\to\infty} 5^{\alpha_i}$.

What is 5^π?

We want

$$5^{3.14159} < 5^\pi < 5^{3.141593}.$$

We can approximate π better and better.

So, with this in mind, how do we define 5^π?

Let $\alpha_1, \alpha_2, \ldots,$ be an infinite sequence of rationals that cvg to π.
5^π is **defined** to be $\lim_{i \to \infty} 5^{\alpha_i}$.
Need to prove that all choices of sequences yield the same result.
We won't do that here

START HERE ON SEPT 7

START HERE ON SEPT 7.
BILL- START RECORDING.

Upshot

Sometimes functions are defined on certain values **not** because its the most natural way to do it, but because it makes prior rules work out.

Upshot

Sometimes functions are defined on certain values **not** because its the most natural way to do it, but because it makes prior rules work out.

This is the case for

Upshot

Sometimes functions are defined on certain values **not** because its the most natural way to do it, but because it makes prior rules work out.

This is the case for

- $\mathrm{GCD}(x, 0) = x$.

Upshot

Sometimes functions are defined on certain values **not** because its the most natural way to do it, but because it makes prior rules work out.

This is the case for

- $\mathrm{GCD}(x, 0) = x$.
- $5^{1/2} = \sqrt{5}$.

Upshot

Sometimes functions are defined on certain values **not** because its the most natural way to do it, but because it makes prior rules work out.

This is the case for

- $\mathrm{GCD}(x, 0) = x$.
- $5^{1/2} = \sqrt{5}$.
- $\frac{1}{2}!$

Upshot

Sometimes functions are defined on certain values **not** because its the most natural way to do it, but because it makes prior rules work out.

This is the case for

- $\mathrm{GCD}(x, 0) = x$.
- $5^{1/2} = \sqrt{5}$.
- $\frac{1}{2}! = \sqrt{\pi}$.

Upshot

Sometimes functions are defined on certain values **not** because its the most natural way to do it, but because it makes prior rules work out.

This is the case for

- $\mathrm{GCD}(x, 0) = x$.
- $5^{1/2} = \sqrt{5}$.
- $\frac{1}{2}! = \sqrt{\pi}$. Don't ask me why.

Upshot

Sometimes functions are defined on certain values **not** because its the most natural way to do it, but because it makes prior rules work out.

This is the case for

- $\mathrm{GCD}(x, 0) = x$.
- $5^{1/2} = \sqrt{5}$.
- $\frac{1}{2}! = \sqrt{\pi}$. Don't ask me why.
- 5^i I leave to you to look up or derive.

A Student Recommended 5^π be...

I defined 5^π using limits. A student recommended the following:

A Student Recommended 5^π be...

I defined 5^π using limits. A student recommended the following:

$$5^\pi = e^{\pi \ln 5}.$$

A Student Recommended 5^π be...

I defined 5^π using limits. A student recommended the following:

$$5^\pi = e^{\pi \ln 5}.$$

The students way is better since it is simpler. With my way you need to prove the answer is independent of which sequence is used.

A Student Recommended 5^π be...

I defined 5^π using limits. A student recommended the following:

$$5^\pi = e^{\pi \ln 5}.$$

The students way is better since it is simpler. With my way you need to prove the answer is independent of which sequence is used.

For a story about me, my Dad, and π see
`https://blog.computationalcomplexity.org/2019/06/a-proof-that-227-pi-0-and-more.html`

Back to the Affine Cipher

Back to the Affine Cipher

1. Key space is $K = \{(a, b) : 0 \leq a, b \leq 25, a \text{ is rel prime to } 26\}$.
2. To encode x goes to $ax + b$.
3. To decode x goes to $a^{-1}(x - b)$.
   ($a^{-1} \pmod{26}$ exists since a is rel prime to 26.)

Back to the Affine Cipher

1. Key space is $K = \{(a, b) : 0 \leq a, b \leq 25, a \text{ is rel prime to } 26\}$.
2. To encode x goes to $ax + b$.
3. To decode x goes to $a^{-1}(x - b)$.
   ($a^{-1} \pmod{26}$ exists since a is rel prime to 26.)

Is it crackable?

Back to the Affine Cipher

1. Key space is $K = \{(a, b) : 0 \leq a, b \leq 25, a \text{ is rel prime to } 26\}$.
2. To encode x goes to $ax + b$.
3. To decode x goes to $a^{-1}(x - b)$.
   ($a^{-1} \pmod{26}$ exists since a is rel prime to 26.)

Is it crackable?

Yes

Back to the Affine Cipher

1. Key space is $K = \{(a, b) : 0 \leq a, b \leq 25, a \text{ is rel prime to } 26\}$.
2. To encode x goes to $ax + b$.
3. To decode x goes to $a^{-1}(x - b)$.
   ($a^{-1} \pmod{26}$ exists since a is rel prime to 26.)

Is it crackable?

Yes

Similar to how we cracked Shift.

Back to the Affine Cipher

1. Key space is $K = \{(a, b) : 0 \leq a, b \leq 25, a \text{ is rel prime to } 26\}$.
2. To encode x goes to $ax + b$.
3. To decode x goes to $a^{-1}(x - b)$.
   ($a^{-1} \pmod{26}$ exists since a is rel prime to 26.)

Is it crackable?

Yes

Similar to how we cracked Shift.

Next Slide.

Cracking Affine Cipher

Cracking Affine Cipher

1. Input T, a long text of normal English.

Cracking Affine Cipher

1. Input T, a long text of normal English.
2. For all $(a, b) \in K$:

Cracking Affine Cipher

1. Input T, a long text of normal English.
2. For all $(a, b) \in K$:
   (i) apply $ax + b$ to T to obtain $T_{a,b}$.

Cracking Affine Cipher

1. Input T, a long text of normal English.
2. For all $(a, b) \in K$:
   (i) apply $ax + b$ to T to obtain $T_{a,b}$.
   (ii) Let $f_{a,b}$ be freq vector of $T_{a,b}$.

Cracking Affine Cipher

1. Input T, a long text of normal English.
2. For all $(a, b) \in K$:
   (i) apply $ax + b$ to T to obtain $T_{a,b}$.
   (ii) Let $f_{a,b}$ be freq vector of $T_{a,b}$.
   (iii) Compute $f_E \cdot f_{a,b}$.

Cracking Affine Cipher

1. Input T, a long text of normal English.
2. For all $(a, b) \in K$:
   (i) apply $ax + b$ to T to obtain $T_{a,b}$.
   (ii) Let $f_{a,b}$ be freq vector of $T_{a,b}$.
   (iii) Compute $f_E \cdot f_{a,b}$.
3. $(a_0, b_0) = \max_{(a,b)\in K} f_{a,b} \cdot f_E$. (a_0, b_0) is key to decode with.

Cracking Affine Cipher

1. Input T, a long text of normal English.
2. For all $(a, b) \in K$:
   (i) apply $ax + b$ to T to obtain $T_{a,b}$.
   (ii) Let $f_{a,b}$ be freq vector of $T_{a,b}$.
   (iii) Compute $f_E \cdot f_{a,b}$.
3. $(a_0, b_0) = \max_{(a,b)\in K} f_{a,b} \cdot f_E$. (a_0, b_0) is key to decode with.

For affine there is a gap just like with Shift. We need to know there IS a gap for this to work, but do not need to know what it is.

Cracking Affine Cipher

1. Input T, a long text of normal English.
2. For all $(a, b) \in K$:
   (i) apply $ax + b$ to T to obtain $T_{a,b}$.
   (ii) Let $f_{a,b}$ be freq vector of $T_{a,b}$.
   (iii) Compute $f_E \cdot f_{a,b}$.
3. $(a_0, b_0) = \max_{(a,b) \in K} f_{a,b} \cdot f_E$. (a_0, b_0) is key to decode with.

For affine there is a gap just like with Shift. We need to know there IS a gap for this to work, but do not need to know what it is.
Freq Vector (A student asked this in my office hours.) Its really a prob vector– the entries sum to 1. So you take the freqs and divide by the length of the text.

The Quadratic Ciphers

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO.

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.
So pick a, b, c so that $f(x)$ has an inverse.

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.
So pick a, b, c so that $f(x)$ has an inverse.
Contrast

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.
So pick a, b, c so that $f(x)$ has an inverse.
Contrast

1. Affine: **Easy** to test if $f(x) = ax + b$ is bijection.

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.
So pick a, b, c so that $f(x)$ has an inverse.
Contrast

1. Affine: **Easy** to test if $f(x) = ax + b$ is bijection.
2. Quad: **Hard** to test if $f(x) = ax^2 + bx + c$ is a bijection.

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.
So pick a, b, c so that $f(x)$ has an inverse.
Contrast

1. Affine: **Easy** to test if $f(x) = ax + b$ is bijection.
2. Quad: **Hard** to test if $f(x) = ax^2 + bx + c$ is a bijection.

Is there **some** way to test? Discuss

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.
So pick a, b, c so that $f(x)$ has an inverse.
Contrast

1. Affine: **Easy** to test if $f(x) = ax + b$ is bijection.
2. Quad: **Hard** to test if $f(x) = ax^2 + bx + c$ is a bijection.

Is there **some** way to test? Discuss
Yes Compute $f(0), \ldots, f(25)$ and see if all are different.

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.
So pick a, b, c so that $f(x)$ has an inverse.
Contrast

1. Affine: **Easy** to test if $f(x) = ax + b$ is bijection.
2. Quad: **Hard** to test if $f(x) = ax^2 + bx + c$ is a bijection.

Is there **some** way to test? Discuss
Yes Compute $f(0), \ldots, f(25)$ and see if all are different.

1. Test takes too long.

The Quadratic Cipher (all math mod 26)

Def The Quadratic cipher with a, b, c: Encrypt via
$x \rightarrow ax^2 + bx + c$.

Does this work? Vote YES or NO. Answer: NO
Need $f(x) = ax^2 + bx + c$ to be a bijection.
So pick a, b, c so that $f(x)$ has an inverse.
Contrast

1. Affine: **Easy** to test if $f(x) = ax + b$ is bijection.
2. Quad: **Hard** to test if $f(x) = ax^2 + bx + c$ is a bijection.

Is there **some** way to test? Discuss
Yes Compute $f(0), \ldots, f(25)$ and see if all are different.

1. Test takes too long.
2. Quad Cipher not secure enough to be worth the time.

History of the Quadratic Cipher

The first place **The Quadratic Cipher** appeared was

History of the Quadratic Cipher

The first place **The Quadratic Cipher** appeared was

my 3-week course on crypto for High School Students in 2010.

History of the Quadratic Cipher

The first place **The Quadratic Cipher** appeared was

my 3-week course on crypto for High School Students in 2010.

So, as the kids say, **it's not a thing**.

The Point of Presenting the Quadratic Cipher

When looking at a cipher one usually asks:

The Point of Presenting the Quadratic Cipher

When looking at a cipher one usually asks:

Is the cipher secure?

The Point of Presenting the Quadratic Cipher

When looking at a cipher one usually asks:

Is the cipher secure?

That is a good question.

The Point of Presenting the Quadratic Cipher

When looking at a cipher one usually asks:

Is the cipher secure?

That is a good question.

But there is another important one:

The Point of Presenting the Quadratic Cipher

When looking at a cipher one usually asks:

Is the cipher secure?

That is a good question.

But there is another important one:

Is the cipher easy to use?

The Point of Presenting the Quadratic Cipher

When looking at a cipher one usually asks:

Is the cipher secure?

That is a good question.

But there is another important one:

Is the cipher easy to use?

Quadratic Cipher fails the **ease of use** test.

The Point of Presenting the Quadratic Cipher

When looking at a cipher one usually asks:

Is the cipher secure?

That is a good question.

But there is another important one:

Is the cipher easy to use?

Quadratic Cipher fails the **ease of use** test.

It is **also** insecure.

Amateur Ciphers

Many amateur's come up with ciphers that they claim are **uncrackable**.

Amateur Ciphers

Many amateur's come up with ciphers that they claim are **uncrackable**.
These ciphers fall into the following categories.

Amateur Ciphers

Many amateur's come up with ciphers that they claim are **uncrackable**.

These ciphers fall into the following categories.

1. Hard to use. That was the problem with Quad Cipher.

Amateur Ciphers

Many amateur's come up with ciphers that they claim are **uncrackable**.
These ciphers fall into the following categories.

1. Hard to use. That was the problem with Quad Cipher.
2. Easy to crack by a trick the inventor didn't know.

Amateur Ciphers

Many amateur's come up with ciphers that they claim are **uncrackable**.
These ciphers fall into the following categories.

1. Hard to use. That was the problem with Quad Cipher.
2. Easy to crack by a trick the inventor didn't know.
3. Only uncrackable on short texts.

Amateur Ciphers

Many amateur's come up with ciphers that they claim are **uncrackable**.
These ciphers fall into the following categories.

1. Hard to use. That was the problem with Quad Cipher.
2. Easy to crack by a trick the inventor didn't know.
3. Only uncrackable on short texts.
4. Only uncrackable if Eve does not know the system (violates Kerckhoff's Principle).

Amateur Ciphers

Many amateur's come up with ciphers that they claim are **uncrackable**.
These ciphers fall into the following categories.

1. Hard to use. That was the problem with Quad Cipher.
2. Easy to crack by a trick the inventor didn't know.
3. Only uncrackable on short texts.
4. Only uncrackable if Eve does not know the system (violates Kerckhoff's Principle).
5. There are other reasons they are wrong.

BILL
STOP RECORDING
THIS LECTURE