BILL
RECORD THIS
LECTURE

September 16, 2020

Affine and Quadratic Ciphers

September 16, 2020

The Affine Ciphers

September 16, 2020

Affine Cipher

Recall: Shift cipher with shift s:

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:

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:

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:

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:

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:

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

Affine Cipher

Recall: Shift cipher with shift s:

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:

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:

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:

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:

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:

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.

Affine Cipher

Recall: Shift cipher with shift s:

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:

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.

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

September 16, 2020

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

GCD(404,192) The Long Way

d div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

GCD(404,192) The Long Way

d div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

GCD(404,192) The Long Way

d div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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

GCD(404,192) The Long Way

d div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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

GCD(404,192) The Long Way

d div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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 div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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 div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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 div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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 div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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 div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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 div **both** 404 and 192
IFF
d div 404 and $404 - 192 = 212$.

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

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:
$4 = 2 \times 192 - 19 \times (404 - 2 \times 192) = 39 \times 192 - 19 \times 404$
Upshot: $GCD(m, n)$ 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

How to find inverse of m mod n

Given m, n with $m < n$ we want to know

How to find inverse of m mod n

Given m, n with $m < n$ we want to know

- Is there an inverse of m mod n

How to find inverse of m mod n

Given m, n with $m < n$ we want to know

- Is there an inverse of m mod n
- If so then find it

How to find inverse of m mod n

Given m, n with $m < n$ we want to know

- Is there an inverse of m mod n
- If so then find it

1. Find $\mathrm{GCD}(m, n)$. If it is NOT 1 then NO inverse.

How to find inverse of m mod n

Given m, n with $m < n$ we want to know

- Is there an inverse of m mod n
- If so then find it

1. Find $\mathrm{GCD}(m, n)$. If it is NOT 1 then NO inverse.
2. If it IS 1 then use the work you did to find $\mathrm{GCD}(m, n)$ to find $a, b \in \mathbb{Z}$

$$am + bn = 1$$

$$am \equiv 1 \pmod{n}$$

3. a is the inverse of m mod n.

How to find inverse of m mod n

Given m, n with $m < n$ we want to know

- Is there an inverse of m mod n
- If so then find it

1. Find $\mathrm{GCD}(m, n)$. If it is NOT 1 then NO inverse.
2. If it IS 1 then use the work you did to find $\mathrm{GCD}(m, n)$ to find $a, b \in \mathbb{Z}$

$$am + bn = 1$$

$$am \equiv 1 \pmod{n}$$

3. a is the inverse of m mod n. Not quite: (1) a might be negative (2) a might be $> n$. That won't do!

How to find inverse of m mod n

Given m, n with $m < n$ we want to know

- Is there an inverse of m mod n
- If so then find it

1. Find $\mathrm{GCD}(m, n)$. If it is NOT 1 then NO inverse.
2. If it IS 1 then use the work you did to find $\mathrm{GCD}(m, n)$ to find $a, b \in \mathbb{Z}$

$$am + bn = 1$$

$$am \equiv 1 \pmod{n}$$

3. a is the inverse of m mod n. Not quite: (1) a might be negative (2) a might be $> n$. That won't do! Take $a \pmod{n}$.

The Quadratic Ciphers

September 16, 2020

The Quadratic Cipher

Def The Quadratic cipher with a, b, c: Encrypt via
$x \to ax^2 + bx + c \pmod{26}$.

The Quadratic Cipher

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c \pmod{26}$.

Does this work? Vote YES or NO.

The Quadratic Cipher

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c \pmod{26}$.

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

The Quadratic Cipher

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c \pmod{26}$.

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

No easy test for Invertibility (depends on def of easy).
How Easy?: Given a quadratic $f(x)$ one could compute $f(0), \ldots, f(25)$ all mod 26 and see if all are different.

The Quadratic Cipher

Def The Quadratic cipher with a, b, c: Encrypt via $x \rightarrow ax^2 + bx + c \pmod{26}$.

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

No easy test for Invertibility (depends on def of easy).
How Easy?: Given a quadratic $f(x)$ one could compute $f(0), \ldots, f(25)$ all mod 26 and see if all are different.

1. This takes to long.
2. The security is not good enough to justify taking this long setting it up.

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.

Ease of Use VS Easy to Crack

Shift and Affine:

Ease of Use VS Easy to Crack

Shift and Affine:

- Some math is used to encrypt and decrypt.

Ease of Use VS Easy to Crack

Shift and Affine:

- Some math is used to encrypt and decrypt.
- The math makes it easy to use. Short Key!

Ease of Use VS Easy to Crack

Shift and Affine:

- Some math is used to encrypt and decrypt.
- The math makes it easy to use. Short Key!
- The math makes it insecure. Few Keys!

Ease of Use VS Easy to Crack

Shift and Affine:

- Some math is used to encrypt and decrypt.
- The math makes it easy to use. Short Key!
- The math makes it insecure. Few Keys!

Next slide packet: We present a cipher with **less** math so **more secure** in next slide packet.

BILL
STOP RECORDING
THIS LECTURE

September 16, 2020