Something ELSE Wrong With All Ciphers So Far

September 16, 2019

How can Bob be Sure it Came from Eve?

1. Eve knows that Alice is going to send Bob a number that is < 999 which indicates how much money Bob should give Eve.
2. They will send the message in binary using use one-time pad.
3. Alice sends the message 1001101010010110.
4. Eve intercepts and tampers with msg before Bob gets it.
5. Can Eve tamper with it in a way that matters? Discuss

Yes: Eve Knows the 10th bit of real message is 0 since she gets $999 < 1024$ dollars. Let b be the 10th bit that is sent. Eve Flips 10th Bit in ciphertext to flip 10th bit in numbers

Original Message: 1001101010010110
Eve Tampers: 1001101000010110

Eve just got 1024 more dollars!

Even if not, Eve can mess with the message to make it meaningless.

Lesson Learned/Our Goal

Security: Eve cannot learn message

Integrity: Bob can be sure the message came from Alice

Lesson Learned: One-time-pad is Secure but lacks integrity. Security does not imply integrity.

Question: Does Integrity imply Security.Discuss

Lesson Learned/Our Goal

Security: Eve cannot learn message

Integrity: Bob can be sure the message came from Alice

Lesson Learned: One-time-pad is Secure but lacks integrity.
Security does not imply integrity.

Question: Does Integrity imply Security.Discuss

No. Will discuss later.

Goal for now: Make Shift Cipher not forgeable.
Discuss

Integrity-Shift

Integrity-Shift: Key is a shift s and a function $g : S \to S$.

1. To send message $(m_1, \ldots, m_L)$ (each m_i is a char) send

$$(m_1 + s, g(m_1)), \ldots, (m_L + s, g(m_L)).$$

2. To decode message $((c_1, d_1), \ldots, (c_L, d_L))$ just

$$(c_1 - s, \ldots, c_L - s).$$

3. To Authenticate Once Bob has $m_1, \ldots, m_L$ he computes $g(m_1), \ldots, g(m_L)$ and checks that, for all i, $g(m_i) = d_i$.

Idea: Bob can make sure that the message he gets is the one Alice sent.

HW 01 Review and NEW material Inspired by it

September 16, 2019

Problem 2

Klingons use an alphabet of 29 letters. Vulcans use an alphabet of 30 letters. Spock notes that Klingons have an easier time using the affine cipher than Vulcans. He is correct.

Why is it easier for Klingons to use the affine cipher than Vulcans?

Problem 2

Klingons use an alphabet of 29 letters. Vulcans use an alphabet of 30 letters. Spock notes that Klingons have an easier time using the affine cipher than Vulcans. He is correct.

Why is it easier for Klingons to use the affine cipher than Vulcans?
ANSWER: Since all $a \in \{1, \ldots, 28\}$ are relatively prime to 29, Klingons can use any a they want. Vulcans need to be careful to make sure that a is rel prime to 30.
Some students said there were more numbers rel primes to 29 then to 30. True but a odd since ALL numbers work.
Mundane Issue: We gave full credit but WILL NOT in the future.

Problem 2

Klingons use an alphabet of 29 letters. Vulcans use an alphabet of 30 letters. Spock notes that Klingons have an easier time using the affine cipher than Vulcans. He is correct.

Why is it easier for Klingons to use the affine cipher than Vulcans?
ANSWER: Since all $a \in \{1, \ldots, 28\}$ are relatively prime to 29, Klingons can use any a they want. Vulcans need to be careful to make sure that a is rel prime to 30.
Some students said there were more numbers rel primes to 29 then to 30. True but a odd since ALL numbers work.
Mundane Issue: We gave full credit but WILL NOT in the future.
Raises Interesting Question: Which composite numbers n are such that many numbers in $\{1, \ldots, n\}$ are rel prime to n?
Will consider this on the next slide.

Problem 2 Inspires us to Look at the ϕ-function

Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are rel prime to n.

$\phi(2) =$

Problem 2 Inspires us to Look at the ϕ-function

Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are rel prime to n.
$\phi(2) = 1$. Just $\{1\}$
$\phi(3) =$

Problem 2 Inspires us to Look at the ϕ-function

Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are rel prime to n.
$\phi(2) = 1$. Just $\{1\}$
$\phi(3) = 2$. Just $\{1, 2\}$. AH-HA: if p prime, $\phi(p) = p - 1$.
$\phi(4) =$

Problem 2 Inspires us to Look at the ϕ-function

Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are rel prime to n.

$\phi(2) = 1$. Just $\{1\}$

$\phi(3) = 2$. Just $\{1, 2\}$. AH-HA: if p prime, $\phi(p) = p - 1$.

$\phi(4) = 2$. Just $\{1, 3\}$.

$\phi(5) =$

Problem 2 Inspires us to Look at the ϕ-function

Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are rel prime to n.

$\phi(2) = 1$. Just $\{1\}$

$\phi(3) = 2$. Just $\{1, 2\}$. AH-HA: if p prime, $\phi(p) = p - 1$.

$\phi(4) = 2$. Just $\{1, 3\}$.

$\phi(5) = 4$. Just $\{1, 2, 3, 4\}$.

$\phi(6) =$

Problem 2 Inspires us to Look at the ϕ-function

Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are rel prime to n.

$\phi(2) = 1$. Just $\{1\}$

$\phi(3) = 2$. Just $\{1, 2\}$. AH-HA: if p prime, $\phi(p) = p - 1$.

$\phi(4) = 2$. Just $\{1, 3\}$.

$\phi(5) = 4$. Just $\{1, 2, 3, 4\}$.

$\phi(6) = 2$. Just $\{1, 5\}$.

$\phi(7) =$

Problem 2 Inspires us to Look at the ϕ-function

Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are rel prime to n.

$\phi(2) = 1$. Just $\{1\}$

$\phi(3) = 2$. Just $\{1, 2\}$. AH-HA: if p prime, $\phi(p) = p - 1$.

$\phi(4) = 2$. Just $\{1, 3\}$.

$\phi(5) = 4$. Just $\{1, 2, 3, 4\}$.

$\phi(6) = 2$. Just $\{1, 5\}$.

$\phi(7) = 6$. Just $\{1, 2, 3, 4, 5, 6\}$.

$\phi(8) =$

Problem 2 Inspires us to Look at the ϕ-function

Let $\phi(n)$ be the number of numbers in $\{1, \ldots, n\}$ that are rel prime to n.

$\phi(2) = 1$. Just $\{1\}$

$\phi(3) = 2$. Just $\{1, 2\}$. AH-HA: if p prime, $\phi(p) = p - 1$.

$\phi(4) = 2$. Just $\{1, 3\}$.

$\phi(5) = 4$. Just $\{1, 2, 3, 4\}$.

$\phi(6) = 2$. Just $\{1, 5\}$.

$\phi(7) = 6$. Just $\{1, 2, 3, 4, 5, 6\}$.

$\phi(8) = 4$. Just $\{1, 3, 5, 7\}$.

Can we be more systematic?

Problem 2 Inspires us to Look at the ϕ-function

If p is prime then $\phi(p) = p - 1$. If q is prime then $\phi(q) = q - 1$.
We assume $p \neq q$. What is $\phi(pq)$?
Set of numbers in $\{1, \ldots, pq - 1\}$ that p divides:

$$\{p, 2p, 3p, \ldots, (q-1)p\} \text{ OH, there are } q - 1 \text{ of them}$$

Set of numbers in $\{1, \ldots, pq - 1\}$ that q divides:

$$\{q, 2q, 3q, \ldots, (p-1)q\} \text{ OH, there are } p - 1 \text{ of them}$$

NO overlap in these sets. So the number of numbers in $\{1, \ldots, pq - 1\}$ that are not in either of these sets is

$$(pq - 1) - (p - 1) - (q - 1) = pq - p - q + 1 = (p - 1)(q - 1).$$

Why did I write it that way?

Problem 2 Inspires us to Look at the ϕ-function

If p is prime then $\phi(p) = p - 1$. If q is prime then $\phi(q) = q - 1$.
We assume $p \neq q$. What is $\phi(pq)$?
Set of numbers in $\{1, \ldots, pq - 1\}$ that p divides:

$$\{p, 2p, 3p, \ldots, (q-1)p\} \text{ OH, there are } q - 1 \text{ of them}$$

Set of numbers in $\{1, \ldots, pq - 1\}$ that q divides:

$$\{q, 2q, 3q, \ldots, (p-1)q\} \text{ OH, there are } p - 1 \text{ of them}$$

NO overlap in these sets. So the number of numbers in $\{1, \ldots, pq - 1\}$ that are not in either of these sets is

$$(pq - 1) - (p - 1) - (q - 1) = pq - p - q + 1 = (p - 1)(q - 1).$$

Why did I write it that way?

$$\phi(pq) = (p - 1)(q - 1) = \phi(p)\phi(q).$$

Problem 2 Inspires us to Look at the ϕ-function

$$\phi(pq) = (p-1)(q-1) = \phi(p)\phi(q).$$

This generalizes:

Theorem: If a, b are rel prime then $\phi(ab) = \phi(a)\phi(b)$.

Example of proof n next slide.

$\phi(5 \times 8)$

x is rel prime to 5×8 if its rel prime to 5 and rel prime to 8.

1	6	11	16	21	26	31	36
2	7	12	17	22	27	32	37
3	8	13	18	23	28	33	38
4	9	14	19	24	29	34	39
5	10	15	20	25	30	35	40

Look at the rows. If the first entry is NOT rel prime to 5, then entire row is not. Hence need only look at the $\phi(5)$ columns that begin with a number rel prime to 5.

$\phi(5 \times 8)$ Continued

x is rel prime to 5×8 if its rel prime to 5 and rel prime to 8.

1	6	11	16	21	26	31	36
2	7	12	17	22	27	32	37
3	8	13	18	23	28	33	38
4	9	14	19	24	29	34	39

Look at any row. How many elts of it are rel prime to 8. Look at the columns mod 8. Will get all 8 congruence classes mod 8. For example, the second row mod 8 is

2 7 4 1 6 3 0 5

without even looking, the number of elts in this row that are rel prime to 8 is $\phi(8)$.
So $\phi(5 \times 8) = \phi(5) \times \phi(8)$.

Which ϕ can we do Systematically?

$$\phi(7 \times 11 \times 13) = \phi(7)\phi(11)\phi(13) = 6 \times 10 = 720.$$

Which ϕ can we do Systematically?

$\phi(7 \times 11 \times 13) = \phi(7)\phi(11)\phi(13) = 6 \times 10 = 720.$

$\phi(2^{10})$. Hmmm, need to do powers systematically.

Which ϕ can we do Systematically?

$\phi(7 \times 11 \times 13) = \phi(7)\phi(11)\phi(13) = 6 \times 10 = 720.$

$\phi(2^{10})$. Hmmm, need to do powers systematically.

$\phi(2^n)$: Number of elts of $\{1, \ldots, 2^n - 1\}$ that are $\not\equiv 0 \pmod 2$.
Half of the elts of $\{1, \ldots, 2^n\}$: $\frac{1}{2}2^n = 2^{n-1}$.

Which ϕ can we do Systematically?

$\phi(7 \times 11 \times 13) = \phi(7)\phi(11)\phi(13) = 6 \times 10 = 720.$

$\phi(2^{10})$. Hmmm, need to do powers systematically.

$\phi(2^n)$: Number of elts of $\{1, \ldots, 2^n - 1\}$ that are $\not\equiv 0 \pmod 2$.
Half of the elts of $\{1, \ldots, 2^n\}$: $\frac{1}{2}2^n = 2^{n-1}$.

$\phi(3^n)$: Number of elts of $\{1, \ldots, 3^n - 1\}$ that $\not\equiv 0 \pmod 3$.
$\frac{2}{3}$'s of the elts of $\{1, \ldots, 3^n\}$: $\frac{2}{3} \times 3^n = 2 \times 3^{n-1}$.

Which ϕ can we do Systematically?

$\phi(7 \times 11 \times 13) = \phi(7)\phi(11)\phi(13) = 6 \times 10 = 720.$

$\phi(2^{10})$. Hmmm, need to do powers systematically.

$\phi(2^n)$: Number of elts of $\{1, \ldots, 2^n - 1\}$ that are $\not\equiv 0 \pmod 2$.
Half of the elts of $\{1, \ldots, 2^n\}$: $\frac{1}{2}2^n = 2^{n-1}$.

$\phi(3^n)$: Number of elts of $\{1, \ldots, 3^n - 1\}$ that $\not\equiv 0 \pmod 3$.
$\frac{2}{3}$'s of the elts of $\{1, \ldots, 3^n\}$: $\frac{2}{3} \times 3^n = 2 \times 3^{n-1}$.

$\phi(p^n)$: Number of elts of $\{1, \ldots, p^n\}$ that are $\not\equiv 0 \pmod p$.
$\frac{p-1}{p}$ of the elts of $\frac{p-1}{p} \times p^n$: $(p-1)p^{n-1}$.

Computing ϕ

1. p prime, $\phi(p^n) = (p-1)p^{n-1})$
2. a, b rel prime, $\phi(nm) = \phi(n)\phi(m)$.

If can factor m then can compute $\phi(m)$. The complexity of ϕ is not our current concern.

Vulcans and Klingons

Vulcans have an alphabet of size 2^n
Klingons have an alphabet of size 3^n
Who is better off for using the affine cipher?

Vulcans and Klingons

Vulcans have an alphabet of size 2^n
Klingons have an alphabet of size 3^n
Who is better off for using the affine cipher?

$\phi(2^n) = 2^{n-1}$. If Vulcans pick an element of $\{1, \ldots, 2^n\}$ at random then prob that its rel prime to 2^n is $\frac{2^{n-1}}{2^n} = 0.5$.

Vulcans and Klingons

Vulcans have an alphabet of size 2^n
Klingons have an alphabet of size 3^n
Who is better off for using the affine cipher?

$\phi(2^n) = 2^{n-1}$. If Vulcans pick an element of $\{1, \ldots, 2^n\}$ at random then prob that its rel prime to 2^n is $\frac{2^{n-1}}{2^n} = 0.5$.
$\phi(3^n) = 2 \times 3^{n-1}$. If Klingons pick an element of $\{1, \ldots, 3^n\}$ at random then prob that its rel prime to 3^n is $\frac{2 \times 3^{n-1}}{3^n} \sim 0.66$.

Vulcans and Klingons

Vulcans have an alphabet of size 2^n
Klingons have an alphabet of size 3^n
Who is better off for using the affine cipher?

$\phi(2^n) = 2^{n-1}$. If Vulcans pick an element of $\{1, \ldots, 2^n\}$ at random then prob that its rel prime to 2^n is $\frac{2^{n-1}}{2^n} = 0.5$.
$\phi(3^n) = 2 \times 3^{n-1}$. If Klingons pick an element of $\{1, \ldots, 3^n\}$ at random then prob that its rel prime to 3^n is $\frac{2 \times 3^{n-1}}{3^n} \sim 0.66$.

So Klingons better off.

Problem Two, Part b

Fill in the following sentence:
It is easier to use the affine cipher if the number of letters in the alphabet is XXXX because XXXX.

ANSWER:
It is easier to use the affine cipher if the number of letters in the alphabet is PRIME because ALL VALUES OF a in $\{1, \ldots, |\Sigma| - 1\}$ are fine to use.

PROBLEM THREE SETUP

Alice and Eve play the game where

Alice randomly chooses to send Eve either (1) a perm generated by a random 7-letter keyword and a shift OR (2) a truly random perm.

Eve tries to figure out which one.

In this problem we give Eve a strategy.

If Alice picks keyword-shift then the encoding table will ALWAYS have three consecutive letters in consecutive positions in the second row.

PROBLEM THREE-a ANSWER

a) Give an upper bound on how many perms of $\{a, \ldots, z\}$ have three consecutive letters in them? (It cannot be trivial or later problems will be harder.)

ANSWER: We form the perm by first picking the first letter in the set of three. We can do that 26 ways. Say its p. Then we place p, q, r where p is the first, second, ..., or 26th letter. We can do that 26 ways. Then the remaining 23 letters are permuted an placed around p, q, r. So there are

$$\leq 26 \times 26 \times 23! \text{ such perms.}$$

PROBLEM THREE-b ANSWER

b) Obtain an upper bound on the probability that a randomly chosen perm has three consecutive letters in them? Your bound has to be < 1. Express as a fraction in lowest terms, but also give an approximation in decimal.

ANSWER: Using the last part the bound is

$$\frac{26^2 \times 23!}{26!} = \frac{26^2}{26 \times 25 \times 24} = \frac{26}{25 \times 24} = \frac{13}{300} \sim 0.04333$$

PROBLEM THREE-c SETUP

c) Alice and Eve are playing that really fun game where Alice randomly chooses to send Eve a perm generated by a random 7-letter keyword and a shift OR a truly random perm, and Eve tries to figure out which one.

Here is Eve's strategy: if the perm she gets has three consecutive letters then she'll guess it comes from Keyword-shift, otherwise rand perm.

PROBLEM THREE-c ANSWER

- Bound prob Alice chose a k-shift cipher AND Eve got it wrong. ANSWER: Prob Alice chose a keyword-shift is $\frac{1}{2}$. Prob Eve wrong is 0 since a k-shift ALWAYS has 3 consecutive.
- Bound prob Alice chose r-perms AND Eve got it wrong. ANSWER: Prob Alice chose r-perm is $\frac{1}{2}$. Prob Eve wrong is prob a r-perm had 3 consecutive in a row: $\frac{13}{300}$. Prob both happen is

$$\frac{13}{300} \times \frac{1}{2} = \frac{13}{600} \sim 0.021666$$

- Bound Prob that Eve is wrong. ANSWER This is the sum of the two prior answers, so $\frac{13}{600} = \sim 0.021666$.

PROBLEM THREE: A Better Strategy by Andrew Frock

ALL of the information on the slides on this strategy are due to Andrew Frock.

If k-shift is used then the letters that are NOT the keyword are an increasing sequence (perhaps wrapped around)
Example: Keyword ANDREWF, shift 4 then the cipher's bottom row is

V X Y Z A N D R E W F B C G H I J K L M O P Q S T U

Notice the part after A N D R E W F and wrap it around:

F B C G H I J K L M O P Q S T U V X Y Z

It IS 19 letters increasing.

Eve's Strategy

1. If Eve sees 19 consecutive letters (include wrap-around) that are increasing then guess Keyword Shift. (She might still be wrong.)
2. If Eve does not sees 19 consecutive letters (include wrap-around) that are increasing then guess Rand Perm. (She will always be right.)

Bound Prob that Eve is Wrong

Bound Prob Eve is wrong with

(Prob that it is rand perm)$\times$(Prob that a random perm has a 19-inc-seq)

(Prob that it is rand perm)$= \frac{1}{2}$

Need

Prob that a random perm has a 19-inc-seq

Bound Prob that Eve is Wrong. Cont

Prob that a random perm has a 19-inc-seq

Need bound on the number of perms that have a 19-inc-seq.

Pick the 19 elements: $\binom{26}{19}$.
Pick where seq will start: 26 (because of wrap-around)
Permute the 7 left: 7!

So number of ways is

$$\binom{26}{19} \times 26 \times 7!$$

Bound Prob that Eve is Wrong. Almost Done

Prob that a random perm has a 19-inc-seq
is

$$\frac{1}{2}\frac{\binom{26}{19} \times 26 \times 7!}{26!} \sim 10^{-16}$$

Bound Prob that Eve is Wrong. Almost Done

Prob that a random perm has a 19-inc-seq
is

$$\frac{1}{2}\frac{\binom{26}{19} \times 26 \times 7!}{26!} \sim 10^{-16}$$

I would bet on Eve! But one caveat on the next slide.

Bound Prob that Eve is Wrong. Done!

Eve's strategy works!

But how long does it take? We want Eve to NOT brute force.
Problem: Given a perm of $\{0, \ldots, 25\}$ determine if there 19 consecutive numbers (counting wrap around) that are increasing.
Discuss how to solve fast.

Bound Prob that Eve is Wrong. Done!

Eve's strategy works!

But how long does it take? We want Eve to NOT brute force.
Problem: Given a perm of $\{0, \ldots, 25\}$ determine if there 19 consecutive numbers (counting wrap around) that are increasing.
Discuss how to solve fast.
Idea One: For all i see if beginning at i works. Takes 26×19 steps. Good Enough. Can we do better?

Bound Prob that Eve is Wrong. Done!

Eve's strategy works!

But how long does it take? We want Eve to NOT brute force.
Problem: Given a perm of $\{0, \ldots, 25\}$ determine if there 19 consecutive numbers (counting wrap around) that are increasing. Discuss how to solve fast.
Idea One: For all i see if beginning at i works. Takes 26×19 steps. Good Enough. Can we do better?
Idea Two: Scan the list looking at every pair (σ_i, σ_{i+1}). If $\sigma_i < \sigma_{i+1}$. If so then write a 1, else write a 0 (26 steps). Need to know if there are 19 1's in a row. Scan sequence keeping track of how many 1's in a row, starting back at 0 when you see a 0. (26 steps). So 2×26.

Bound Prob that Eve is Wrong. Done!

Eve's strategy works!

But how long does it take? We want Eve to NOT brute force.
Problem: Given a perm of $\{0, \ldots, 25\}$ determine if there 19 consecutive numbers (counting wrap around) that are increasing. Discuss how to solve fast.
Idea One: For all i see if beginning at i works. Takes 26×19 steps. Good Enough. Can we do better?
Idea Two: Scan the list looking at every pair (σ_i, σ_{i+1}). If $\sigma_i < \sigma_{i+1}$. If so then write a 1, else write a 0 (26 steps). Need to know if there are 19 1's in a row. Scan sequence keeping track of how many 1's in a row, starting back at 0 when you see a 0. (26 steps). So 2×26.
More Interesting Problem this Inspires: Given a sequence of n numbers is there a set of k consecutive numbers that are increasing (count wrap around).
Idea One: would take $O(kn)$ steps.
Idea Two: would take $O(n)$ steps.

PROBLEM FOUR

Programming assignment.
Not going to do that on the slides.

PROBLEM FIVE

Alice and Bob us Vig cipher with keyword justin. Alice sends

Bill's course on Ramsey Theory this spring will be awesome!

ANS: I used `https://www.dcode.fr/vigenere-cipher` to get:

Kcde'a pxojlm bw Lsfarh Nzxweh nzba fylago jrfd um nfykhur!

This leaks LOTS of information: Spacing, Punctuation, Cap letters.

The point of this problem is that many of the online available ciphers are awful for security.

Why do they do that? Discuss.

Finding Inverse Mod n

September 16, 2019

Greatest Common Divisor (GCD)

$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.
Examples
$\mathrm{GCD}(10, 15) =$

Greatest Common Divisor (GCD)

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

Greatest Common Divisor (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)

$\mathrm{GCD}(m, n)$ is the largest number that divides m AND n.
Examples
$\mathrm{GCD}(10, 15) = 5$
$\mathrm{GCD}(11, 15) = 1$

Greatest Common Divisor (GCD)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

$\mathrm{GCD}(m, n)$ 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)

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

Examples

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

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

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

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

$\mathrm{GCD}(14, 15) = 1$

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

$\mathrm{GCD}(15, 24) = 3$

$\mathrm{GCD}(15, 25) = 5$

$\mathrm{GCD}(15, 30) = 15$

$\mathrm{GCD}(15, 0) = 15$

$\mathrm{GCD}(404, 192)$ **The Long Way**

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

$\mathrm{GCD}(404, 192)$ **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 $404 - 192 = 212$.

$\mathrm{GCD}(404, 192)$ 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:

$$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192 = 212, 192)$$

$$= \mathrm{GCD}(212 - 192 = 20, 192) = \mathrm{GCD}(20, 192 - 20 = 172).$$

$\mathrm{GCD}(404, 192)$ 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:

$$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192 = 212, 192)$$

$$= \mathrm{GCD}(212 - 192 = 20, 192) = \mathrm{GCD}(20, 192 - 20 = 172).$$

Could keep going, but will be subtracting 20's for a while.

Idea: Subtract LOTS of 20's.

$\mathrm{GCD}(404, 192)$ 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:

$$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192 = 212, 192)$$

$$= \mathrm{GCD}(212 - 192 = 20, 192) = \mathrm{GCD}(20, 192 - 20 = 172).$$

Could keep going, but will be subtracting 20's for a while.

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

$\mathrm{GCD}(404, 192)$ 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:

$$\mathrm{GCD}(404, 192) = \mathrm{GCD}(404 - 192 = 212, 192)$$

$$= \mathrm{GCD}(212 - 192 = 20, 192) = \mathrm{GCD}(20, 192 - 20 = 172).$$

Could keep going, but will be subtracting 20's for a while.
Idea: Subtract LOTS of 20's.Largest x:$192 - 20x \geq 0$, $x = 9$.

$$= \mathrm{GCD}(20, 192 - 20 \times 9 = 12) = \mathrm{GCD}(20 - 12, 12) = \mathrm{GCD}(8, 12)$$

$$= \mathrm{GCD}(8, 12 - 8 = 4) = \mathrm{GCD}(8 - 2 \times 4, 4) = \mathrm{GCD}(0, 4) = 4.$$

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

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

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

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

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

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

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

$404 = 2 \times 192 + 20$
$192 = 9 \times 20 + 12$
$20 = 1 \times 12 + 8$
$12 = 1 \times 8 + 4$ (AH- 4 is the answer).

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

$404 = 2 \times 192 + 20$

$192 = 9 \times 20 + 12$

$20 = 1 \times 12 + 8$

$12 = 1 \times 8 + 4$ (AH- 4 is the answer).

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

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

$404 = 2 \times 192 + 20$

$192 = 9 \times 20 + 12$

$20 = 1 \times 12 + 8$

$12 = 1 \times 8 + 4$ (AH- 4 is the answer).

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

Write 4 as a combo of 12's and 8's:

$4 = 12 - 1 \times 8$

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

$404 = 2 \times 192 + 20$

$192 = 9 \times 20 + 12$

$20 = 1 \times 12 + 8$

$12 = 1 \times 8 + 4$ (AH- 4 is the answer).

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:

$4 = 12 - 1 \times (20 - 12) = 2 \times 12 - 1 \times 20$

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

$404 = 2 \times 192 + 20$

$192 = 9 \times 20 + 12$

$20 = 1 \times 12 + 8$

$12 = 1 \times 8 + 4$ (AH- 4 is the answer).

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:

$4 = 2 \times (192 - 9 \times 20) - 1 \times 20 = 2 \times 192 - 19 \times 20$

$\mathrm{GCD}(404, 192)$ The Short Way and More Info

$404 = 2 \times 192 + 20$

$192 = 9 \times 20 + 12$

$20 = 1 \times 12 + 8$

$12 = 1 \times 8 + 4$ (AH- 4 is the answer).

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

And now a more interesting case: $\mathrm{GCD}(38, 101)$

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

And now a more interesting case: $\mathrm{GCD}(38, 101)$

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

And now a more interesting case: $\mathrm{GCD}(38, 101)$

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

And now a more interesting case: $\mathrm{GCD}(38, 101)$

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$ GREAT - 1 is GCD.

And now a more interesting case: $\mathrm{GCD}(38, 101)$

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$ GREAT - 1 is GCD.

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

And now a more interesting case: $\mathrm{GCD}(38, 101)$

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$ GREAT - 1 is GCD.

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

And now a more interesting case: $\mathrm{GCD}(38, 101)$

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$ GREAT - 1 is GCD.

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

And now a more interesting case: $\mathrm{GCD}(38, 101)$

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$ GREAT - 1 is 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?

And now a more interesting case: $\mathrm{GCD}(38, 101)$

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$ GREAT - 1 is 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
$1 = 8 \times 38 \pmod{101}$

And now a more interesting case: $\mathrm{GCD}(38, 101)$

$101 = 2 \times 38 + 25$
$38 = 1 \times 25 + 13$
$25 = 1 \times 13 + 12$
$13 = 12 + 1$ GREAT - 1 is 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
$1 = 8 \times 38 \pmod{101}$
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

- 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.
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 y.

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 y. 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 y. Not quite: (1) a might be negative (2) a might be $> n$. That won't do! Take $a \pmod{n}$.