CS 170: Algorithms

Account forms now or after class!

CS 170: Algorithms

Account forms now or after class!

Static Course Webpage. (inst.cs.berkeley.edu/~cs170)

CS 170: Algorithms

Account forms now or after class!

Static Course Webpage. (inst.cs.berkeley.edu/~cs170)

Watching piazza yet?

CS 170: Algorithms

Account forms now or after class!

Static Course Webpage. (inst.cs.berkeley.edu/~cs170)

Watching piazza yet?

Did you find a scanner, yet?

Modular Arithmetic.

n-bit numbers x, y, z.

Modular Arithmetic.

n-bit numbers x, y, z. Addition: $O(n)$
Multiplication: $O(n^2)$
Modular Exponentiation: $O(n^3)$

Modular Arithmetic.

n-bit numbers x, y, z. Addition: $O(n)$
Multiplication: $O(n^2)$
Modular Exponentiation: $O(n^3)$
Division.

Modular Arithmetic.

n-bit numbers x, y, z. Addition: $O(n)$
Multiplication: $O(n^2)$
Modular Exponentiation: $O(n^3)$
Division. Multiplicative inverse of x mod N?

Modular Arithmetic.

n-bit numbers x, y, z. Addition: $O(n)$
Multiplication: $O(n^2)$
Modular Exponentiation: $O(n^3)$
Division. Multiplicative inverse of x mod N?
Find a, where $ax = 1 \pmod N$.

Is there an inverse?

Inverse of $4 \pmod 6$?

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

Is there an inverse?

Inverse of $4 \pmod{6}$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Thm: $gcd(x, y) = d \rightarrow$ no inverse.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Thm: $gcd(x, y) = d \rightarrow$ no inverse.

Proof:

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Thm: $gcd(x, y) = d \rightarrow$ no inverse.

Proof: $ax = 1 \pmod y$ "$\equiv$"

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Thm: $gcd(x, y) = d \rightarrow$ no inverse.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq 1$ implies no inverse.

Thm: $gcd(x, y) = d \rightarrow$ no inverse.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$.

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Thm: $gcd(x, y) = d \rightarrow$ no inverse.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$.

$x = id, y = jd$

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Thm: $gcd(x,y) = d \rightarrow$ no inverse.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$.

$x = id, y = jd$

$a(id) - b(jd) = 1 \rightarrow d(ia - jd) = 1$.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Thm: $gcd(x, y) = d \rightarrow$ no inverse.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$.

$x = id, y = jd$

$a(id) - b(jd) = 1 \rightarrow d(ia - jd) = 1$.

d must be a factor of 1.

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Thm: $gcd(x,y) = d \rightarrow$ no inverse.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$.

$x = id, y = jd$

$a(id) - b(jd) = 1 \rightarrow d(ia - jd) = 1$.

d must be a factor of 1. That is, $d = 1$. $\square$

Is there an inverse?

Inverse of $4 \pmod{6}$?

Is there an inverse?

Inverse of $4 \pmod{6}$?

No!

Is there an inverse?

Inverse of $4 \pmod{6}$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

Is there an inverse?

Inverse of $4 \pmod{6}$?

No!

> $4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Theorem:
$gcd(x, y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Theorem:
$gcd(x,y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof:

Is there an inverse?

Inverse of $4 \pmod{6}$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq 1$ implies no inverse.

Theorem:
$gcd(x, y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof: $ax = 1 \pmod{y}$ "$\equiv$"

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq 1$ implies no inverse.

Theorem:
$gcd(x, y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq 1$ implies no inverse.

Theorem:
$gcd(x, y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$.

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq 1$ implies no inverse.

Theorem:
$gcd(x,y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$. $x = id, y = jd$ since d divides both.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq 1$ implies no inverse.

Theorem:
$gcd(x,y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$. $x = id, y = jd$ since d divides both.

$a(id) - b(jd) = 1 \rightarrow d(ia - jb) = 1$.

Is there an inverse?

Inverse of $4 \pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq 1$ implies no inverse.

Theorem:
$gcd(x,y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$. $x = id, y = jd$ since d divides both.

$a(id) - b(jd) = 1 \rightarrow d(ia - jb) = 1$.

d must be a factor of 1.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq 1$ implies no inverse.

Theorem:
$gcd(x, y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$. $x = id, y = jd$ since d divides both.

$a(id) - b(jd) = 1 \rightarrow d(ia - jb) = 1$.

d must be a factor of 1. That is, $d = 1$.

Is there an inverse?

Inverse of 4 $\pmod 6$?

No!

$4j$ is at least 2 away from $6k$ for any j, k.

They have a common divisor that is greater than 1.

gcd(x,y) - greatest common divisor of x and y.

gcd(x,y) $\neq$ 1 implies no inverse.

Theorem:
$gcd(x, y) = d$, $d \geq 1 \rightarrow x$ has no multiplicative inverse modulo y.

Proof: $ax = 1 \pmod y$ "$\equiv$" $ax = 1 + by$ for integer b

$ax - by = 1$. $x = id, y = jd$ since d divides both.

$a(id) - b(jd) = 1 \rightarrow d(ia - jb) = 1$.

d must be a factor of 1. That is, $d = 1$. $\square$

Review: extended euclid's algorithm and inverses.

Extended GCD:

Review: extended euclid's algorithm and inverses.

Extended GCD:

Given x, y.

Review: extended euclid's algorithm and inverses.

Extended GCD:

Given x, y.
Returns: (d, a, b) where $ax + by = d$, and $d = gcd(x, y)$

Review: extended euclid's algorithm and inverses.

Extended GCD:

Given x, y.
Returns: (d, a, b) where $ax + by = d$, and $d = gcd(x, y)$

Find inverse of x modulo N, if $gcd(x, N) = 1$?

Review: extended euclid's algorithm and inverses.

Extended GCD:

Given x, y.
Returns: (d, a, b) where $ax + by = d$, and $d = gcd(x, y)$

Find inverse of x modulo N, if $gcd(x, N) = 1$?

(A) Run Euclid on x, N, output a.

(B) Run Euclid on x, N, output b.

Review: extended euclid's algorithm and inverses.

Extended GCD:

Given x, y.
Returns: (d, a, b) where $ax + by = d$, and $d = gcd(x, y)$

Find inverse of x modulo N, if $gcd(x, N) = 1$?

(A) Run Euclid on x, N, output a.

(B) Run Euclid on x, N, output b.

A. $1 = ax + bN$

Review: extended euclid's algorithm and inverses.

Extended GCD:

Given x, y.
Returns: (d, a, b) where $ax + by = d$, and $d = gcd(x, y)$

Find inverse of x modulo N, if $gcd(x, N) = 1$?

(A) Run Euclid on x, N, output a.

(B) Run Euclid on x, N, output b.

A. $1 = ax + bN = ax \pmod{N}$,

Review: extended euclid's algorithm and inverses.

Extended GCD:

Given x, y.
Returns: (d, a, b) where $ax + by = d$, and $d = gcd(x, y)$

Find inverse of x modulo N, if $gcd(x, N) = 1$?

(A) Run Euclid on x, N, output a.

(B) Run Euclid on x, N, output b.

A. $1 = ax + bN = ax \pmod{N}$,
so a is multiplicative inverse of x modulo N.

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d, a, b); d = ax + by$.

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d, a, b); d = ax + by$.

$x =$ __________

$y =$ ____

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d,a,b); d = ax + by$.

$x =$__________

$y =$____

Get "close" to y with x's:

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d,a,b); d = ax + by$.

$x =$__________

$y =$____

Get "close" to y with x's:

$kx =$____

$y =$ ____

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d,a,b); d = ax + by$.

$x =$__________

$y =$____

Get "close" to y with x's:

$kx =$____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d, a, b); d = ax + by$.

$x =$ __________

$y =$ ____

Get "close" to y with x's:

$kx =$ ____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d,a,b); d = ax + by$.

$x =$ ________

$y =$ ____

Get "close" to y with x's:

$kx =$ ____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d, a, b); d = ax + by$.

$x =$__________

$y =$____

Get “close” to y with x’s:

$kx =$____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d,a,b); d = ax + by$.

$x =$ ________

$y =$ ____

Get "close" to y with x's:

$kx =$ ____________________________________

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x
$d|x$ and $d|(y - kx)$

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d,a,b); d = ax + by$.

$x =$__________

$y =$____

Get “close” to y with x’s:

$kx =$____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x
$d|x$ and $d|(y - kx)$ Also $d'|x$ and $d'|(y - kx)$

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d, a, b); d = ax + by$.

$x =$_________

$y =$____

Get “close” to y with x’s:

$kx =$____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x
$d|x$ and $d|(y - kx)$ Also $d'|x$ and $d'|(y - kx) \implies d'|y$.

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d,a,b); d = ax + by$.

$x =$ ________

$y =$ ____

Get "close" to y with x's:

$kx =$ ______________________________________

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x
$d|x$ and $d|(y - kx)$ Also $d'|x$ and $d'|(y - kx) \implies d'|y$.
$\rightarrow gcd(x,y) = gcd(x, y - kx)$.

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d, a, b); d = ax + by$.

$x =$ __________

$y =$ ____

Get "close" to y with x's:

$kx =$ ____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x
$d|x$ and $d|(y - kx)$ Also $d'|x$ and $d'|(y - kx) \implies d'|y$.
$\rightarrow gcd(x, y) = gcd(x, y - kx)$.

Get (d, a', b') where $d = a'(y - kx) + b'x$

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d,a,b); d = ax + by$.

$x =$_________

$y =$____

Get "close" to y with x's:

$kx =$____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x
$d|x$ and $d|(y - kx)$ Also $d'|x$ and $d'|(y - kx) \implies d'|y$.
$\rightarrow gcd(x,y) = gcd(x, y - kx)$.

Get (d, a', b') where $d = a'(y - kx) + b'x = (b' - ka')x + a'y$.

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d, a, b); d = ax + by$.

$x =$ __________

$y =$ ____

Get "close" to y with x's:

$kx =$ ____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!

Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x

$d|x$ and $d|(y - kx)$ Also $d'|x$ and $d'|(y - kx) \implies d'|y$.

$\rightarrow gcd(x, y) = gcd(x, y - kx)$.

Get (d, a', b') where $d = a'(y - kx) + b'x = (b' - ka')x + a'y$.

Return $(d, b' - ka', a')$.

Extended Euclid/Correctness.

Ext-gcd(x,y): $(d, a, b); d = ax + by$.

$x =$ __________

$y =$ ____

Get "close" to y with x's:

$kx =$ ____

$y =$ ____

$k = \lfloor y/x \rfloor$ (Use long division.) (Time: $O(n^2)$ time.)

$(y - kx)$ preserves common divisor!
Anything that divides both x and y, divides $(y - kx)$

Recurse for $y - kx$ and x
$d|x$ and $d|(y - kx)$ Also $d'|x$ and $d'|(y - kx) \implies d'|y$.
$\rightarrow gcd(x, y) = gcd(x, y - kx)$.

Get (d, a', b') where $d = a'(y - kx) + b'x = (b' - ka')x + a'y$.

Return $(d, b' - ka', a')$.
Time for one recursive call: $O(n^2)$.

Complexity

Time is $O(L) \times O(n^2)$ where L is depth.

Complexity

Time is $O(L) \times O(n^2)$ where L is depth.

What is recursion depth?

Depth of recursion.

Original inputs:

Depth of recursion.

Original inputs:

$x =$ __________

$y =$ ____

Depth of recursion.

Original inputs:

$x =$___________

$y =$____

Recurse on

Depth of recursion.

Original inputs:

$x =$ __________

$y =$ ____

Recurse on

$$y - kx = \quad \_\_\_\_\_\_$$
$$x = \quad \_\_\_\_\_\_\_\_\_\_$$

Depth of recursion.

Original inputs:

$x =$__________

$y =$____

Recurse on

$$y - kx = \quad \_\_\_\_\_$$
$$x = \quad \_\_\_\_\_\_\_\_\_\_$$

$y - kx$ is at most half of y.

Depth of recursion.

Original inputs:

$x =$ _________

$y =$ ____

Recurse on

$$y - kx = \quad \_\_\_\_\_$$
$$x = \quad \_\_\_\_\_\_\_\_\_$$

$y - kx$ is at most half of y. And $x > y - kx$.

Depth of recursion.

Original inputs:

$x =$ _________

$y =$ ____

Recurse on

$$\begin{aligned} y - kx &= \quad \underline{\hspace{2cm}} \\ x &= \quad \underline{\hspace{3.5cm}} \end{aligned}$$

$y - kx$ is at most half of y. And $x > y - kx$.

Next recursion:

Depth of recursion.

Original inputs:

$x =$ __________

$y =$ ____

Recurse on

$$y - kx = \quad \_\_\_\_\_\_$$

$$x = \quad \_\_\_\_\_\_\_\_\_\_$$

$y - kx$ is at most half of y. And $x > y - kx$.

Next recursion:

$$x - (y - kx) = \quad \_\_\_\_\_$$

$$y - kx = \quad \_\_\_\_\_\_$$

Depth of recursion.

Original inputs:

$x =$ __________

$y =$ ____

Recurse on

$$y - kx = \_\_\_\_\_$$
$$x = \_\_\_\_\_\_\_\_\_\_$$

$y - kx$ is at most half of y. And $x > y - kx$.

Next recursion:

$$x - (y - kx) = \_\_\_\_$$
$$y - kx = \_\_\_\_\_$$

$x - (y - kx)$ is at most half of x.

Depth of recursion.

Original inputs:

$x =$ ________

$y =$ ____

Recurse on

$$y - kx = \quad \underline{\hspace{2cm}}$$
$$x = \quad \underline{\hspace{3cm}}$$

$y - kx$ is at most half of y. And $x > y - kx$.

Next recursion:

$$x - (y - kx) = \quad \underline{\hspace{1.5cm}}$$
$$y - kx = \quad \underline{\hspace{2cm}}$$

$x - (y - kx)$ is at most half of x.

Every 2 recursive calls:

Depth of recursion.

Original inputs:

$x =$ __________

$y =$ ____

Recurse on

$$y - kx = \quad \_\_\_\_\_$$
$$x = \quad \_\_\_\_\_\_\_\_\_\_$$

$y - kx$ is at most half of y. And $x > y - kx$.

Next recursion:

$$x - (y - kx) = \quad \_\_\_\_$$
$$y - kx = \quad \_\_\_\_\_$$

$x - (y - kx)$ is at most half of x.

Every 2 recursive calls: both arguments halve in value -

Depth of recursion.

Original inputs:

$x =$ ________

$y =$ ____

Recurse on

$$y - kx = \quad \_\_\_\_\_$$
$$x = \quad \_\_\_\_\_\_\_\_\_$$

$y - kx$ is at most half of y. And $x > y - kx$.

Next recursion:

$$x - (y - kx) = \quad \_\_\_\_$$
$$y - kx = \quad \_\_\_\_\_$$

$x - (y - kx)$ is at most half of x.

Every 2 recursive calls: both arguments halve in value -
get shorter by one bit.

Depth of recursion.

Original inputs:

$x =$ _________

$y =$ ____

Recurse on

$$y - kx = \quad \_\_\_\_\_$$
$$x = \quad \_\_\_\_\_\_\_\_\_$$

$y - kx$ is at most half of y. And $x > y - kx$.

Next recursion:

$$x - (y - kx) = \quad \_\_\_\_$$
$$y - kx = \quad \_\_\_\_\_$$

$x - (y - kx)$ is at most half of x.

Every 2 recursive calls: both arguments halve in value - get shorter by one bit.

Depth is less than $2n$

Depth of recursion.

Original inputs:

$x =$ __________

$y =$ ____

Recurse on

$$y - kx = \quad \_\_\_\_\_$$
$$x = \quad \_\_\_\_\_\_\_\_\_\_$$

$y - kx$ is at most half of y. And $x > y - kx$.

Next recursion:

$$x - (y - kx) = \quad \_\_\_\_$$
$$y - kx = \quad \_\_\_\_\_$$

$x - (y - kx)$ is at most half of x.

Every 2 recursive calls: both arguments halve in value - get shorter by one bit.

Depth is less than $2n$ where n is number of bits.

Complexity

Time is $O(L) \times O(n^2)$ where L is depth.

Complexity

Time is $O(L) \times O(n^2)$ where L is depth.

$L = O(n)$.

Complexity

Time is $O(L) \times O(n^2)$ where L is depth.

$L = O(n)$.

Time: $O(n^3)$.

Modular arithmetic operations.

Addition: $O(n)$
Multiplication: $O(n^2)$
Modular Exponentiation: $O(n^3)$
Modular Division: $O(n^3)$.

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reduce exponents?

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reduce exponents?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reduce exponents?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

What is $3^{25} \pmod{7}$?

(A) 2

(B) 3

(C) 4

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reduce exponents?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

What is $3^{25} \pmod{7}$?

(A) 2

(B) 3

(C) 4

3^{25}

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reduce exponents?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

What is $3^{25} \pmod{7}$?

(A) 2

(B) 3

(C) 4

$3^{25} = 3 \times 3^{24}$

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reduce exponents?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

What is $3^{25} \pmod{7}$?

(A) 2

(B) 3

(C) 4

$3^{25} = 3 \times 3^{24} = 3 \times (3^6)^4$

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reduce exponents?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

What is $3^{25} \pmod{7}$?

(A) 2

(B) 3

(C) 4

$3^{25} = 3 \times 3^{24} = 3 \times (3^6)^4 = 3 \times (1)^4 \pmod{7}$

Reducing Exponents.

Recall: $x \times y \times u \times v \times w \cdots \pmod{z}$.

Reduce each intermediate result $\pmod{z}$!

Reduce exponents?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

What is $3^{25} \pmod{7}$?

(A) 2

(B) 3

(C) 4

$3^{25} = 3 \times 3^{24} = 3 \times (3^6)^4 = 3 \times (1)^4 \pmod{7}$

B. 3

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod p$.

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Idea: Multiply nonzero elements of Z_p ($\{0, \ldots, p-1\}$) together!

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod p$.

Idea: Multiply nonzero elements of Z_p ($\{0,\ldots,p-1\}$) together!

More details:

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Idea: Multiply nonzero elements of Z_p ($\{0, \ldots, p-1\}$) together!

More details:
Let T be $\{1, \ldots, p-1\}$.

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Idea: Multiply nonzero elements of Z_p ($\{0, \ldots, p-1\}$) together!

More details:
Let T be $\{1, \ldots, p-1\}$.
Let S be $\{ax : x \in T\}$.

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Idea: Multiply nonzero elements of Z_p ($\{0, \ldots, p-1\}$) together!

More details:
Let T be $\{1, \ldots, p-1\}$.
Let S be $\{ax : x \in T\}$.
How big is S?

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Idea: Multiply nonzero elements of Z_p ($\{0, \ldots, p-1\}$) together!

More details:
Let T be $\{1, \ldots, p-1\}$.
Let S be $\{ax : x \in T\}$.
How big is S?
Are S and T related?

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Idea: Multiply nonzero elements of Z_p ($\{0, \ldots, p-1\}$) together!

More details:
Let T be $\{1, \ldots, p-1\}$.
Let S be $\{ax : x \in T\}$.
How big is S?
Are S and T related?

Proof?

Fermat's Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Idea: Multiply nonzero elements of Z_p ($\{0, \ldots, p-1\}$) together!

More details:
Let T be $\{1, \ldots, p-1\}$.
Let S be $\{ax : x \in T\}$.
How big is S?
Are S and T related?

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.

Proof:

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1,\ldots,p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes?

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes? No?

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes? No?

Recall a has multiplicative inverse. ($gcd(a, p) = 1$)

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes? No?

Recall a has multiplicative inverse. ($gcd(a,p) = 1$)

$$ax = ay \pmod{z}$$

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1,\ldots,p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes? No?

Recall a has multiplicative inverse. ($gcd(a,p) = 1$)

$$\begin{aligned} ax &= ay \pmod{z} \\ a^{-1}ax &= a^{-1}ay \pmod{z} \end{aligned}$$

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes? No?

Recall a has multiplicative inverse. ($gcd(a,p) = 1$)

$$\begin{aligned} ax &= ay \pmod{z} \\ a^{-1}ax &= a^{-1}ay \pmod{z} \\ x &= y \pmod{z} \end{aligned}$$

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes? No?

Recall a has multiplicative inverse. ($gcd(a,p) = 1$)

$$\begin{aligned} ax &= ay \pmod{z} \\ a^{-1}ax &= a^{-1}ay \pmod{z} \\ x &= y \pmod{z} \end{aligned}$$

Thus, $ax = ay \pmod{z} \implies x = y \pmod{z}$.

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes? No?

Recall a has multiplicative inverse. $(gcd(a,p) = 1)$

$$\begin{aligned} ax &= ay \pmod{z} \\ a^{-1}ax &= a^{-1}ay \pmod{z} \\ x &= y \pmod{z} \end{aligned}$$

Thus, $ax = ay \pmod{z} \implies x = y \pmod{z}$.

Thus, mutliply by a is 1-to-1,

Fermat's Theorem.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Let S be $\{ax \pmod{p} : x \in T\}$.
How big is S?

(A) Exactly $p-1$.

(B) Possibly less than $p-1$.

Are there different x and y where $ax = ay \pmod{z}$?

Yes? No?

Recall a has multiplicative inverse. ($gcd(a,p) = 1$)

$$
\begin{aligned}
ax &= ay \pmod{z} \\
a^{-1}ax &= a^{-1}ay \pmod{z} \\
x &= y \pmod{z}
\end{aligned}
$$

Thus, $ax = ay \pmod{z} \implies x = y \pmod{z}$.

Thus, mutliply by a is 1-to-1, and $|S| = p-1$.

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1,\ldots,p-1\}$. (Nonzero elements of Z_p.)

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S?

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T?

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \dots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ...

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Multiply elements of T:

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Multiply elements of T: $\pi_T = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Multiply elements of T: $\pi_T = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$
Multiply elements of S:

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Multiply elements of T: $\pi_T = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$
Multiply elements of S: $\pi_S = 1a \cdot 2a \cdot 3a \cdots (p-1)a \pmod{p}$

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Multiply elements of T: $\pi_T = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$
Multiply elements of S: $\pi_S = 1a \cdot 2a \cdot 3a \cdots (p-1)a \pmod{p}$

$$\pi_S = a^{p-1}\pi_T$$

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Multiply elements of T: $\pi_T = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$
Multiply elements of S: $\pi_S = 1a \cdot 2a \cdot 3a \cdots (p-1)a \pmod{p}$

$$\pi_S = a^{p-1}\pi_T = \pi_T \pmod{p}.$$

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Multiply elements of T: $\pi_T = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$
Multiply elements of S: $\pi_S = 1a \cdot 2a \cdot 3a \cdots (p-1)a \pmod{p}$

$$\pi_S = a^{p-1}\pi_T = \pi_T \pmod{p}.$$

So $a^{p-1} = 1 \pmod{p}$.

Fermat's Theorem: proof, continued.

Thm: For a prime p and $0 < a < p$, $a^{p-1} = 1 \pmod{p}$.
Proof:

Let T be $\{1, \ldots, p-1\}$. (Nonzero elements of Z_p.)
Consider the set $S = \{ax \pmod{p} : x \in T\}$.
How big is S? $p-1$ since a has an inverse
Relationship between S and T? They are ... the same!
Elts of S are in $T = \{1, \ldots, p-1\}$ and set size $p-1$.

Multiply elements of T: $\pi_T = 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$
Multiply elements of S: $\pi_S = 1a \cdot 2a \cdot 3a \cdots (p-1)a \pmod{p}$

$$\pi_S = a^{p-1}\pi_T = \pi_T \pmod{p}.$$

So $a^{p-1} = 1 \pmod{p}$.

$\square$

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones.

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

For 100 digit number,

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

For 100 digit number, one in $\ln 10^{100}$,

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

For 100 digit number, one in $\ln 10^{100}$, around 1 in 200.

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

For 100 digit number, one in $\ln 10^{100}$, around 1 in 200.

Demo.

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

For 100 digit number, one in $\ln 10^{100}$, around 1 in 200.

Demo.

Why was the demo, so fast?

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

For 100 digit number, one in $\ln 10^{100}$, around 1 in 200.

Demo.

Why was the demo, so fast?

How could it tell whether a number was prime?

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

For 100 digit number, one in $\ln 10^{100}$, around 1 in 200.

Demo.

Why was the demo, so fast?

How could it tell whether a number was prime?

Obvious method: check for factors up to $\sqrt{N}$.

Primes, primes, primes..

Arithmetic modulo a prime is so nice!

I want some primes! Big ones. Big is good.

How do I find one?

Are there even any big primes?

There are lots!

Around $\frac{1}{\ln N}$ for numbers with value N.

For 100 digit number, one in $\ln 10^{100}$, around 1 in 200.

Demo.

Why was the demo, so fast?

How could it tell whether a number was prime?

Obvious method: check for factors up to $\sqrt{N}$.
  should take around 10^{50} steps.

Primes.

What is your favorite prime?

Primes.

What is your favorite prime? 7

Primes.

What is your favorite prime? 7 ...of course!

Primes.

What is your favorite prime? 7 ...of course!

What is

$$2^6 \mod 7?$$

(a) 1
(b) 2
(c) 3

Primes.

What is your favorite prime? 7 ...of course!

What is

$$2^6 \mod 7?$$

(a) 1
(b) 2
(c) 3

$2^6 = 64$

Primes.

What is your favorite prime? 7 ...of course!

What is

$$2^6 \mod 7?$$

(a) 1
(b) 2
(c) 3

$2^6 = 64 = 7 * 9 + 1$

Primes.

What is your favorite prime? 7 ...of course!

What is

$$2^6 \mod 7?$$

(a) 1

(b) 2

(c) 3

$2^6 = 64 = 7 * 9 + 1 \equiv 1 \pmod 7)$

Primes.

What is your favorite prime? 7 ...of course!

What is

$$2^6 \mod 7?$$

(a) 1
(b) 2
(c) 3

$2^6 = 64 = 7*9+1 \equiv 1 \pmod 7$

Again!

What about $3^6 \mod 7$?

Again!

What about $3^6 \mod 7$?

(a) 1

(b) 2

(c) 3

Again!

What about $3^6 \mod 7$?

(a) 1
(b) 2
(c) 3

Fermat's Theorem:
If p is prime, and any $0 < a < p$, $a^{p-1} \equiv 1 \pmod{p}$.

Again!

What about $3^6 \mod 7$?

(a) 1
(b) 2
(c) 3

Fermat's Theorem:
If p is prime, and any $0 < a < p$, $a^{p-1} \equiv 1 \pmod{p}$.

Answer is A or 1.

Again!

What about $3^5 \mod 6$?

Again!

What about $3^5 \mod 6$?

(a) 1

(b) 2

(c) 3

Again!

What about $3^5 \mod 6$?

(a) 1

(b) 2

(c) 3

I don't know.

Again!

What about $3^5 \mod 6$?

(a) 1
(b) 2
(c) 3

I don't know. Fermat's Theorem doesn't tell us!

Again!

What about $3^5 \mod 6$?

(a) 1

(b) 2

(c) 3

I don't know. Fermat's Theorem doesn't tell us!
...with some work...

Again!

What about $3^5 \mod 6$?

(a) 1

(b) 2

(c) 3

I don't know. Fermat's Theorem doesn't tell us!
...with some work...it's 3!

Again!

What about $3^5 \mod 6$?

(a) 1
(b) 2
(c) 3

I don't know. Fermat's Theorem doesn't tell us!
...with some work...it's 3! not 1!

Testing primality.

Theorem: For any non prime N, except for "Carmichael" numbers (ridiculously rare), for at least half the $0 < a < N$,

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

Testing primality.

Theorem: For any non prime N, except for "Carmichael" numbers (ridiculously rare), for at least half the $0 < a < N$,

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

Fermat's Theorem:
If p is prime, and any $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Testing primality.

Theorem: For any non prime N, except for "Carmichael" numbers (ridiculously rare), for at least half the $0 < a < N$,

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

Fermat's Theorem:
If p is prime, and any $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Approximate converse of Fermat's Theorem.

Testing primality.

Theorem: For any non prime N, except for "Carmichael" numbers (ridiculously rare), for at least half the $0 < a < N$,

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

Fermat's Theorem:
If p is prime, and any $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Approximate converse of Fermat's Theorem.
Not exact

Testing primality.

Theorem: For any non prime N, except for "Carmichael" numbers (ridiculously rare), for at least half the $0 < a < N$,

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

Fermat's Theorem:
If p is prime, and any $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Approximate converse of Fermat's Theorem.
Not exact
because "test" fails for only half the a's.

Testing primality.

Theorem: For any non prime N, except for "Carmichael" numbers (ridiculously rare), for at least half the $0 < a < N$,

$$a^{N-1} \not\equiv 1 \pmod{N}.$$

Fermat's Theorem:
If p is prime, and any $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Approximate converse of Fermat's Theorem.
Not exact
because "test" fails for only half the a's.
and rare exceptions.

Some questions....

Some questions....

Given N, and a, where $a^{N-1} = 1 \pmod{N}$, is N prime?

Some questions....

Given N, and a, where $a^{N-1} = 1 \pmod{N}$, is N prime?

1. Yes. Prime!
2. No. Not prime!
3. It could be prime or composite.

Some questions....

Given N, and a, where $a^{N-1} = 1 \pmod{N}$, is N prime?

1. Yes. Prime!
2. No. Not prime!
3. It could be prime or composite.

C. It could be prime or composite.

Questions.

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, is N prime?

Questions.

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, is N prime?

(A) Yes. It is prime.

(B) No. It is not prime.

(C) It could be prime or composite.

Questions.

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod N$, is N prime?

(A) Yes. It is prime.
(B) No. It is not prime.
(C) It could be prime or composite.

B. No. Not Prime!

Questions.

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod N$, is N prime?

(A) Yes. It is prime.
(B) No. It is not prime.
(C) It could be prime or composite.

B. No. Not Prime!

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod N$, it is easy to factor N.

Questions.

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, is N prime?

(A) Yes. It is prime.
(B) No. It is not prime.
(C) It could be prime or composite.

B. No. Not Prime!

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, it is easy to factor N.

(A) Yes.
(B) No.

Questions.

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, is N prime?

(A) Yes. It is prime.
(B) No. It is not prime.
(C) It could be prime or composite.

B. No. Not Prime!

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, it is easy to factor N.

(A) Yes.
(B) No.
(C) We rely on not knowing how!

Questions.

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, is N prime?

(A) Yes. It is prime.
(B) No. It is not prime.
(C) It could be prime or composite.

B. No. Not Prime!

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, it is easy to factor N.

(A) Yes.
(B) No.
(C) We rely on not knowing how!

C.

Questions.

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, is N prime?

(A) Yes. It is prime.
(B) No. It is not prime.
(C) It could be prime or composite.

B. No. Not Prime!

Given N, and a, where $a^{N-1} \not\equiv 1 \pmod{N}$, it is easy to factor N.

(A) Yes.
(B) No.
(C) We rely on not knowing how!

C. RSA cryptosystem.

Flipping around the theorem..

Flipping around the theorem..

Given N is not prime (and not a Carmichael number), how many $0 < a < N$, where $a^{N-1} \not\equiv 1 \pmod{N}$?

(A) at least one of them.

(B) at least half of them.

(C) all of them.

Flipping around the theorem..

Given N is not prime (and not a Carmichael number), how many $0 < a < N$, where $a^{N-1} \not\equiv 1 \pmod{N}$?

(A) at least one of them.

(B) at least half of them.

(C) all of them.

B

Flipping around the theorem..

Given N is not prime (and not a Carmichael number), how many $0 < a < N$, where $a^{N-1} \not\equiv 1 \pmod{N}$?

(A) at least one of them.

(B) at least half of them.

(C) all of them.

B (and A).

Flipping around the theorem..

Given N is not prime (and not a Carmichael number), how many $0 < a < N$, where $a^{N-1} \not\equiv 1 \pmod{N}$?

(A) at least one of them.

(B) at least half of them.

(C) all of them.

B (and A).

Primality Testing Algorithm?

Flipping around the theorem..

Given N is not prime (and not a Carmichael number), how many $0 < a < N$, where $a^{N-1} \not\equiv 1 \pmod{N}$?

(A) at least one of them.

(B) at least half of them.

(C) all of them.

B (and A).

Primality Testing Algorithm?

Repeat 100 times:

Flipping around the theorem..

Given N is not prime (and not a Carmichael number), how many $0 < a < N$, where $a^{N-1} \not\equiv 1 \pmod{N}$?

(A) at least one of them.

(B) at least half of them.

(C) all of them.

B (and A).

Primality Testing Algorithm?
Repeat 100 times:
Choose a at random and test

Flipping around the theorem..

Given N is not prime (and not a Carmichael number), how many $0 < a < N$, where $a^{N-1} \not\equiv 1 \pmod{N}$?

(A) at least one of them.

(B) at least half of them.

(C) all of them.

B (and A).

Primality Testing Algorithm?

Repeat 100 times:

Choose a at random and test

$$a^{N-1} \equiv 1 \mod N.$$

Primality Testing

```
def primalityOrCarmichael(N):
   for i in xrange(100):
     a = random_int(1,N-1)
     if  not( exp(a,N-1,N) == 1):
        return False
   return True
```

Primality Testing

```
def primalityOrCarmichael(N):
   for i in xrange(100):
     a = random_int(1,N-1)
     if  not( exp(a,N-1,N) == 1):
        return False
   return True
```

Use modular exponentiation.

Primality Testing

```
def primalityOrCarmichael(N):
   for i in xrange(100):
     a = random_int(1,N-1)
     if  not( exp(a,N-1,N) == 1):
        return False
   return True
```

Use modular exponentiation.
If not prime or Carmichael,
  passes test once
    with probability at most 1/2.

Correctness

If return False:

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

N is "prime or Carmichael", then the algorithm is correct.

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

N is "prime or Carmichael", then the algorithm is correct.

N is "not prime (or Carmichael)":

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

N is "prime or Carmichael", then the algorithm is correct.

N is "not prime (or Carmichael)":

Probability of passing test 100 times is

(A) $1/2$

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

N is "prime or Carmichael", then the algorithm is correct.

N is "not prime (or Carmichael)":

Probability of passing test 100 times is

(A) $1/2$

(B) $1/100$

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

N is "prime or Carmichael", then the algorithm is correct.

N is "not prime (or Carmichael)":

Probability of passing test 100 times is

(A) $1/2$

(B) $1/100$

(C) $1/(100)^2$

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

N is "prime or Carmichael", then the algorithm is correct.

N is "not prime (or Carmichael)":

Probability of passing test 100 times is

(A) $1/2$

(B) $1/100$

(C) $1/(100)^2$

(D) $1/2^{100}$

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

N is "prime or Carmichael", then the algorithm is correct.

N is "not prime (or Carmichael)":

Probability of passing test 100 times is

(A) $1/2$

(B) $1/100$

(C) $1/(100)^2$

(D) $1/2^{100}$

D. $1/2^{100}$.

Correctness

If return False:

N not prime by Fermat's Theorem ($a^{N-1} \neq 1 \mod N$).

If return True:

It passes the test 100 times.

N is "prime or Carmichael", then the algorithm is correct.

N is "not prime (or Carmichael)":

Probability of passing test 100 times is

(A) $1/2$

(B) $1/100$

(C) $1/(100)^2$

(D) $1/2^{100}$

D. $1/2^{100}$.

The probability that the algorithm fails is at most $1/2^{100}$.

Probability Review

Probability of t heads in a row, if heads probability is p?

Probability Review

Probability of t heads in a row, if heads probability is p?

Assume each coin toss is independent.

Probability Review

Probability of t heads in a row, if heads probability is p?

Assume each coin toss is independent.

p

Probability Review

Probability of t heads in a row, if heads probability is p?

Assume each coin toss is independent.

$p \times p$

Probability Review

Probability of t heads in a row, if heads probability is p?

Assume each coin toss is independent.

$p \times p \times p \cdots$

Probability Review

Probability of t heads in a row, if heads probability is p?

Assume each coin toss is independent.

$p \times p \times p \cdots = (p)^{100}$.

Probability Review

Probability of t heads in a row, if heads probability is p?

Assume each coin toss is independent.

$p \times p \times p \cdots = (p)^{100}$.

For algorithm, test fails on nonprime/nonCarmichael with $p \leq 1/2$.

Probability Review

Probability of t heads in a row, if heads probability is p?

Assume each coin toss is independent.

$p \times p \times p \cdots = (p)^{100}$.

For algorithm, test fails on nonprime/nonCarmichael with $p \leq 1/2$.

So, probability of failing $p^{100} \leq \left(\frac{1}{2}\right)^{100}$

Probability Review

Probability of t heads in a row, if heads probability is p?

Assume each coin toss is independent.

$p \times p \times p \cdots = (p)^{100}$.

For algorithm, test fails on nonprime/nonCarmichael with $p \leq 1/2$.

So, probability of failing $p^{100} \leq \left(\frac{1}{2}\right)^{100}$

Tune algorithm: for t tests,
probability fails on nonprime/nonCarmichael
is $\leq \left(\frac{1}{2}\right)^{t}$

...finish lemma Monday.