Proof review. Consequence.

Thm: If \( \gcd(x, m) = 1 \), then \( x \) has a multiplicative inverse modulo \( m \).

**Proof Sketch:** The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y = 1 \mod m \) if all distinct modulo \( m \).

For \( x = 4 \) and \( m = 6 \). All products of 4...

\( S = (0, 4, 1, 4, 2, 4, 3, 4, 4, 4, 5, 4) \) = (0, 4, 8, 12, 16, 20) reducing \( \mod 6 \)

\( S = (0, 4, 2, 0, 4, 2) \)

Not distinct. Common factor 2. Can’t be 1. No inverse.

For \( x = 5 \) and \( m = 6 \).

\( S = (0, 5, 1, 5, 2, 5, 3, 5, 4, 5, 5, 5) \) = (0, 5, 4, 3, 2, 1)

All distinct, contains 1! 5 is multiplicative inverse of 5 \( \mod 6 \).

(Hmm. What normal number is it own multiplicative inverse?) 1 -1.

\[ 5x = 3 \mod 6 \]

What is \( x \)? Multiply both sides by 5.

\[ x = 15 = 3 \mod 6 \]

\[ 4x = 3 \mod 6 \]

No solutions. Can’t get an odd.

\[ 4x = 2 \mod 6 \]

Two solutions! \( x = 2, 5 \mod 6 \)

Very different for elements with inverses.

---

Greatest Common Divisor and Inverses.

**Thm:**
If greatest common divisor of \( x \) and \( m \), \( \gcd(x, m) \), is 1, then \( x \) has a multiplicative inverse modulo \( m \).

**Proof**

\[ \Rightarrow \]

**Claim:** The set \( S = \{0x, 1x, \ldots, (m-1)x\} \) contains \( y = 1 \mod m \) if all distinct modulo \( m \).

Each of \( m \) numbers in \( S \) correspond to one of \( m \) equivalence classes modulo \( m \).

\[ \Rightarrow \] One must correspond to 1 modulo \( m \). Inverse Exists!

Proof of Claim: If not distinct, then \( :a, b \in \{0, \ldots, m - 1\} \), a \( \neq \) b, where

\[ \underbrace{(ax = bx \mod m)} \Rightarrow (a - b)x = 0 \mod m \]

Or \( (a - b)x = km \) for some integer \( k \).

\[ \gcd(x, m) = 1 \]

\[ \Rightarrow \] Prime factorization of \( m \) and \( x \) do not contain common primes.

\[ \Rightarrow (a - b) \text{ factorization contains all primes in } m \text{'s factorization.} \]

So \( (a - b) \) has to be multiple of \( m \).

\[ \Rightarrow (a - b) \geq m. \] But \( a, b \in \{0, m - 1\} \). Contradiction.

---

Proof Review 2: Bijections.

If \( \gcd(x, m) = 1 \),

Then the function \( f(a) = xa \mod m \) is a bijection.

One to one: there is a unique pre-image.

Onto: the sizes of the domain and co-domain are the same.

\[ x = 3, m = 4. \]

\[ f(1) = 3(1) = 3 \mod 4, f(2) = 6 = 2 \mod 4, f(3) = 1 \mod 3. \]

Oh yeah. \( f(0) = 0. \)

Bijection = unique pre-image and same size.

All the images are distinct. \( \Rightarrow \) unique pre-image for any image.

\[ x = 2, m = 4. \]

\[ f(1) = 2, f(2) = 0, f(3) = 2 \]

Oh yeah. \( f(0) = 0. \)

Not a bijection.
Finding inverses.

How to find the inverse?

How to find if \( x \) has an inverse modulo \( m \)?

Find \( \gcd(x, m) \): Greater than 1? No multiplicative inverse.

Equal to 1? Multiplicative inverse.

Algorithm: Try all numbers up to \( x \) to see if it divides both \( x \) and \( m \).

Very slow.

More divisibility

**Notation:** \( d | x \) means “\( d \) divides \( x \)” or \( x = kd \) for some integer \( k \).

**Lemma 1:** If \( d | x \) and \( d | y \) then \( d | y \) and \( d | \gcd(x, y) \).

**Proof:**

\[
\gcd(x, y) = x - [x/y] \cdot y = x - \lfloor x/y \rfloor \cdot y = x - \lfloor x/y \rfloor \cdot y = \lfloor x/y \rfloor \cdot y.
\]

Therefore \( d \) divides \( x \). And \( d \) divides \( y \) since it is in condition.

**Lemma 2:** If \( d | y \) and \( d | x \) then \( d | y \) and \( d | x \).

**Proof:** Similar. Try this at home.

**GCD Mod Corollary:** \( \gcd(x, y) = \gcd(y, \mod(x, y)) \).

**Proof:** \( x \) and \( y \) have same set of common divisors as \( x \) and \( \mod(x, y) \) by Lemma 1 and 2.

Same common divisors \( \implies \) largest is the same.

Euclid procedure is fast.

**Theorem:** \( \text{euclid}(x, y) \) uses \( 2n \) “divisions” where \( n = b(x) = \log_2 x \).

Is this good? Better than trying all numbers in \( \{2, \ldots, \lfloor x/2 \rfloor \} \)?

Check 2, check 3, check 4, check 5, \ldots, check \( y/2 \).

If \( y = x \) roughly \( y \) uses \( n \) bits:

\[ 2^{n-1} \text{ divisions! Exponential dependence on size!} \]

101 bit number. \( 2^{100} \approx 10^{30} = \text{“million, trillion, trillion” divisions!} \)

\( 2n \) is much faster! \( \approx \) roughly 200 divisions.

Euclid’s algorithm.

**GCD Mod Corollary:** \( \gcd(x, y) = \gcd(y, \mod(x, y)) \).

Hey, what’s \( \gcd(7, 0) \)? 7 since 7 divides 7 and 7 divides 0

What’s \( \gcd(x, 0) \)? \( x \)

\[
\text{(define (euclid x y)}
\[
\text{if (= y 0)}
\[
x \mod (x, y)))
\]

**Theorem:** \( \text{euclid}(x, y) = \gcd(x, y) \) if \( x \geq y \).

**Proof:** Use Strong Induction.

**Base Case:** \( y = 0 \), “\( x \) divides \( y \) and \( x \)”

**Induction Step:** \( \gcd(x, y) < y \leq x \) when \( x \geq y \)

call in line (***) meets conditions plus arguments “smaller” and by strong induction hypothesis

computes \( \gcd(y, \mod(x, y)) \)

which is \( \gcd(x, y) \) by GCD Mod Corollary.

**Poll.**

Assume \( \log_2 1,000,000 \) is 20 to the nearest integer.

Mark what’s true.

(A) The size of 1,000,000 is 20 bits.

(B) The size of 1,000,000 is one million.

(C) The value of 1,000,000 is one million.

(D) The value of 1,000,000 is 20.

(A) and (C).
Poll

Which are correct?
(A) \( \gcd(700, 568) = \gcd(568, 132) \)
(B) \( \gcd(8, 3) = \gcd(3, 2) \)
(C) \( \gcd(8, 3) = 1 \)
(D) \( \gcd(4, 0) = 4 \)

Algorithms at work.

Trying everything
Check 2, check 3, check 4, check 5, ..., check \( y \).

"(gcd x y)" at work.
\[
\begin{align*}
euclid(700, 568) & \\
euclid(568, 132) & \\
euclid(132, 40) & \\
euclid(40, 12) & \\
euclid(12, 4) & \\
euclid(4, 0) & = 4
\end{align*}
\]

Notice: The first argument decreases rapidly.
At least a factor of 2 in two recursive calls.
(The second is less than the first.)

Runtime Proof.

\[
\begin{align*}
 & (\text{define } (\text{euclid } x y)) \\
 & \text{if } (\text{=} y 0) \\
 & \quad x \\
 & \quad (\text{euclid } y \text{ (mod } x y )) \\
\end{align*}
\]

Theorem: \((\text{euclid } x y)\) uses \(O(n)\) "divisions" where \( n = b(x) \).

Proof:
Fact: First arg decreases by at least factor of two in two recursive calls.
After \( 2 \log_2 x = O(n) \) recursive calls, argument \( x \) is 1 bit number.
One more recursive call to finish.
1 division per recursive call.
\( O(n) \) divisions.

Poll

Mark correct answers.
Note: Mod\((x, y)\) is the remainder of \( x \) divided by \( y \).
(A) \( \text{mod} \ (x, y) < y \)
(B) If \( \text{euclid}(x, y) \) calls \( \text{euclid}(u, v) \) calls \( \text{euclid}(a, b) \) then \( a \leq x/2 \).
(C) \( \text{euclid}(x, y) \) calls \( \text{euclid}(u, v) \) means \( u = y \).
(D) If \( y > x/2 \), \( \text{mod} \ (x, y) < y/2 \)
(E) If \( y > x/2 \), \( \text{mod} \ (x, y) = (y - x) \)
(D) is not always true.

Runtime Proof (continued.)

\[
\begin{align*}
 & (\text{define } (\text{euclid } x y)) \\
 & \text{if } (\text{=} y 0) \\
 & \quad x \\
 & \quad (\text{euclid } y \text{ (mod } x y )) \\
\end{align*}
\]

Fact:
First arg decreases by at least factor of two in two recursive calls.
Proof of Fact: Recall that first argument decreases every call.
Case 1: \( y < x/2 \), first argument is \( y \)
\( \implies \text{true in one recursive call;} \)
Case 2: Will show \( "y \geq x/2" \) \( \implies \) "\( \text{mod}(x, y) \leq x/2." \)
\( \text{mod} \ (x, y) \) is second argument in next recursive call,
and becomes the first argument in the next one.
When \( y \geq x/2 \), then
\( \left\lfloor \frac{x}{y} \right\rfloor = 1 \)
\( \text{mod} \ (x, y) = x - y \left\lfloor \frac{x}{y} \right\rfloor = x - y \leq x - x/2 = x/2 \)

Finding an inverse?

We showed how to efficiently tell if there is an inverse.
Extend euclid to find inverse.
Euclid's GCD algorithm.

\[
\text{(define (euclid x y)}
\begin{cases}
(\text{if } (= y 0)) & (x) \\
(\text{euclid } y \mod (x y)))
\end{cases}
\)\]

Computes the gcd\((x, y)\) in \(O(n)\) divisions. (Remember \(n = \log_2 x\).)

For \(x\) and \(m\), if \(\text{gcd}(x, m) = 1\) then \(x\) has an inverse modulo \(m\).

Multiplicative Inverse.

GCD algorithm used to tell if there is a multiplicative inverse.

How do we find a multiplicative inverse?

Extended GCD Algorithm.

\[
\begin{align*}
\text{ext-gcd}(x, y) & \quad \text{if } y = 0 \text{ then return } (x, 1, 0) \\
& \quad \text{else} \\
& \quad (d, a, b) \leftarrow \text{ext-gcd}(y, \mod(x, y)) \\
& \quad \text{return } (d, b, a - \text{floor}(x/y) \cdot b)
\end{align*}
\]

Theorem: Returns \((d, a, b)\), where \(d = \text{gcd}(a, b)\) and \(d = ax + by\).

Extended GCD

Euclid's Extended GCD Theorem: For any \(x, y\) there are integers \(a, b\) such that

\[ax + by = d\]

where \(d = \text{gcd}(x, y)\).

“Make \(d\) out of sum of multiples of \(x\) and \(y\).”

What is multiplicative inverse of \(x\) modulo \(m\)?

By extended GCD theorem, when \(\text{gcd}(x, m) = 1\).

\[ax + bm = 1\]

\[ax = 1 - bm = 1 \pmod{m}\]

So \(a\) multiplicative inverse of \(x \pmod{m}\)!!

Example: For \(x = 12\) and \(y = 35, \text{gcd}(12, 35) = 1\).

\((3)12 + (−1)35 = 1\)

\(a = 3\) and \(b = −1\).

The multiplicative inverse of \(12 \pmod{35}\) is 3.

Check: \(3(12) = 36 = 1 \pmod{35}\).

Make \(d\) out of multiples of \(x\) and \(y\).?

\[
\begin{align*}
\text{gcd}(35, 12) & = 11; \quad \text{gcd}(12, 35) = 11 \\
\text{gcd}(11, 1) & = 1 \\
\text{gcd}(10, 0) & = 1
\end{align*}
\]

How did \(\text{gcd}\) get 11 from 35 and 12?

\[35 = \frac{35}{12} \cdot 2 = 35 - (2)12 = 11\]

How does \(\text{gcd}\) get 1 from 12 and 11?

\[12 = \frac{12}{11} \cdot 11 - (1)11 = 1\]

Algorithm finally returns 1.

But we want 1 from sum of multiples of 35 and 12?

Get 1 from 12 and 11.

\[1 = 12 - (1)11 = 12 - (1)(35 - (2)12) = (3)12 + (−1)35\]

Get 11 from 35 and 12 and plugin... Simplify. \(a = 3\) and \(b = −1\).
Bijections

Bijection is one to one and onto.

\[ f: A \rightarrow B. \]

Domain: A, Co-Domain: B.

Versus Range.

E.g. \( \sin \) \( x \): \( A = \mathbb{R} \) - reals. \nRange is \([-1, 1]\). Onto: \([-1, 1]\).

Not one-to-one: \( \sin (x) = \sin (0) = 0 \).

Range Definition always is onto.

Consider \( f(x) = ax \ mod \ m. \)
\[ f: \{0, \ldots , m-1\} \rightarrow \{0, \ldots , m-1\}. \]

Domain/Co-Domain: \( \{0, \ldots , m-1\} \).

When is it a bijection?
When \( \gcd (a, m) = 1 \).

Not Example: \( a = 2, m = 4, f(0) = f(2) = 0 \) \( \mod 4 \).

Hand Calculation Method for Inverses.

Example: \( \gcd(7, 60) = 1. \)

\[ \text{egcd}(7, 60). \]

\[
\begin{align*}
7(0) + 60(1) & = 60 \\
7(1) + 60(0) & = 7 \\
7(-8) + 60(1) & = 4 \\
7(9) + 60(-1) & = 3 \\
7(-17) + 60(2) & = 1 \\
\end{align*}
\]

Confirm: \(-119 + 120 = 1\).

Note: an “iterative” version of the e-gcd algorithm.

Lots of Mods

\[ x = 5 \mod 7 \text{ and } x = 3 \mod 5. \]

What is \( x \) \( \mod 35 \)?

Let’s try 5. Not 3 \( \mod 5 \).
Let’s try 3. Not 5 \( \mod 7 \).

If \( x = 5 \mod 7 \),
then \( x \) is in \( \{5, 12, 19, 26, 33\} \).

Oh, only 33 is \( 3 \mod 5 \).
Hmmm... only one solution.

A bit slow for large values.
My love is won. Zero and One. Nothing and nothing done.

Find $x = a \mod mn$ and $x = b \mod mn$ where $\gcd(m, n) = 1$.

**CRT Thm:** There is a unique solution $x$ $(\mod mn)$.

**Proof (solution exists):**
Consider $u = n^{-1} (\mod m)$.
$u = 0 \mod m$ and $u = 1 \mod m$
Consider $v = m^{-1} (\mod n)$.
$v = 1 \mod n$ and $v = 0 \mod n$
Let $x = au + bv$.

$x = a \mod m$ since $bv = 0 \mod m$ and $au = a \mod m$

$x = b \mod n$ since $au = 0 \mod n$ and $bv = b \mod n$

This shows there is a solution.

**CRT Thm:** There is a unique solution $x$ $(\mod mn)$.

**Proof (uniqueness):**
If not, two solutions, $x$ and $y$.
$x - y = 0 \mod m$ and $(x - y) = 0 \mod n$.

$x - y \mod mn \iff mn(x - y) \equiv x - y \mod 0 \iff 0, \ldots, mn - 1$.

Thus, only one solution modulo $mn$.

**Fermat’s Theorem:** Reducing Exponents.

**Fermat’s Little Theorem:** For prime $p$, and $a \not\equiv 0 \mod p$,
\[ a^{p-1} \equiv 1 \mod p. \]

**Proof:** Consider $S = \{a, 1 \ldots, a - (p - 1)\}$.

All different modulo $p$ since $a$ has an inverse modulo $p$.

$S$ contains representative of $\{1, \ldots, p - 1\}$ modulo $p$.

Since multiplication is commutative,
\[ a^{p-1} (\cdots (p - 1)) = (\cdots (p - 1)) \mod p. \]

Each of $2, \ldots, (p - 1)$ has an inverse modulo $p$, solve to get...
\[ a^{p-1} \equiv 1 \mod p. \]

**Poll.**

My love is won, Zero and one. Nothing and nothing done.

What is the rhyme saying?

(A) Multiplying by 1 gives back number. (Does nothing.)

(B) Adding 0 gives back number. (Does nothing.)

(C) Rao has gone mad.

(D) Multiplying a number by 0 gives 0.

(E) Adding one does not too much.

All are (maybe) correct.

(A), (C), and (E)

For $m, n, \gcd(m, n) = 1$.

$x \mod mn \iff x = a \mod m$ and $x = b \mod n$

$y \mod mn \iff y = c \mod m$ and $y = d \mod n$

Also, true that $x + y \mod mn \iff a + c \mod m$ and $b + d \mod n$.

Mapping is “isomorphic”: corresponding addition (and multiplication) operations consistent with mapping.

Which was used in Fermat’s theorem proof?

(A) The mapping $f(x) = ax \mod p$ is a bijection.

(B) Multiplying a number by 1 gives the number. (Does nothing.)

(C) All nonzero numbers $\mod p$, have an inverse.

(D) Multiplying a number by 0 gives 0.

(E) Multiplying elements of sets A and B together is the same if $A = B$.

(A), (C), and (E)
**Fermat and Exponent reducing.**

**Fermat's Little Theorem:** For prime \( p \), and \( a \not\equiv 0 \) (mod \( p \)),
\[ a^{p-1} \equiv 1 \pmod{p}. \]

What is \( 2^{101} \pmod{7} \)?

Wrong: \( 2^{101} = 2^{7} \times 14 + 3 = 2^{3} \pmod{7} \)

Fermat: 2 is relatively prime to 7.
\[ \Rightarrow 2^{6} \equiv 1 \pmod{7}. \]

Correct: \( 2^{101} = 2^{6} \times 16 + 5 = 2^{5} = 32 = 4 \pmod{7} \).

For a prime modulus, we can reduce exponents modulo \( p-1! \).

---

**Lecture in a minute.**

Euclid's Alg: \( \gcd(x,y) = \gcd(y,x \mod y) \)
Fast cuz value drops by a factor of two every two recursive calls.

Extended Euclid: Find \( a, b \) where \( ax + by = \gcd(x, y) \).
Idea: compute \( a, b \) recursively (euclid), or iteratively.
Inverse: \( ax + by = \gcd(x, y) \pmod{y} \).
If \( \gcd(x, y) = 1 \), we have \( ax \equiv 1 \pmod{y} \)
\[ \rightarrow a = x^{-1} \pmod{y}. \]

Chinese Remainder Theorem:
If \( \gcd(n,m) = 1 \), \( x \equiv a \pmod{n} \), \( x \equiv b \pmod{m} \) unique sol.
Proof: Find \( u = 1 \pmod{n} \), \( u = 0 \pmod{m} \),
\[ \text{and } v = 0 \pmod{n} \), \( v = 1 \pmod{m} \).
Then: \( x = au + bv = a \pmod{n} \),
\[ u = m(m^{-1} \pmod{n}) \pmod{m} \text{ works!} \]

Fermat: Prime \( p \), \( a^{p-1} \equiv 1 \pmod{p} \).
Proof Idea: \( f(x) = a(x) \pmod{p} \): bijection on \( S = \{1, \ldots, p-1\} \).
Product of els \( \equiv \pmod{ \text{range/domain: } a^{p-1} \text{ factor in range.}} \)