Modular Arithmetic

CS70: Discrete Mathematics and Probability Theory

UC Berkeley – Summer 2025

Lecture 7

Ref: Note 6

Lecture Outline

1. Modular Arithmetic
   Clock math
   General mathematical definition
2. Inverses for Modular Arithmetic
   Relationship to Greatest Common Divisor (GCD)
   Necessary and sufficient conditions
3. Computing GCDs
   The slow way
   Euclid's GCD Algorithm

Clock Math

American 12 hour clock

If it is 1:00 now.

- What time is it in 2 hours? 3:00
- What time is it in 5 hours? 6:00
- What time is it in 15 hours? 16:00 ...actually 4:00

16 is the "same as 4" with respect to a 12 hour clock system

- "Wraps around" back to 1 after 12 – subtract 12 to get equivalent time

What time is it in 100 hours? 101:00! ...or 5:00

- 101 is eight 12-hour spans plus 5 hours: $101 = 8 \times 12 + 5$
- 101 is the "same as 5" with respect to a 12 hour clock system

Clock time equivalent up to addition of any integer multiple of 12.

Custom is only to use the representative in $\{12, 1, \ldots, 11\}$

- Almost remainder after dividing by 12... except for 12 instead of 0.

Day of the Week

Today is Wednesday, July 2, 2025

What day is it a year from now? ...on July 2, 2026?

Encode days with numbers: 0 for Sunday, 1 for Monday, . . . , 6 for Saturday

Today: Day 3 (Wednesday)

What day (number) in 3 days? Day 6 (Saturday)

What day (number) in 4 days? Day 7? ..Day 0 (Sunday)

$\Rightarrow$ Days are equivalent up to addition/subtraction of a multiple of 7

What day (number) in 82 days? Day 85. $85 = 12 \times 7 + 1$ ..Day 1 (Monday)

What day is it a year from now?

Number days? 365 (leap year some years... not this time though)

Day $3 + 365 = 368$

Divide by 7: quotient 52, remainder 4

$368 = 52 \times 7 + 4$ (Thursday)

Dividing by 7, remainder is always in range $0, \ldots, 6$

Making it a valid encoding of a day of the week

Modular Arithmetic

Definition: x is congruent to y modulo m, written "$x \equiv y \pmod{m}$," if and only if $(x-y)$ is divisible by m.

Equivalent: x and y have the same remainder when divided by m.
Or add multiple of m: $x = y + km$ for some $k \in \mathbb{Z}$.

Defines "mod m equivalence classes" (or "residue classes")
For "mod 7": $\{\ldots,-7,0,7,14,\ldots\}$, $\{\ldots,-6,1,8,15,\ldots\}$, ...
In each class: exactly one value in range $0,\ldots,m-1$
Reduce x modulo m: The value in $0,\ldots,m-1$ in x's equivalence class
Example: Reduce 368 mod 7 gives 4 (from previous slide)
Can write "$368 \bmod 7 = 4$"

Useful Fact: Working "mod m", addition, subtraction, multiplication can be done with any equivalent x and y.

So $(7 \times 15 - 6) \equiv (14 \times 8 + 15) \pmod{7}$
Simplifying: $99 \equiv 127 \pmod{7}$ and $(127-99) = 28$, *a multiple of 7*

For "what day in a year?" Can add 365 or add $(365 \bmod 7) = 1$
$\Rightarrow$ Add 1 or add 365 — same result mod 7

Basic Arithmetic Modulo m

Formalizing previous "useful fact"

Theorem: If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $a+b \equiv c+d \pmod{m}$.

Proof: If $a \equiv c \pmod{m}$, then $a = c + km$ for some $k \in \mathbb{Z}$.
Similarly, if $b \equiv d \pmod{m}$, then $b = d + jm$ for some $j \in \mathbb{Z}$.
Adding these two together we get $a+b = c+d+(k+j)m$, so
$(a+b) \equiv (c+d) \pmod{m}$. $\square$

Similarly:

Theorem: If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $a-b \equiv c-d \pmod{m}$.

Theorem: If $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$, then $a \cdot b \equiv c \cdot d \pmod{m}$.

Consequence: Can calculate with smaller numbers, using $\{0, \ldots, m-1\}$.

Silly example: What is $7771 \times 7771 \bmod 7$?

$\Rightarrow$ Calculating it out: $7771 \times 7771 = 60{,}388{,}441$, remainder in div by 7 is 1

$\Rightarrow$ With "this one simple trick": $7771 \bmod 7 = 1$, so $7771 \times 7771 \equiv 1 \times 1 \pmod{7}$

Notation

$x \bmod m$ ...or... $\bmod(x, m)$ ...or in programming... `x % m`
All mean reduce x by m: remainder of x divided by m

Common notation in programming:

```
Python 3.12.3 (main, Jun 18 2025, 17:59:45) [GCC 13.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> 368 % 7
4
>>>
```

Do *not* use "%" in mathematical writing! Use mod
$\Rightarrow$ Warning: In programs, "%" may not agree with math for negative values!

Subtle distinction between similar notations:

$x \bmod m$ is an *operation* giving a value in $0, \ldots, m-1$

$a \equiv b \pmod{m}$ is a *relation* – doesn't give a value

If $r = x \bmod m$ (operator) then $r \equiv x \pmod{m}$

BUT if $r \equiv x \pmod{m}$ it does *not* mean $r = x \bmod m$
r may not be in $0, \ldots, m-1$

Multiplicative Inverses

The multiplicative inverse of a value x is a value y such that $x \cdot y = 1$.

$\Rightarrow$ More generally, product gives *multiplicative identity* – "1" is good enough for now

But wait! Multiplication over what set? How is multiplication defined?

Multiplication over $\mathbb{Q}$: The multiplicative inverse of $\frac{a}{b}$ is $\frac{b}{a}$.

Multiplication over $\mathbb{R}$ example: The multiplicative inverse of 2 is 0.5.

Multiplication over $\mathbb{Z}$ example: The multiplicative inverse of 2 is ... ????

Multiplication over $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$: Multiplicative inverse of 0 is... ????

Bottom line: Multiplicative inverses don't always exist

$\Rightarrow$ Depends on the set you're working over, value you're asking about, ...

Division of a by b is just a times the multiplicative inverse of b.

Example over $\mathbb{Q}$ – normally would say "divide both sides by 2," but really:

$$2x = 3 \implies (\frac{1}{2}) \cdot 2x = (\frac{1}{2}) \cdot 3 \implies x = \frac{3}{2}$$

Multiplicative Inverses in Modular Arithmetic

Bottom line: Multiplicative inverses don't always exist

$\Rightarrow$ Depends on the set you're working over, value you're asking about, ...

What if we're multiplying $\bmod m$?

Multiplicative inverse of $x \pmod m$ is a value y such that $x \cdot y \equiv 1 \pmod m$

Do multiplicative inverses exist in modular arithmetic?

Consider $4 \pmod 7$: we have $2 \cdot 4 \equiv 1 \pmod 7$

$\Rightarrow$ So 2 is multiplicative inverse of $4 \pmod 7$

$\Rightarrow$ Use to solve $4x \equiv 5 \pmod 7$

$$2 \cdot 4x \equiv 2 \cdot 5 \pmod 7$$

$$x \equiv 3 \pmod 7$$

[Check it: What's $4 \cdot 3 \bmod 7$?]

Consider $4 \pmod 6$: Multiplicative inverse?

$\Rightarrow$ Need x such that $4 \cdot x \equiv 1 \pmod 6$

... or $4x - 1 = 6k$ for some $k \in \mathbb{Z}$

... but LHS is odd, RHS is even... impossible!

In modular arithmetic, some values have mult inverses; some don't; ... why?

Concept Check!

Question: Which of the following are true?

(A) Multiplicative inverse of $2 \pmod 5$ is $3 \pmod 5$.
$2 \cdot 3 = 6$ and $6 \equiv 1 \pmod 5$ ✓

(B) The multiplicative inverse of $(n-1) \pmod n$ is $(n-1) \pmod n$.
$(n-1)(n-1) = n^2 - 2n + 1 = n(n-2) + 1 \quad \longrightarrow$ a multiple of n plus 1 ✓

(C) Multiplicative inverse of $2 \pmod 5$ is 0.5.

(D) Multiplicative inverse of $4 \pmod 5$ is $-1 \pmod 5$.
$4 \cdot -1 = -4$ and $-4 \equiv 1 \pmod 5$ [note that $-4 - 1 = -5$, a multiple of 5] ✓

(E) Multiplicative inverse of $4 \pmod 5$ is $4 \pmod 5$.
$4 \cdot 4 = 16$ and $16 \equiv 1 \pmod 5$ [note: this is just (B) with numbers] ✓

Answer: All but (C). 0.5 has no meaning in arithmetic modulo 5.

Relative Primality is Sufficient for Inverses

Theorem: If $\gcd(x,m) = 1$, then x has a unique multiplicative inverse mod m.

Proof: Consider all multiples of $x \pmod{m}$: $0x, 1x, \ldots, (m-1)x$ (all mod m)

Claim: *If $\gcd(x,m) = 1$ then all these products are distinct.*

Proof of Claim: *Assume for the sake of contradiction that there is a pair a, b from $\{0, 1, \ldots, m-1\}$ with $a \neq b$ and $ax \equiv bx \pmod{m}$.*

Then $ax - bx = (a-b)x = km$ for some $k \in \mathbb{Z}$.

x and m share no prime factors, so $a-b$ must contain all factors of m, meaning $a-b$ is a multiple of m.

For values in $\{0, 1, \ldots, m-1\}$, can't have $|a-b| \geq m$ and since $a \neq b$ can't have $a-b = 0$. Therefore impossible – contradiction! QED claim

Products are m distinct values with m possible values, so each value appears exactly once. Therefore exactly one product is 1, which gives the multiplicative inverse of x. □

Earlier Examples – Put Into This Proof

Proof looked at products $0x, 1x, \ldots, (m-1)x$ (all mod m)

Earlier example: Inverse of 4 $\pmod 7$?

Note: $\gcd(4,7) = 1$

Products are $0 \cdot 4$, $1 \cdot 4$, $2 \cdot 4$, $3 \cdot 4$, $4 \cdot 4$, $5 \cdot 4$, $6 \cdot 4$ = 0, 4, 8, 12, 16, 20, 24

Mod 7: 0, 4, 1, 5, 2, 6, 3

$\Rightarrow$ Every value $\{0, \ldots, 6\}$ appears exactly once including 1 for inverse

Second example: Inverse of 4 $\pmod 6$? *Note:* $\gcd(4,6) = 2$

Products are $0 \cdot 4$, $1 \cdot 4$, $2 \cdot 4$, $3 \cdot 4$, $4 \cdot 4$, $5 \cdot 4$ = 0, 4, 8, 12, 16, 20

Mod 6: 0, 4, 2, 0, 4, 2

$\Rightarrow$ Repetitions! (and no 1)

Another observation: 0 is a multiple of a non-zero ($4 \cdot 3 \equiv 0 \pmod 6$)

That's ... interesting

Suggests an interesting possibility: mod p, where p is prime

$\Rightarrow$ *All* non-zero residues are relatively prime so have an inverse

Gettin' Mathy With It

$f(x) = x \cdot 4 \bmod 7$

x	$f(x)$
0	0
1	4
2	1
3	5
4	2
5	6
6	3

$f(x)$ is a bijection

Alternate terminology: one-to-one and onto
Implies: $f(x)$ is invertible
$f^{-1}(x) = x \cdot 2 \bmod 7$
Why? $f^{-1}(f(x)) \equiv (x \cdot 4 \cdot 2) \equiv x \pmod 7$

Important: For $f(x) = c \cdot x \bmod m$, bijection whenever $\gcd(c, m) = 1$

$g(x) = x \cdot 4 \bmod 6$

x	$f(x)$
0	0
1	4
2	2
3	0
4	4
5	2

$g(x)$ is *not* a bijection

Multiple values map to same image
Can't invert — no unique pre-image

Concept Check!

Question: Which is bijection?

(A) $f(x) = x$ for domain and range being $\mathbb{R}$

(B) $f(x) = ax \pmod{m}$ for $x \in \{0, ..., m-1\}$ and $gcd(a, m) = 2$

(C) $f(x) = ax \pmod{m}$ for $x \in \{0, ..., m-1\}$ and $gcd(a, m) = 1$

Answer: (A) and (C)

(A) is the identify function over $\mathbb{R}$ – always a bijection

(B) and (C): Bijection if and only if $\gcd(a, m) = 1$

Relative Primality is Necessary for Inverses

Theorem: For $x, m \in \mathbb{N}$, if $\gcd(x, m) \neq 1$ then x has no multiplicative inverse modulo m.

Proof: Let $x, m \in \mathbb{N}$ with $\gcd(x, m) = d$ and $d > 1$. Assume for the sake of contradiction that x has a multiplicative inverse, say y with $yx \equiv 1 \pmod{m}$.

Then there exists a $k \in \mathbb{Z}$ such that $yx + km = 1$. Since d is a divisor of x and m, we can write $x = x'd$ and $m = m'd$, and so $yx'd + km'd = (yx' + km')d = 1$. This implies that 1 is a multiple of d, which is impossible for $d > 1$.

Thus we reach a contradiction, so x cannot have a multiplicative inverse. $\square$

Combining the necessary and sufficient results:

Theorem: For $x, m \in \mathbb{N}$, x has a multiplicative inverse modulo m if and only if $\gcd(x, m) = 1$.

Algorithms for GCD

To test if multiplicative inverse exists, compute gcd. How?

Algorithm 1 – count down to find a common divisor – stops at largest:

```
def gcd(x, y):
    d = x
    while d >= 1:
        if (x%d == 0) and (y%d == 0):
            return d
        d = d - 1
```

Does it work? Yes!

Fast? No!

`gcd(1000000, 999999)` takes a million iterations (remember this!)

Divisibility and $\bmod$

Lemma 1: If $d \mid x$ and $d \mid y$, then $d \mid (x \bmod y)$.

Proof: Let $z = x \bmod y$, so by definition $x = ky + z$ for some $k \in \mathbb{Z}$.
Since $d \mid x$ there is an $x' \in \mathbb{Z}$ such that $x = x'd$.
Similarly, since $d \mid y$ there is an $y' \in \mathbb{Z}$ such that $y = y'd$.
Then we can write $x = ky + z \implies x'd = ky'd + z \implies (x' - ky')d = z$.
Therefore, $d \mid z$ (with $z = x \bmod y$). □

Lemma 2: If $d \mid y$ and $d \mid (x \bmod y)$ then $d \mid x$.

Proof: "Trust me" (or prove it on your own!). □

GCD Mod Theorem: $\gcd(x, y) = \gcd(y, x \bmod y)$

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

Same common divisors $\implies$ largest is the same. □

Euclid's Algorithm ($\approx$ 300 B.C.)

GCD Mod Theorem: $\gcd(x,y) = \gcd(y, x \bmod y)$

Suggests a recursive algorithm – what's the base case?

By Theorem: $\gcd(4,4) = \gcd(4,0)$ – what's $\gcd(4,0)$???

$4 | 4$ and $4 | 0$ — so $\gcd(4,0) = 4$

In general: $\gcd(x,0) = x$

```
def euclid(x, y):
    if y == 0:
        return x

    return euclid(y, x % y)
```

Theorem: `euclid(x,y)` correctly computes $\gcd(x,y)$.

Proof: Does it halt? Yes! 2nd argument gets smaller each step, and stays non-negative. $\implies$ It reaches 0.

Is the answer right? Yes! By GCD Mod Theorem, GCD of the two arguments stays the same with every recursive call. □

Concept Check!

Question: Which of the following 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

Answer: All are correct!

How Fast is `euclid`?

Recall: Algorithm 1 took 1,000,000 steps for `gcd(1000000, 999999)`

What about `euclid`?

```
euclid(1000000, 999999)
... euclid(999999, 1)
    ... euclid(1, 0)
        ... 1
```

`euclid` takes 3 steps!

OK... this example was "cheating"

- ⇒ Best possible case for `euclid`
- ⇒ Worst possible case for Algorithm 1

How Fast is `euclid`?

More realistic example: compute $\text{gcd}(700, 568)$:

```
euclid(700,568)
  euclid(568, 132)
    euclid(132, 40)
      euclid(40, 12)
        euclid(12, 4)
          euclid(4, 0)
            4
```

Notice: The first argument decreases rapidly.

At least a factor of 2 every two recursive calls.

Can we prove this?

Proof for Argument Decrease

Recursive call: $\gcd(x, y) = \gcd(y, x \bmod y)$

Slight technicality: Assume $x \geq y$ – no big deal, if it's not it will be after 1 call

Theorem: If we start with $x \geq y$, then after two recursive calls the first argument is halved.

Proof: By cases...

Case 1: $x \geq 2y$
    Here $y \leq x/2$ and first argument to rec call is $\leq x/2$
    Halved in one call!

Case 2: $x < 2y$
    Since $x \geq y$, we have $y \leq x < 2y$, so $\lfloor \frac{x}{y} \rfloor = 1$
    So the remainder: $x \bmod y = x - y \cdot \lfloor \frac{x}{y} \rfloor = x - y$
    In this case, $y > x/2$, so $x - y < x/2$
    $x \bmod y$ becomes first arg in 2 steps, and $x \bmod y < x/2$

Halved in two steps in both cases. □

How Fast *Is* This?

How many times can we half something until we get to 1? For example:

$$128 \to 64 \to 32 \to 16 \to 8 \to 4 \to 2 \to 1$$

In general, starting with x (and ignoring non-integer results....):

$$x \to \frac{x}{2} \to \frac{x}{2^2} \to \frac{x}{2^3} \to \frac{x}{2^4} \to \cdots \to 2 \to 1$$

Observation: After k steps we have $\frac{x}{2^k}$

$\Rightarrow$ Solve $\frac{x}{2^k} = 1 \implies x = 2^k \implies k = \log_2 x$

Algorithm halves in *two* steps, so takes at most $2 \log_2 x$ steps

x	Algorithm 1	`euclid`
1000	1000	≈ 20
1 million	1 million	≈ 40
1 billion	1 billion	≈ 60

So first example was cheating, and `euclid` finished in 3 steps, but...

It will never take more than 40 steps!

Computing Multiplicative Inverse

Multiplicative inverse of $x \pmod{m}$ if and only if $\gcd(x, m) = 1$.

$\Rightarrow$ `euclid` can quickly tell if a multiplicative inverse exists!

But we want to compute the multiplicative inverse! How?

Turns out:

- A modification of `euclid` computes multiplicative inverse
- Same running time – *fast!*

Details?

... next time

Summary

Modular Arithmetic: $x \equiv y \pmod{N}$ if $x = y + kN$ for some integer k.

For $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$:
$ac \equiv bd \pmod{N}$ and $(a+c) \equiv (b+d) \pmod{N}$.

Division?
Multiply by multiplicative inverse
$a \pmod{N}$ has multiplicative inverse iff $\gcd(a, N) = 1$

Euclid's Algorithm:
Based on fact that $gcd(x, y) = gcd(y, x \bmod y)$
Very fast!
Algorithm invented around 300 B.C. is still in use today! Cool.