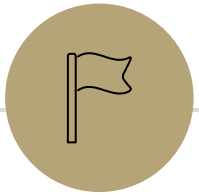
Number Theory Continued

CSE 311 25Su
Lecture 9

Announcements

- HW3 is out and due Wednesday!
  - Start today if you haven't already

- Pick up HW1 solutions at the front of the room or during Parker's OH this week.



Review

Why Number Theory?

Applicable in Computer Science

“hash functions” (you’ll see them in 332) commonly use modular arithmetic
Much of classical cryptography is based on prime numbers.

More importantly, a great playground for writing English proofs.

Divides

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Informally: "a fits into b" or "a is a factor of b"

"The small number goes first*" *when both are positive integers

Examples: $5 \mid 15$ $\quad -3 \mid 9$ $\quad 5 \nmid 21$

Division Theorem

Division Theorem:

For any integer a and positive integer d, there exist unique integers q, r with $0 \leq r < d$ such that $a = qd + r$.

In Java, q is the result of the operation a/d

In Java, r is the result of the operation $a \,\%\, d$

Warning
When dealing with negative numbers, Java's % may behave differently!

The mod (%) operator

Division Theorem
$a = qd + r$ with $0 \leq r < d$

- The % operator is often referred to as "mod"
- $a \,\%\, d$ returns the remainder r when you divide a by d

$22 \,\%\, 5 = 2$

$22 = 4 \cdot 5 + \mathbf{2}$

$25 \,\%\, 5 = 0$

$25 = 5 \cdot 5 + \mathbf{0}$

$0 \,\%\, 5 = 0$

$0 = 0 \cdot 5 + \mathbf{0}$

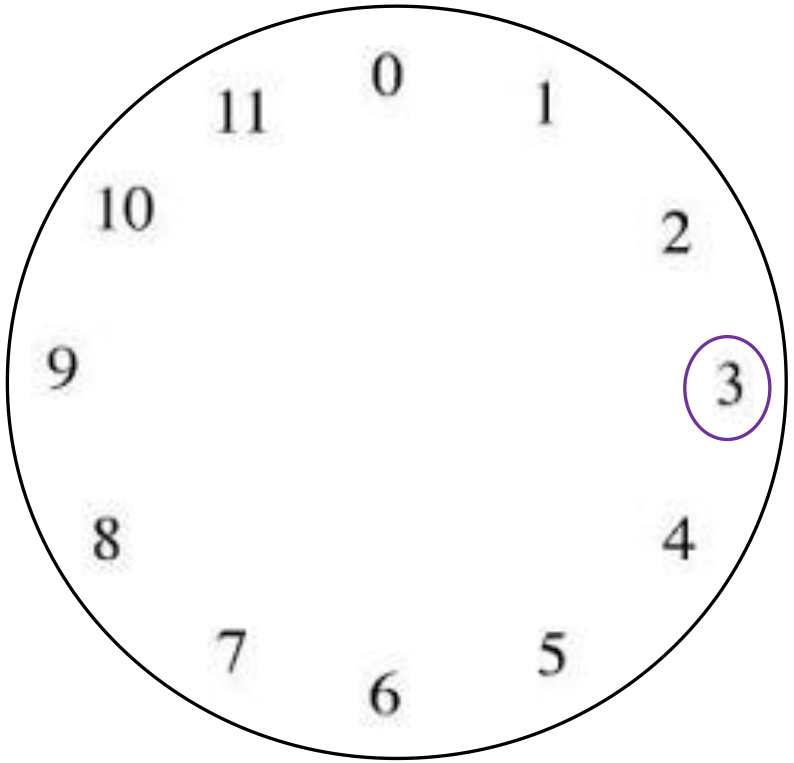
$-1 \,\%\, 4 = 3$

$-1 = -1 \cdot 4 + \mathbf{3}$

Modular Arithmetic: Like a Clock

Imagine you can only represent numbers 0, … , 11. We call this "arithmetic mod 12".

What's 8 + 7? 3



Observation
The solution is $a \% 12$.

Congruence

We need a formal definition of $a \equiv b \pmod{m}$.

We can't just say "a and b are on the same place in the m clock ☺"

Definition:

For integers a, b and positive integer m, we say $a \equiv b \pmod{m}$ iff $m \mid (a - b)$.

Note: $a \equiv b \pmod{m}$ is equivalent to $a \,\%\, m = b \,\%\, m$.

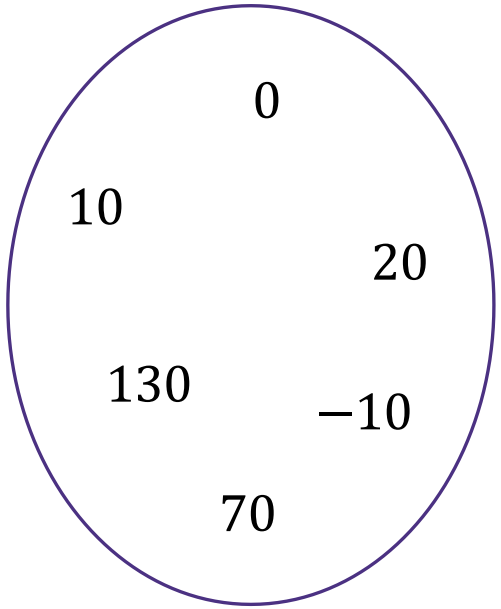
We will actually prove that the two notions are the same. But, the formal definition is much easier to use in proofs.

Intuition

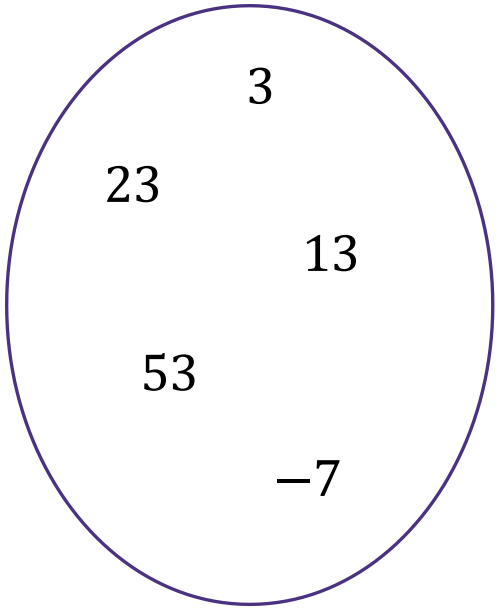
Definition: $a \equiv b \pmod{m}$ is defined as $m \mid (a - b)$

Intuition: Equivalently, $a \equiv b \pmod{m}$ means $a \% m = b \% m$

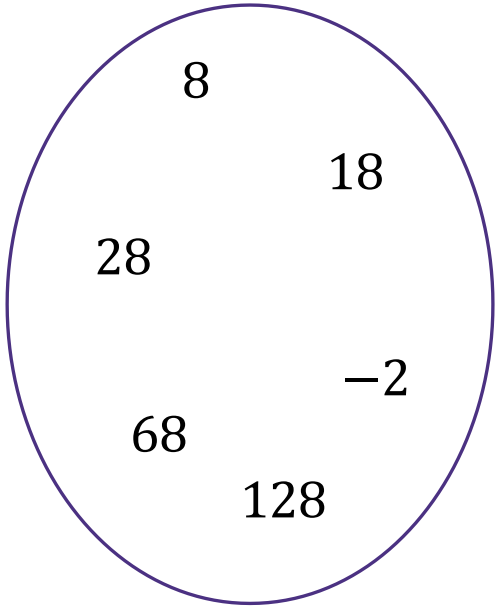
Here we have some groups of numbers that are congruent mod 10.



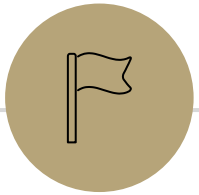
Congruent to 0



Congruent to 3



Congruent to 8



Warm Up: (Does Not) Divides Proof

Warm Up: (Does Not) Divides Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Warm Up: (Does Not) Divides Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:

Let a, b, c be arbitrary integers, and suppose $a \nmid (bc)$.

Then there is not an integer z such that $az = bc$

So $a \nmid b$ or $a \nmid c$

Warm Up: (Does Not) Divides Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

Proof:

Let a, b, c be arbitrary integers, and suppose $a \nmid (bc)$.

Then there is not an integer z such that $az = bc$

So $a \nmid b$ or $a \nmid c$

Warm Up: (Does Not) Divides Proof

For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

There has to be a better way!

If only there were some equivalent implication…

One where we could negate everything…

Take the contrapositive of the statement:

For all integers, a, b, c: Show if $a|b$ and $a|c$ then $a|(bc)$.

By contrapositive

Claim: For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

We argue by contrapositive.

Let a, b, c be arbitrary integers, and suppose $a|b$ and $a|c$.

Therefore $a|bc$

By contrapositive

Claim: For all integers, a, b, c: Show that if $a \nmid (bc)$ then $a \nmid b$ or $a \nmid c$.

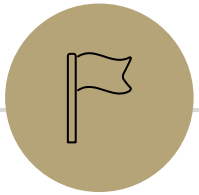
We argue by contrapositive.

Let a, b, c be arbitrary integers, and suppose $a|b$ and $a|c$.

By definition of divides, $ax = b$ and $ay = c$ for some integers x and y.

Multiplying the two equations, we get $axay = bc$

Since a, x, y are all integers, xay is an integer. Applying the definition of divides, we have $a|bc$.



Properties of Congruence

Recall: Familiar Properties of $=$ in algebra

- If $a = b$, then $b = a$.
- If $a = b$ and $c = d$, then $a + c = b + d$.
- If $a = b$ and $c = d$, then $ac = bd$.
- If $a = b$ and $b = c$, then $a = c$.

These are the facts that allow us to use algebra to solve problems. We will prove analogous facts for modular arithmetic.

Claim 1: for all integers a, b, c, m, with $m > 0$:

$$a \equiv b \pmod{m} \rightarrow a + c \equiv b + c \pmod{m}$$

Before we start, we must know:

1. What every word in the statement means.
2. What the statement as a whole means.
3. Where to start.
4. What your target is.

Divides

For integers x, y we say $x|y$ ("x divides y") iff there is an integer z such that $xz = y$.

Equivalence in modular arithmetic

Let a, b, m be integers with $m > 0$.
We say $a \equiv b \pmod{m}$ if and only if $m|(b - a)$

Claim 1

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 1: For integers a, b and positive integer m, if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

Claim 1

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 1: For integers a, b and positive integer m, if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

Proof: Let a, b be arbitrary integers and let m be an arbitrary positive integer. Suppose that $a \equiv b \pmod{m}$.

Then by definition of congruence, $b \equiv a \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Claim 1

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 1: For integers a, b and positive integer m, if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

Proof: Let a, b be arbitrary integers and let m be an arbitrary positive integer. Suppose that $a \equiv b \pmod{m}$.

[Unroll definitions]

[Manipulate towards goal]

[Reroll definitions]

Then by definition of congruence, $b \equiv a \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Claim 1

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 1: For integers a, b and positive integer m, if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

Proof: Let a, b be arbitrary integers and let m be an arbitrary positive integer. Suppose that $a \equiv b \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$.

[Manipulate towards goal]

[Reroll definitions]

Then by definition of congruence, $b \equiv a \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Claim 1

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 1: For integers a, b and positive integer m, if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

Proof: Let a, b be arbitrary integers and let m be an arbitrary positive integer. Suppose that $a \equiv b \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$.

Then by definition of divides, there exists some integer k such that $a - b = mk$.

[Manipulate towards goal]

[Reroll definitions]

Then by definition of congruence, $b \equiv a \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Claim 1

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 1: For integers a, b and positive integer m, if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$.

Proof: Let a, b be arbitrary integers and let m be an arbitrary positive integer. Suppose that $a \equiv b \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$.

Then by definition of divides, there exists some integer k such that $a - b = mk$.

Multiplying both sides by -1, we have $b - a = -mk = m(-k)$. Since k is an integer, $-k$ is an integer.

So by definition of divides, $m \mid (b - a)$.

Then by definition of congruence, $b \equiv a \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Note on Claim 1

- You'll see $a \equiv b \pmod{m}$ defined as $m \mid (a - b)$ or $m \mid (b - a)$ depending on where you look.
- Claim 1 proves these definitions are equivalent. From now on, you can use either definition in your proofs.
- In general, once we have proved claims in class, you can use those claims in your homework without proof.

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.

Intuition

$3 \equiv 13 \pmod{10}$ and $14 \equiv 24 \pmod{10} \Rightarrow 17 \equiv 37 \pmod{10}$

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.

Proof: Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $a + c \equiv b + d \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.

Proof: Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

[Unroll definitions]

[Manipulate towards goal]

[Reroll definitions]

Then by definition of congruence, $a + c \equiv b + d \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.

Proof: Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $c - d = mj$.

[Manipulate towards goal]

[Reroll definitions]

Then by definition of congruence, $a + c \equiv b + d \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.

Proof: Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $c - d = mj$.

Then adding both expressions, we have:

$$a - b + c - d = mk + mj$$

$$a + c \; - (b + d) = m(k + j)$$

[Reroll definitions]

Then by definition of congruence, $a + c \equiv b + d \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 2

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 2: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. then $a + c \equiv b + d \pmod{m}$.

Proof: Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $c - d = mj$.

Then adding both expressions, we have:

$$a - b + c - d = mk + mj$$

$$a + c \; - (b + d) = m(k + j)$$

So by definition of divides, $m \mid (a + c) - (b + d)$.

Then by definition of congruence, $a + c \equiv b + d \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Intuition

$2 \equiv 12 \pmod{10}$ and $3 \equiv 13 \pmod{10} \Rightarrow 6 \equiv 156 \pmod{10}$

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Proof (Attempt 1): Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

[Unroll definitions]

[Manipulate towards goal]

[Reroll definitions]

Then by definition of congruence, $ac \equiv bd \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Proof (Attempt 1): Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $c - d = mj$.

[Manipulate towards goal]

[Reroll definitions]

Then by definition of congruence, $ac \equiv bd \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Proof (Attempt 1): Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $c - d = mj$.

Starting Point: $a - b = mk$ and $c - d = mj$

Goal: $ac - bd = mx$

[Reroll definitions]

Then by definition of congruence, $ac \equiv bd \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Proof (Attempt 1): Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $c - d = mj$.

Then multiplying both expressions, we have:

$$(a - b)(c - d) = mk \cdot mj$$

$$ac - bc - ad + bd = m^2kj$$

??

Goal: $ac - bd = mx$

Then by definition of congruence, $ac \equiv bd \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Proof (Attempt 2): Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $c - d = mj$.

Rearranging, we have $a = mk + b$ and $c = mj + d$. Multiplying both expressions, we have:

$$ac = (mk + b)(mj + d)$$
$$ac = m^2kj + mbj + mdk + bd$$
$$ac - bd = m^2kj + mbj + mdk$$
$$ac - bd = m(mkj + bj + dk)$$

Goal: $ac - bd = mx$

[Reroll definitions]

Then by definition of congruence, $ac \equiv bd \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 3

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 3: For integers a, b, c, d and positive integer m, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$.

Proof (Attempt 2): Let a, b, c, d and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Then by definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $c - d = mj$.

Rearranging, we have $a = mk + b$ and $c = mj + d$. Multiplying both expressions, we have:

$$ac = (mk + b)(mj + d)$$
$$ac = m^2kj + mbj + mdk + bd$$
$$ac - bd = m^2kj + mbj + mdk$$
$$ac - bd = m(mkj + bj + dk)$$

Since m, k, j, b, d are integers, $mkj + bj + dk$ is an integer. Thus by definition of divides, $m \mid (ac - bd)$. Then by definition of congruence, $ac \equiv bd \pmod{m}$. Since a, b, c, d, m were arbitrary, the claim holds.

Claim 4

Definitions:

$a \mid b$ iff $\exists k \in \mathbb{Z} \;\; b = ka$

$a \equiv b \pmod{m}$ iff $m \mid (a - b)$

Claim 4: For integers a, b, c and positive integer m, if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

Proof

Let a, b, c and $m > 0$ be arbitrary integers. Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then by definition of congruence, $m \mid (a - b)$ and $m \mid (b - c)$. Then by definition of divides, there exists some integers k, j such that $a - b = mk$ and $b - c = mj$.Adding the expressions, we have:

$$(a - b) + (b - c) = mk + mj$$

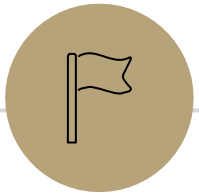
$$a - c = m(k + j)$$

Since k, j are integers, $k + j$ is an integer. Thus by definition of divides, $m \mid a - c$. Then by definition of congruence, $a \equiv c \pmod{m}$. Since a, b, c, m were arbitrary, the claim holds.

The Properties of Congruence We've Proven

- If $a \equiv b$ (mod m), then $b \equiv a$ (mod m).
- If $a \equiv b$ (mod m) and $c \equiv d$ (mod m), then $a + c \equiv b + d$ (mod m).
- If $a \equiv b$ (mod m) and $c \equiv d$ (mod m), then $ac \equiv bd$ (mod m).
- If $a \equiv b$ (mod m) and $b \equiv c$ (mod m), then $a \equiv c$ (mod m).

You may use these properties in your homework without re-proving them!



Primes, GCD, & LCM

Prime and Composite

Definition:

An integer $p > 1$ is prime iff its only positive divisors are 1 and p.

An integer $p > 1$ is composite iff it is not prime.

Least Common Multiple

Definition:

The Least Common Multiple of integers a and b (denoted $\mathbf{lcm}(a, b)$) is the smallest positive integer c such that $\mathbf{a} \mid \mathbf{c}$ and $\mathbf{b} \mid \mathbf{c}$.

For Example:

$\mathbf{lcm}(4, 6) = 12$

$\mathbf{lcm}(14, 20) = 140$

$\mathbf{lcm}(45, 60) = 180$

$\mathbf{lcm}(13, 1) = 13$

Greatest Common Divisor

Definition:

The Greatest Common Divisor of integers a and b (denoted $\gcd(a, b)$) is the largest integer c such that $c \mid a$ and $c \mid b$.

For Example:

$\gcd(99,18) = 9$

$\gcd(100, 125) = 25$

$\gcd(7,11) = 1$

$\gcd(13,0) = 13$

Calculating the GCD: Approach 1

Fundamental Theorem of Arithmetic: Every positive integer greater than 1 has a unique prime factorization.

Approach 1 to finding $\mathbf{gcd}(a, b)$:

- Find the prime factorization of a
- Find the prime factorization of b
- Identify all common prime factors.
- Multiply the common prime factors together. This is the GCD.

GCD facts

1. If a is a positive integer, $\gcd(a,0) = a$

Main Idea of Proof: a is a common divisor ($a = 1 \cdot a$; $0 = 0 \cdot a$); larger numbers don't divide a (for positive numbers, if $x|y$ then $x \leq y$)

2. If a and b are positive integers, then $\gcd(a,b) = \gcd(b, a \,\%\, b)$

For example:

$$\gcd(10,6) = \gcd(6,4)$$

$$\gcd(110,30) = \gcd(30,20)$$

Why is 2 true? The proof isn't easy, it's at the end of this deck.

Why should you care?

Calculating the GCD: Approach 2

Euclid's Algorithm. To find $\mathbf{gcd}(a, b)$:

- Repeatedly use $\mathbf{gcd}(a, b) = \mathbf{gcd}(b, a \,\%\, b)$ to reduce numbers
- Stop once you reach $\mathbf{gcd}(\mathrm{c}, 0)$. Return c.

For Example:

$$\begin{aligned}\mathbf{gcd}(660,126) &= \mathbf{gcd}(126,30)\\ &= \mathbf{gcd}(30,6)\\ &= \mathbf{gcd}(6,0)\\ &= 6\end{aligned}$$

Euclid's Algorithm in Java

```
// assumes a >= 0 and b >= 0
public int gcd(int a, int b) {
     if (b == 0) {
          return a;
     } else {
          return gcd(b, a % b);
     }
}
```

So…what's it good for?

Remember everything we're learning contributes to us eventually understanding RSA. This is a key step in generating keys.

Suppose I want to solve $7x \equiv 1 \ (mod\ n)$

Just multiply both sides by $\frac{1}{7}$…

Oh wait. We want a number to multiply by 7 to get 1.

What number can we pick?

Solving in Modular Arithmetic

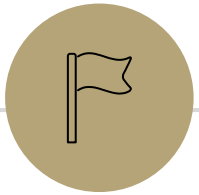
Solve: $7x \equiv 1 \pmod{10}$

Solution: $x \equiv 3 \pmod{10}$ (Guess and check)

None of our properties so far help us solve this.

3 is called the multiplicative inverse of 7 modulo 10, i.e. the value x such that $7x \equiv 1 \pmod{10}$.

We will use something called Bézout's Theorem to extend the Euclidean Algorithm to find multiplicative inverses.



Bézout’s Theorem

Bézout's Theorem

Bézout's Theorem

If a and b are positive integers, then there exist integers s and t such that

gcd(a,b)= $sa + tb$

So…what's it good for?

Suppose I want to solve $8x \equiv 3(mod\ n)$

Just multiply both sides by $\frac{1}{8}$…

We once again want to find the multiplicative inverse of 8 (mod n).

If the $\gcd(8, n) = 1$
Then by Bézout's Theorem, $s \cdot 8 + t \cdot n = 1$, so $8s - 1 = -tn$ i.e.
$n|(8s - 1)$ so $8s \equiv 1(mod\ n)$.
So the s from Bézout's Theorem is what we should multiply by!

Ok…how am I supposed to find s, t?

It turns out that while you're calculating the GCD (using Euclid's Algorithm), you can keep some extra information recorded, and end up with the s, t for Bézout's Theorem

This is called the "Extended Euclidian algorithm"

We'll see an example of running the Extended Euclidean Algorithm at the start of next lecture.

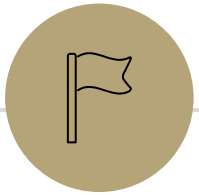
Todo

Tonight:

Start HW3 Today if you haven’t already!

CC 9 due Wednesday at noon

HW2 Feedback will be released soon!



[Extra Material]
Proving a key fact about GCDs

gcd(a,b) = gcd(b, a % b)

Let $\mathrm{x} = \gcd(a, b)$ and $y = \gcd(b, a\%b)$.

We show that y is a common divisor of a and b.

By definition of gcd, $y|b$ and $y|(a\%b)$. So it is enough to show that $y|a$.

Applying the definition of divides we get $b = yk$ for an integer k, and $(a\%b) = yj$ for an integer j.

By definition of mod, $a\%b$ is $a = qb + (a\%b)$ for an integer q.

Plugging in both of our other equations:

$a = qyk + yj = y(qk + j)$. Since q, k, and j are integers, $y|a$. Thus y is a common divisor of a, b and thus $y \leq x$.

gcd(a,b) = gcd(b, a % b)

Let $\mathrm{x} = \gcd(a, b)$ and $y = \gcd(b, a\%b)$.

We show that x is a common divisor of b and $\mathrm{a}\%b$.

By definition of gcd, $\mathrm{x}|b$ and $x|a$. So it is enough to show that $\mathrm{x}|(a\%b)$.

Applying the definition of divides we get $b = xk'$ for an integer k', and $\mathrm{a} = xj'$ for an integer j'.

By definition of mod, $a\%b$ is $a = qb + (a\%b)$ for an integer q

Plugging in both of our other equations:

$xj' = qxk' + a\%b$. Solving for $a\%b$, we have $a\%b = xj' - qxk' = x(j' - qk')$. So $x|(a\%b)$. Thus x is a common divisor of $b, a\%b$ and thus $x \leq y$.

gcd(a,b) = gcd(b, a % b)

Let $\mathrm{x} = \gcd(a, b)$ and $y = \gcd(b, a\%b)$.

We show that x is a common divisor of b and $\mathrm{a}\%b$.

We have shown $x \leq y$ and $y \leq x$.

Thus $x = y$, and $\gcd(a, b) = \gcd(b, a\%b)$.