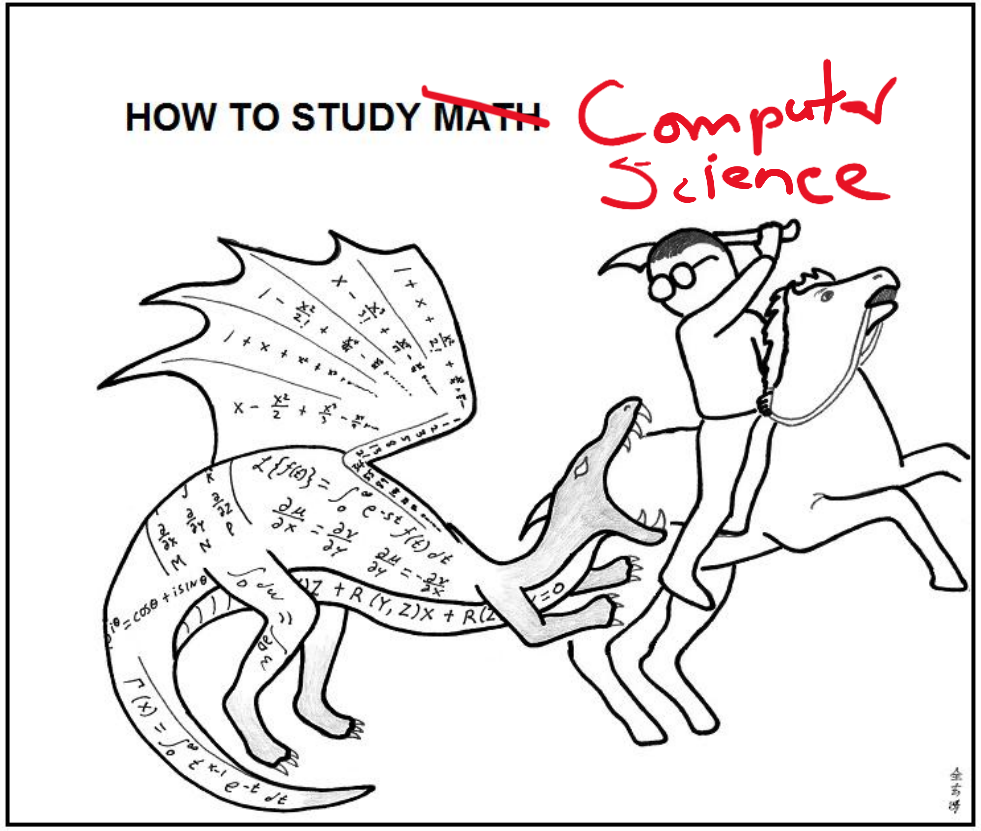


Don't just read it; fight it!

--- Paul R. Halmos

https://abstrusegoose.com/353

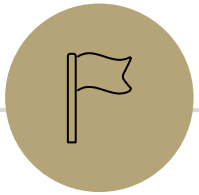
Number Theory

CSE 311 Summer 2025
Lecture 8

Announcements

- HW3 is out and due Wednesday!
  - Please start early- this HW is a significant step up from HW1 and HW2

- HW1 Resubmission is due tonight
  - Make sure to follow all resubmission directions to ensure your revised work is graded



Review

Direct Proof Steps

These are the usual steps. We'll see different outlines in the future!!

- Introduction
  - Declare an arbitrary variable for each ∀ quantifier
  - Assume the left side of the implication
- Core of the proof
  - Unroll the predicate definitions
  - Manipulate towards the goal (using creativity, algebra, etc.)
  - Reroll definitions into the right side of the implication
- Conclude that you have proved the claim

Proof by Contrapositive

Proof by contrapositive is another strategy for proving statements of the form $\forall x(P(x) \rightarrow Q(x))$.

The strategy is to prove the contrapositive, i.e. prove $\forall x \left(\neg \mathrm{Q}(x) \rightarrow \neg \mathrm{P}(x)\right)$

Remember, an implication is equivalent to its contrapositive!

Signs you might want to use proof by contrapositive

1. The hypothesis of the implication you're proving has a "not" in it (that you think is making things difficult)

2. The target of the implication you're proving has an "or" or "not" in it.

3. There's a step that is difficult forward, but easy backwards

   e.g., taking a square-root forward, squaring backwards.

4. You get halfway through the proof and you can't "get ahold of" what you're trying to show.

   e.g., you're working with a "not equal" instead of an "equals" or "every thing doesn't have this property" instead of "some thing does have that property"

All of these are reasons you **might** want contrapositive. Sometimes you just have to try and see what happens!

Proof of a Biconditional

Recall that biconditionals are statements of the form:
$\forall x\big(\mathrm{P}(x) \leftrightarrow \mathrm{Q}(x)\big)$

The strategy is to prove such statements is to prove an implication in both directions. I.e. prove $\forall x(\mathrm{P}(x) \to \mathrm{Q}(x)) \wedge \forall x(\mathrm{Q}(x) \to \mathrm{P}(x))$.

$$\begin{aligned}\forall x\ \big(P(x) \leftrightarrow Q(x)\big) &\equiv \forall x\ \big(P(x) \to Q(x) \wedge Q(x) \to P(x)\big)\\ &\equiv \forall x\big(P(x) \to Q(x)\big) \wedge \forall x(Q(x) \to P(x))\end{aligned}$$

Proof of a Biconditional

Prove: For an integer x, $2x + 3 = 15$ if and only if $x = 6$.

$\Rightarrow$ Let x be an arbitrary integer. Suppose $2x + 3 = 15$.

Then $2x = 12$. Thus, $x = 6$

Since x was arbitrary, for all integers x if $2x + 3 = 15$ then $x = 6$.

$\Leftarrow$ Let x be an arbitrary integer. Suppose $x = 6$.

Consider $2x + 3$:

$$2x + 3 = 2(6) + 3 = 12 + 3 = 15$$

Since x was arbitrary, for all integers x if $x = 6$ then $2x + 3 = 15$.

Proof by Cases

Proof by cases is the strategy of:

1. Breaking your assumption(s) into smaller cases.

   Be careful to make sure that your cases are exhaustive (cover all of the possible scenarios). It's ok if they have overlap though.

2. Proving that the claim holds in all of these cases.

Formally: $(P \vee Q) \rightarrow R \equiv (P \rightarrow R) \wedge (Q \rightarrow R)$.

5 numbers: Proof by Cases

Suppose that $x_1, \ldots, x_5$ are real numbers such that $x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5$ and $x_1 + x_2 + x_3 + x_4 + x_5 = 50$. Prove that $x_1 + x_2 \leq 20$.

Let x_1, x_2, x_3, x_4, x_5 be arbitrary real numbers such that $x_1 \leq x_2 \leq x_3 \leq x_4 \leq x_5$ and $x_1 + x_2 + x_3 + x_4 + x_5 = 50$.

Case 1: $x_2 \leq 10$. Then since $x_1 \leq x_2$, $x_1 \leq 10$. So $x_1 + x_2 \leq 20$, as desired.

Case 2: $x_2 > 10$. Then since $x_3, x_4, x_5 \geq x_2$, we have that $x_3 > 10$, $x_4 > 10$, $x_5 > 10$. So $x_3 + x_4 + x_5 > 30$. Thus $x_1 + x_2 < 20$, as desired.

Since $x_1, \ldots, x_5$ were arbitrary, our cases were exhaustive, and the claim holds in each case, we've proven our claim.

Existence Proof

Prove: There is some prime number p such that $p + 6$ and $p + 8$ are also prime.

What's the claim in logic?

$$\exists p(\text{Prime}(p) \wedge \text{Prime}(p + 6) \wedge \text{Prime}(p + 8))$$

How would we prove this claim?

Provide such a prime number.

Existence Proof

Prove: There is some prime number p such that $p + 6$ and $p + 8$ are also prime.

Consider $p = 5$. Then $p + 6 = 11$ is also prime, as is $p + 8 = 13$.

Proof by Counterexample

A single example can't *prove* a ∀ statement.

A single counterexample can *disprove* a ∀ statement.

For example, to disprove "all professors like pizza", you must find a professor who does not like pizza.

In formal logic:

$$\neg\forall x\,\big(P(x)\rightarrow Q(x)\big) \equiv \exists x\,\neg\big(P(x)\rightarrow Q(x)\big)$$ DeMorgan's Law for Quantifiers

$$\equiv \exists x\,\neg\big(\neg P(x)\vee Q(x)\big)$$ Law of Implication

$$\equiv \exists x\,\big(\neg\neg P(x)\wedge\neg Q(x)\big)$$ DeMorgan's Law

$$\equiv \exists x\,\big(P(x)\wedge\neg Q(x)\big)$$ Double Negation

Proof by Counterexample

For all real numbers a, b, c, if $|a + c| = |b + c|$, then $|a| = |b|$.

This claim is false. Disprove!

Consider $a = -6, b = 4, c = 1$. Certainly $|a| \neq |b|$. Observe that:

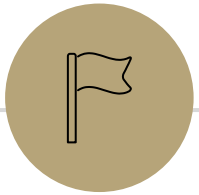
$|a + c| = |-6 + 1| = |-5| = 5$

$|b + c| = |4 + 1| = |5| = 5$

So this is a counterexample to the claim.

Proof Strategies So Far

- Direct Proof
- Proof by Contrapositive
- Proof of Biconditional
- Proof by Cases
- Proof of Existence
- Proof by Counterexample



Warm Up: Prove or Disprove

Prove or Disprove

- In practice, we don't usually know if a claim is true or false beforehand
- We want to prove the statement if it's true, and disprove it if it's false.
- Strategy:
  - Play around with many examples in an attempt to show that the claim is false
  - If the claim is false, hopefully you'll find a counterexample
  - If the claim is true, you'll gain intuition for why from the examples

Prove or Disprove

Identify if the following claims are true or false, and then prove or disprove.

1. For all positive integers n, $n^2 + 3n + 1$ is always prime.

2. For all positive integers n, the sum $1 + 2 + \cdots + n$ is equal to $\frac{n(n+1)}{2}$.

3. For every real number n, $n^2 \geq n$.

4. For an integer n, $3n^2 + n + 10$ is always even.

Prove or Disprove

Identify if the following claims are true or false, and then prove or disprove.

1. For all positive integers n, $n^2 + 3n + 1$ is always prime.

   False: e.g. $n = 6$ gives $36 + 18 + 1 = 55$.

2. For all positive integers n, the sum $1 + 2 + \cdots + n$ is equal to $\frac{n(n+1)}{2}$.

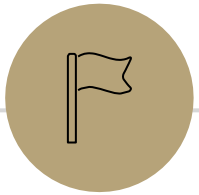
   True. Hint to prove: regroup $1 + 2 + \ldots + n - 1 + n$ into pairs $(1 + n) + (2 + (n - 1)) + \ldots$

3. For every real number n, $n^2 \geq n$.

   False: e.g. $n = \frac{1}{2}$, since $\frac{1}{4} < \frac{1}{2}$.

4. For an integer n, $3n^2 + n + 10$ is always even.

   True. Hint to prove: break into the cases that n is even and n is false.



Some Final Proof Tips

Proof Style

We use predicate logic to make the proof claim very precise. However, please write the actual proofs in English, not logic!

E.g. for all integers x, if x is odd then $x + 1$ is even.

Good: Let x be arbitrary. Suppose x is odd. Then $x = 2k + 1$ for some integer k …

Bad: Let x be arbitrary. Suppose $\mathbf{Odd}(x)$. Then $\exists k\ (x = 2k + 1)$…

Proof Tip: Without Loss of Generality

If you're writing a proof with 2+ very similar cases, you can use the phrase:

Assume without loss of generality that we are in Case 1....

For example:

Case 1: x is red and y is blue, we want to show $x + y$ is purple.

Case 2: x is blue, y is red, we want to show $x + y$ is purple.

In my proof: "Observe that there are two cases. We can assume without loss of generality that x is red and y is blue"

Logical Ordering

When doing a proof, we often work from both sides…

But we have to be careful!

When you read from top to bottom, every step has to follow only from what's **before** it, not after it.

Suppose our target is q and I know $q \to p$ and $r \to q$.

What can I put as a "new target?"

Logical Ordering

So why have all our prior steps been ok backward?

They've all been either:

A definition (which is always an "if and only if")

An algebra step that is an "if and only if"

Even if your steps are "if and only if" you still have to put everything in order – start from your assumptions, and only assert something once it can be shown.

A bad proof

Claim: if x is positive then $x + 5 = -x - 5$.

$x + 5 = -x - 5$

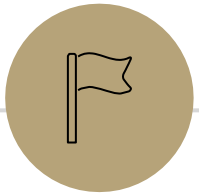
$|x + 5| = |-x - 5|$

$|x + 5| = |-(x + 5)|$

$|x + 5| = |x + 5|$

$0 = 0$

This claim is **false** – if you're trying to do algebra, you need to start with an equation you know (say $x = x$ or $2 = 2$ or $0 = 0$) and expand to the equation you want.



Computer-Verifiable Proofs

Recall: Proofs are written for an audience

Computer Science Theorist

"The proof is clear ☺"

Computer

Possibly many steps to show $1 + 1 = 2$

Computer-Verifiable Proofs

How do they work?

1. Write down all the facts that we know.
2. Combine facts into new facts using a set of known rules.

   Example Rule: Modus Ponens

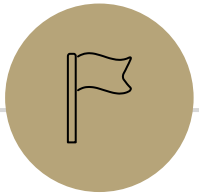
   If $p \to q$ and p are known, then q is known

3. Continue until we reach what we want to show.

Computer-Verifiable Proofs

If n and m are odd, then $n + m$ is even.

1.	Let x be an arbitrary integer.		
2.	Let y be an arbitrary integer.		
	3.1.	$\text{Odd}(x) \wedge \text{Odd}(y)$	[Assumption]
	3.2.	$\text{Odd}(x)$	[Elim $\wedge$: 3.1]
	3.3.	$\exists k\ (x = 2k + 1)$	[Definition of Odd, 3.2]
	3.4.	$x = 2k + 1$	[Elim $\exists$: 3.3]
	3.5.	$\text{Odd}(y)$	[Elim $\wedge$: 3.1]
	3.6.	$\exists k\ (y = 2k + 1)$	[Definition of Odd, 3.5]
	3.7.	$y = 2j + 1$	[Elim $\exists$: 3.7]
	3.8.	$x + y = 2k + 1 + 2j + 1$	[Algebra: 3.4, 3.7]
	3.9.	$x + y = 2(k + j + 1)$	[Algebra: 3.8]
	3.10.	$\exists r\ (x + y = 2r)$	[Intro $\exists$: 3.9]
	3.11.	$\text{Even}(x + y)$	[Definition of Even, 3.10]
3.	$\text{Odd}(x) \wedge \text{Odd}(y) \rightarrow \text{Even}(x + y)$		[Direct Proof Rule]
4.	$\forall m(\text{Odd}(x) \wedge \text{Odd}(m) \rightarrow \text{Even}(x + m))$		[Intro $\forall$: 2,3]
5.	$\forall n \forall m(\text{Odd}(n) \wedge \text{Odd}(m) \rightarrow \text{Even}(n + m))$		[Intro $\forall$: 1,4]



Number Theory

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.

Modular Arithmetic

- Arithmetic over a finite domain
- In computing, almost all computations are over a finite domain

Modular Arithmetic

```
public class Test {
        final static int SEC_IN_YEAR =  365*24*60*60;
        public static void main(String args[]) {
                System.out.println( “I will be alive for at least ” +   SEC_IN_YEAR * 100 + “ seconds.” );
        }
}
```

```
I will be alive for -1141367296 seconds.
```

Framing Device

We're going to give you enough background to (mostly) understand the RSA encryption system.

Key generation [edit]

The keys for the RSA algorithm are generated in the following way:

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random and should be similar in magnitude but differ in length by a few digits to make factoring harder.[2] Prime integers can be efficiently found using a primality test.
   - p and q are kept secret.
2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
   - n is released as part of the public key.
3. Compute $\lambda(n)$, where λ is Carmichael's totient function. Since $n = pq$, $\lambda(n) = \operatorname{lcm}(\lambda(p), \lambda(q))$, and since p and q are prime, $\lambda(p) = \varphi(p) = p - 1$, and likewise $\lambda(q) = q - 1$. Hence $\lambda(n) = \operatorname{lcm}(p - 1, q - 1)$.
   - $\lambda(n)$ is kept secret.
   - The lcm may be calculated through the Euclidean algorithm, since $\operatorname{lcm}(a, b) = |ab|/\gcd(a, b)$.
4. Choose an integer e such that $1 < e < \lambda(n)$ and $\gcd(e, \lambda(n)) = 1$; that is, e and $\lambda(n)$ are coprime.
   - e having a short bit-length and small Hamming weight results in more efficient encryption – the most commonly chosen value for e is $2^{16} + 1 = 65\,537$. The smallest (and fastest) possible value for e is 3, but such a small value for e has been shown to be less secure in some settings.[15]
   - e is released as part of the public key.
5. Determine d as $d \equiv e^{-1} \pmod{\lambda(n)}$; that is, d is the modular multiplicative inverse of e modulo $\lambda(n)$.
   - This means: solve for d the equation $d \cdot e \equiv 1 \pmod{\lambda(n)}$; d can be computed efficiently by using the extended Euclidean algorithm, since, thanks to e and $\lambda(n)$ being coprime, said equation is a form of Bézout's identity, where d is one of the coefficients.
   - d is kept secret as the *private key exponent*.

The *public key* consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the private (or decryption) exponent d, which must be kept secret. p, q, and $\lambda(n)$ must also be kept secret because they can be used to calculate d. In fact, they can all be discarded after d has been computed.[16]

Framing Device

We're going to give you enough background to (mostly) understand the RSA encryption system.

Key generation [edit]

Prime Numbers

The keys for the RSA algorithm are genera

1. Choose two distinct prime numbers p and q.
   - For security purposes, the integers p and q should be chosen at random and should be similar in magnitude but differ in length by a few digits to make factoring harder.[2] Prime integers can be efficiently found using a primality test.
   - p and q are kept secret.

Modular Arithmetic

2. Compute $n = pq$.
   - n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.
   - n is released as part of the public key.
3. Compute $\lambda(n)$, where λ is Carmichael's totient function. Since $n = pq$, $\lambda(n) = \operatorname{lcm}(\lambda(p), \lambda(q))$, and since p and q are prime, $\lambda(p) = \varphi(p) = p - 1$, and likewise $\lambda(q) = q - 1$. Hence $\lambda(n) = \operatorname{lcm}(p - 1, q - 1)$.
   - $\lambda(n)$ is kept secret.
   - The lcm may be calculated through the Euclidean algorithm, since $\operatorname{lcm}(a, b)$

Modular Multiplicative Inverse

4. Choose an integer e such that $1 < e < \lambda(n)$ and $\gcd(e, \lambda(n)) = 1$; that is, e and $\lambda(n)$ are cop
   - e having a short bit-length and small Hamming weight results in more efficient enc … he most commonly chosen value for e is $2^{16} + 1 = 65\,537$. The smallest (and fastest) possible value for e is 3, but such a small value for e has been shown to be less secure in some settings.[15]
   - e is released as part of the public key.

Bezout's Theorem

5. Determine d as $d \equiv e^{-1} \pmod{\lambda(n)}$; that is, d is the modular multiplicative inverse of e modulo $\lambda(n)$.
   - This means: solve for d the equation $d \cdot e \equiv 1 \pmod{\lambda(n)}$; d can be computed efficiently by using the extended Euclidean algorithm, since, thanks to e and $\lambda(n)$ being coprime, said equation is a form of Bézout's identity, where d is one of the coefficients.
   - d is kept secret as the *private key exponent*.

Extended Euclidian Algorithm

The *public key* consists of the modulus n and the public (or encryption) exponent e. The *private key* consists of the private (or decryp … t also be kept secret because they can be used to calculate d. In fact, they can all be discarded after d has been computed.[16]

Framing Device

We're going to give you enough background to (mostly) understand the RSA encryption system.

Encryption [edit]

After Bob obtains Alice's public key, he can send a message M to Alice.

To do it, he first turns M (strictly speaking, the un-padded plaintext) into an integer m (strictly speaking, the padded plaintext), such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c, using Alice's public key e, corresponding to

$$c \equiv m^e \pmod{n}.$$

This can be done reasonably quickly, even for very large numbers, using modular exponentiation. Bob then transmits c to Alice. Note that at least nine values of m will yield a ciphertext c equal to m,[22] but this is very unlikely to occur in practice.

Decryption [edit]

Alice can recover m from c by using her private key exponent d by computing

$$c^d \equiv (m^e)^d \equiv m \pmod{n}.$$

Given m, she can recover the original message M by reversing the padding scheme.

Framing Device

We're going to give you enough background to (mostly) understand the RSA encryption system.

Encryption [edit]

After Bob obtains Alice's public key, he can send a message M to Alice.

To do it, he first turns M (strictly speaking, the un-padded plaintext) into an integer m (strictly speaking, the padded plaintext), such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c, using Alice's public key e, corresponding to

$$c \equiv m^e \pmod{n}.$$

This can be done reasonably quickly, even for very large numbers, using modular exponentiation. Bob then transmits c to Alice. Note that at least nine values of m will yield a ciphertext c equal to m,[22] but this is very unlikely to occur in practice.

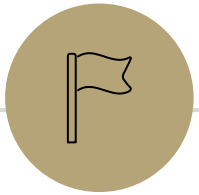
Modular Exponentiation

Decryption [edit]

Alice can recover m from c by using her private key exponent d by computing

$$c^d \equiv (m^e)^d \equiv m \pmod{n}.$$

Given m, she can recover the original message M by reversing the padding scheme.



Divisibility

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

Divides

Divides

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

Which of these are true?

$2|4$ $\quad$ $4|2$ $\quad$ $2|-2$

$5|0$ $\quad$ $0|5$ $\quad$ $1|5$

Divides

Divides

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

Which of these are true?

$2|4$ True

$4|2$ False

$2|-2$ True

$5|0$ True

$0|5$ False

$1|5$ True

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 $a = qd + r$.

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 $a = qd + r$.

q is referred to as the quotient

r is referred to as the remainder

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

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

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

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

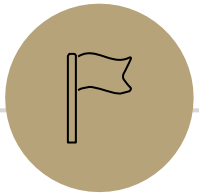
$25 = 5 \cdot 5 + \mathbf{0}$

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

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

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

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



Modular Arithmetic

Terminology

Java's % is an operator (like + or ·) you give it two numbers, it produces a number.

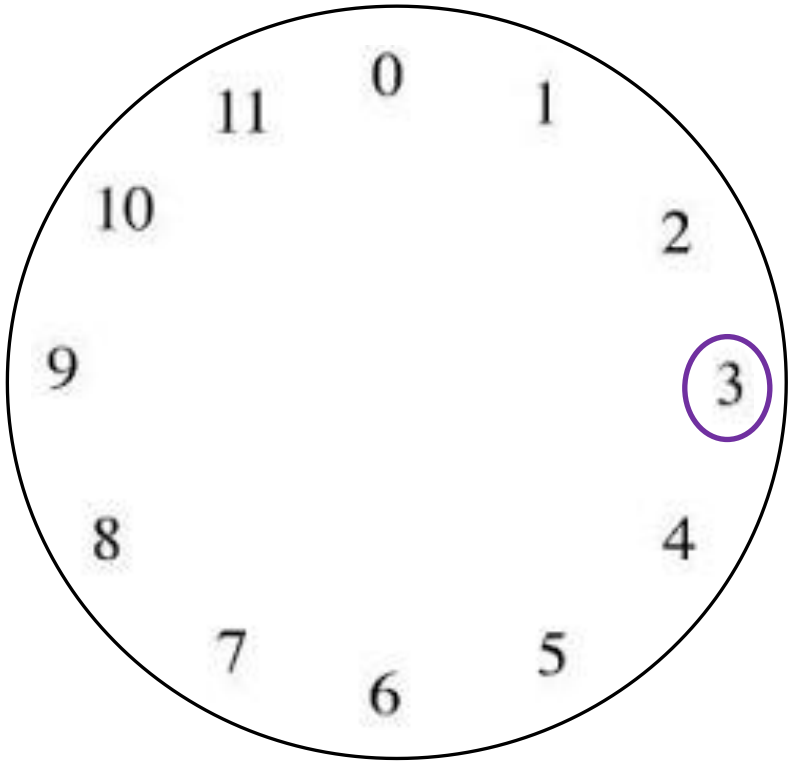
We're going to use the word "mod" to mean a closely related, but different thing.

The word "mod" in this class, refers to a set of rules

Modular Arithmetic: Like a Clock

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

What's $8 + 7$? 3

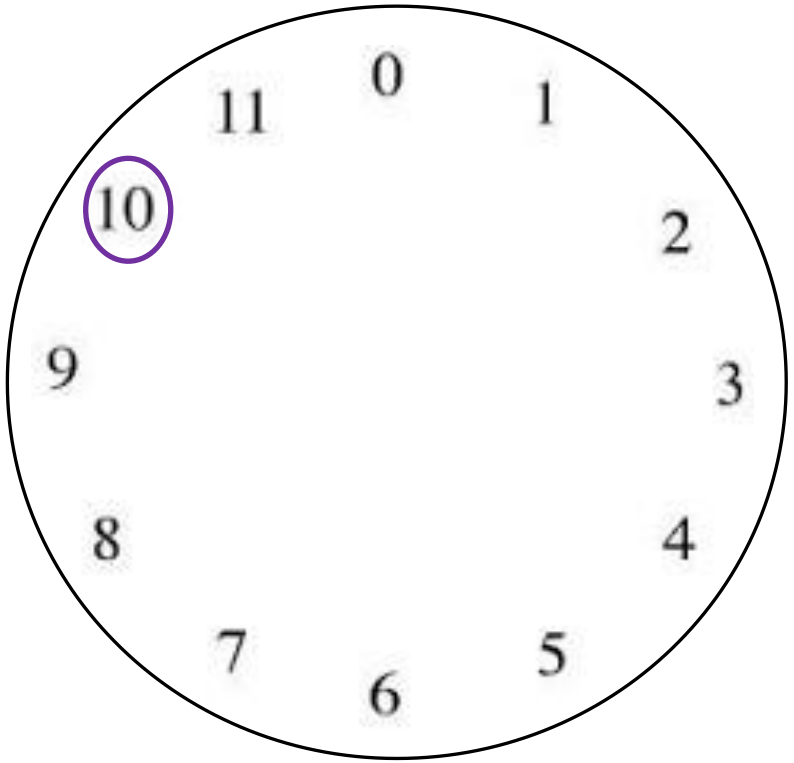


Observation
The solution is a % 12.

Modular Arithmetic: Like a Clock

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

What's $3 - 5$? 10

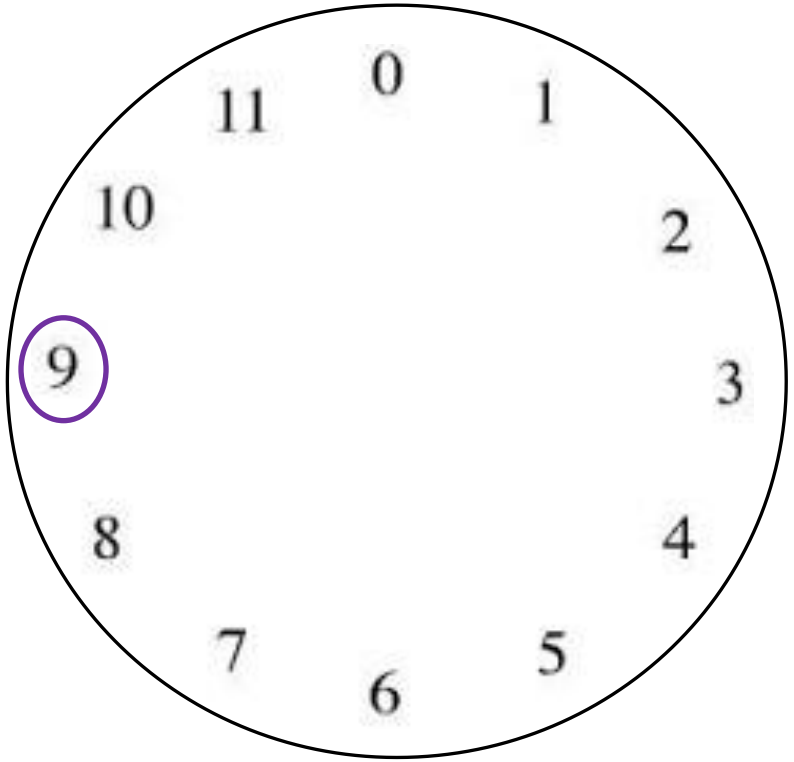


Observation
The solution is $a \,\%\, 12$.

Modular Arithmetic: Like a Clock

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

What's $3 \cdot 7$? 9

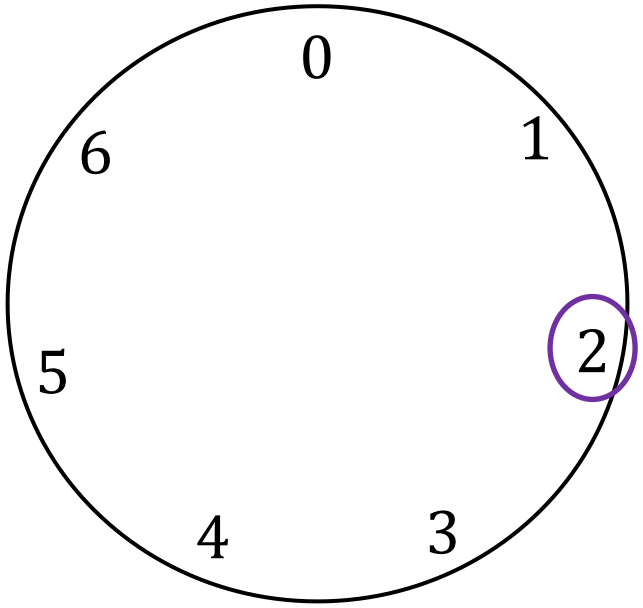


Observation
The solution is a % 12.

Modular Arithmetic: Generalizing

We can extend modular arithmetic to clocks of any positive integer size.

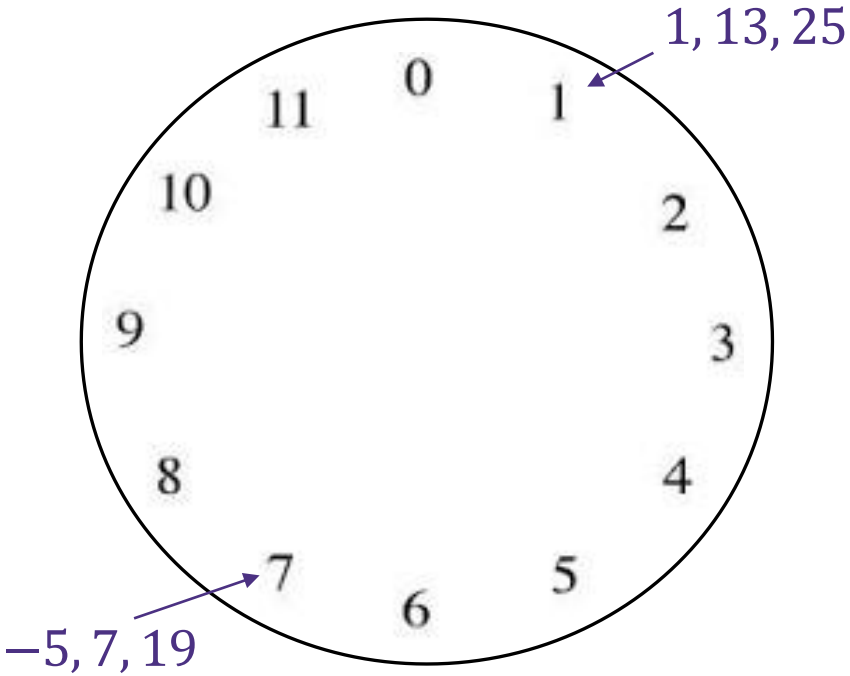
E.g. $3 + 6$ in arithmetic mod 7 is 2



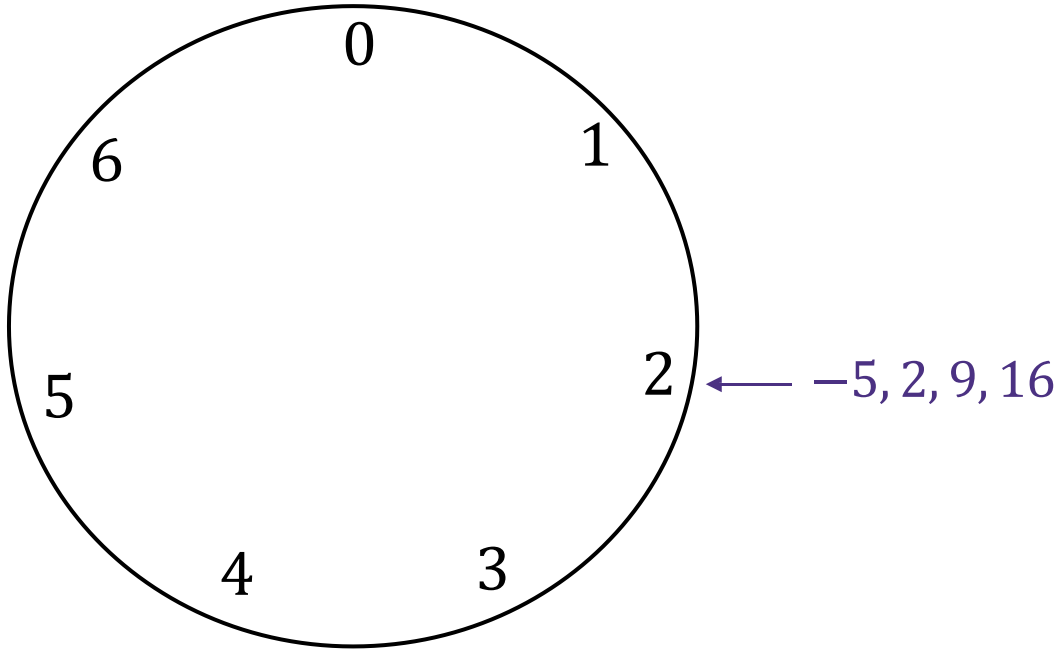
“Sameness”

In modular arithmetic, many numbers have a notion of “sameness”.

Arithmetic mod 12:



Arithmetic mod 7:



Modular Arithmetic

To say "the same" we don't want to use $=$ … that means the normal $=$

We'll write $13 \equiv 1 (\mathrm{mod}\ 12)$
$\equiv$ because "equivalent" is "like equal," and the "modulus" we're using in parentheses at the end so we don't forget it.

(we'll also say "congruent mod 12")

The notation here is bad. We all agree it's bad. Most people still use it.

$13 \equiv_{12} 1$ would have been better. "mod 12" is giving you information about the $\equiv$ symbol, it's not operating on 1.

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 $a \,\%\, m = b \,\%\, m$.

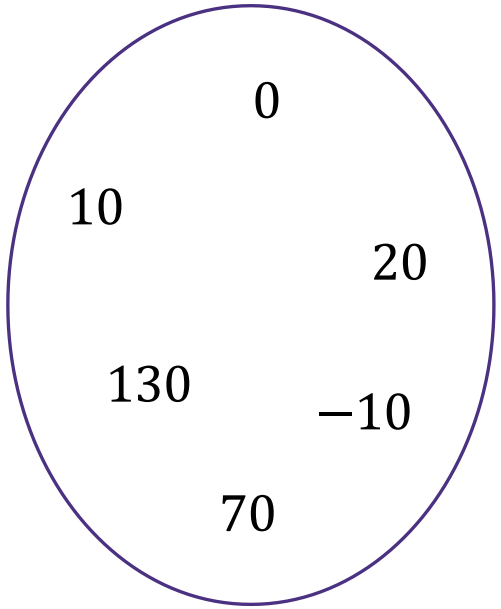
We will actually prove that the two notions are the same. But, the formal definition is much easier to use in proofs.

Intuition

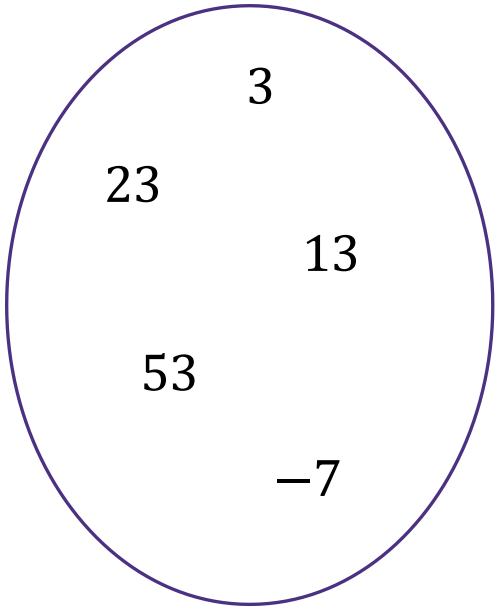
Definition: $a \equiv b \pmod{m}$ is defined as $m \mid (a - b)$

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

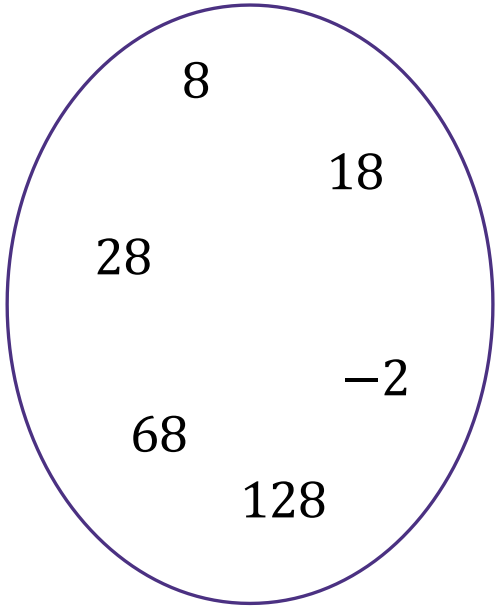
Here we have some groups of numbers that are congruent mod 10.



Congruent to 0



Congruent to 3



Congruent to 8

Don’t lose your intuition!

Let’s check that we understand “intuitively” what mod means:

$$x \equiv 0 \pmod 2$$

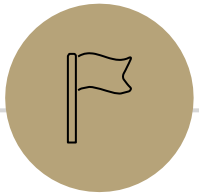
“x is even” Note that negative (even) x values also make this true.

$$-1 \equiv 19 \pmod 5$$

This is true! They both have remainder 4 when divided by 5.

$$y \equiv 2 \pmod 7$$

This is true as long as $y = 2 + 7k$ for some integer k



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

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

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 $a + c \equiv b + d \pmod{m}$.

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: $ac - bd = mx$

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 $c - d = mj$.

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 $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

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

Todo

Tonight:

Take a look at HW3 today or over the weekend- plan ahead for this HW taking longer

Finish your HW1 resubmissions by 11:59 pm tonight!

CC8 due Monday at noon