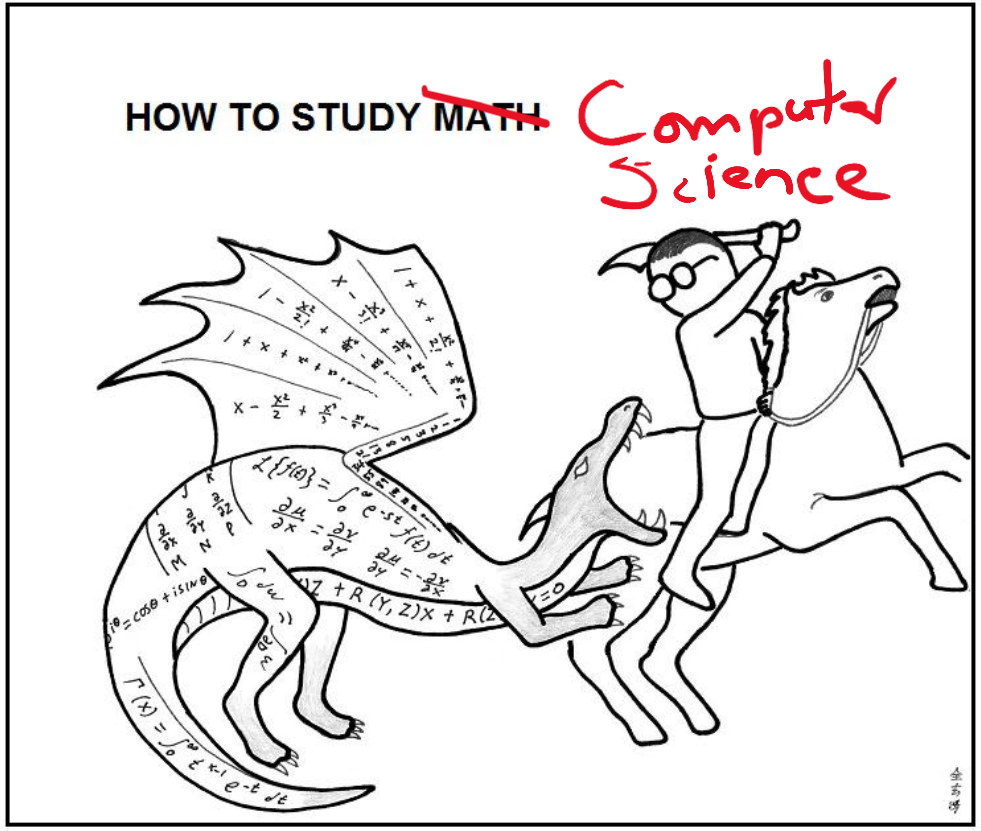


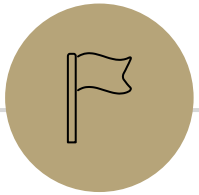
Don't just read it; fight it!

--- Paul R. Halmos

https://abstrusegoose.com/353

Number Theory

CSE 311 Autumn 2025
Lecture 10



Extra Example

Inference Proof with Even/Odd definitions

If x is even, then x^2 is even.

You want to prove "$\forall x(\mathbf{Even}(x) \rightarrow \mathbf{Even}(x^2))$

What variable(s) do you need (are they arbitrary?)

What do you expect the very big proof steps to be?

1. Are you using the direct proof rule?
2. If so, what will your assumption be and what are you targeting in that subproof?
3. What quantifiers do you need to introduce/eliminate
4. Any other big steps you can think of?

If x is even, then x^2 is even. (skeleton)

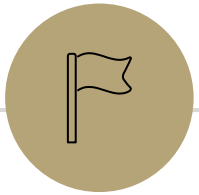
1. Let a be arbitrary	
2.1 $\texttt{Even}(a)$	Assumption
2.2 $????'$	?
	?
	?
	?
	?
2.7 $\texttt{Even}(a^2)$	Definition of Even
3. $\texttt{Even}(a) \rightarrow \texttt{Even}(a^2)$	Direct Proof Rule (2.1-2.7)
4. $\forall x(\texttt{Even}(x) \rightarrow \texttt{Even}(x^2))$	Intro ∀ (3)

If x is even, then x^2 is even. (inference pf)

1. Let a be arbitrary	
2.1 $\texttt{Even}(a)$	Assumption
2.2 $\exists y\,(2y = a)$	Definition of Even (2.1)
2.3 $2z = a$	Elim ∃(2.2)
2.4 $a^2 = 4z^2$	Algebra (2.3)
2.5 $a^2 = 2 \cdot 2z^2$	Algebra (2.4)
2.6 $\exists w(2w = a^2)$	Intro ∃ (2.5)
2.7 $\texttt{Even}(a^2)$	Definition of Even
3. $\texttt{Even}(a) \rightarrow \texttt{Even}(a^2)$	Direct Proof Rule (2.1-2.7)
4. $\forall x(\texttt{Even}(x) \rightarrow \texttt{Even}(x^2))$	Intro ∀ (3)

If x is even, then x^2 is even. (inference and English)

1. Let a be arbitrary		
2.1 $\texttt{Even}(a)$	Assumption	Let x be an arbitrary even integer. By definition, there is an integer y such that $2y = x$.
2.2 $\exists y\,(2y = a)$	Definition of Even (2.1)	
2.3 $2z = a$	Elim $\exists(2.2)$	
2.4 $a^2 = 4z^2$	Algebra (2.3)	Squaring both sides, we see that $x^2 = 4y^2 = 2 \cdot 2y^2$.
2.5 $a^2 = 2 \cdot 2z^2$	Algebra (2.4)	
2.6 $\exists w(2w = a^2)$	Intro $\exists$ (2.5)	Because y is an integer, $2y^2$ is also an integer, and x^2 is two times an integer. Thus x^2 is even by the definition of even.
2.7 $\texttt{Even}(a^2)$	Definition of Even	
3. $\texttt{Even}(a) \rightarrow \texttt{Even}(a^2)$	Direct Proof Rule (2.1-2.7)	
4. $\forall x(\texttt{Even}(x) \rightarrow \texttt{Even}(x^2))$	Intro $\forall$ (3)	Since x was an arbitrary even integer, we can conclude that for every even x, x^2 is also even.



Why 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.

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 … 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.

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.

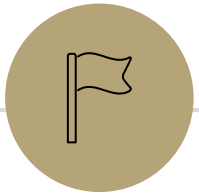
Modular Exponentiation

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.



Number Theory Definitions

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?

$2|4$

$4|2$

$2|-2$

$5|0$

$0|5$

$1|5$

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

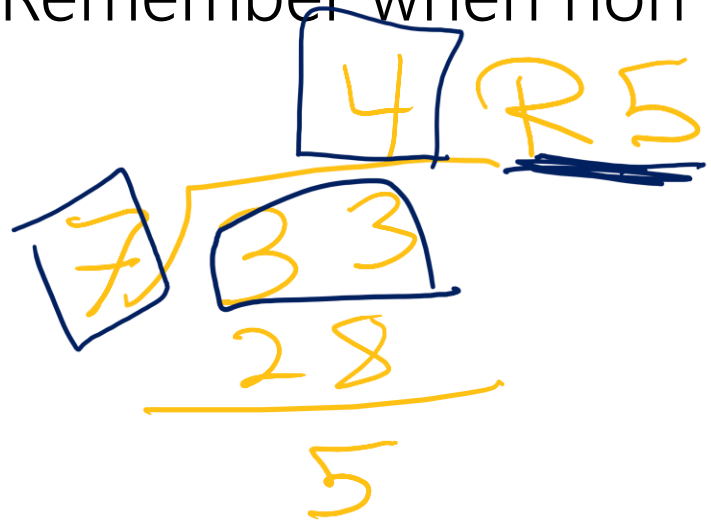
$1|5$ True

A useful theorem

The Division Theorem

For every $a \in \mathbb{Z}$, $d \in \mathbb{Z}$ with $d > 0$
There exist *unique* integers q, r with $0 \leq r < d$
Such that $a = dq + r$

Remember when non integers were still secret, you did division like this?



q is the "quotient"
r is the "remainder"

Unique

The Division Theorem

For every $a \in \mathbb{Z}$, $d \in \mathbb{Z}$ with $d > 0$
There exist *unique* integers q, r with $0 \leq r < d$
Such that $a = dq + r$

"unique" means "only one"....but be careful with how this word is used.

r is unique, **given** a, d. – it still depends on a, d but once you've chosen a and d

"unique" is not saying $\exists r \forall a, d \quad P(a, d, r)$
It's saying $\forall a, d \exists r [P(a, d, r) \wedge [P(a, d, x) \rightarrow x = r]]$

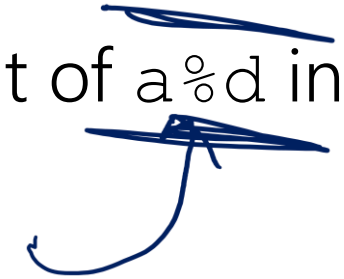
A useful theorem

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
There exist *unique* integers q, r with $0 \leq r < d$
Such that $a = dq + r$

The q is the result of `a/d` (integer division) in Java

The r is the result of `a%d` in Java



That's slightly a lie, r is always non-negative, Java's % operator sometimes gives a negative number.

Terminology

a % b

You might have called the % operator in Java “mod”

We’re going to use the word “mod” to mean a closely related, but different thing.

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

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

Modular Arithmetic

"arithmetic mod 12" is familiar to you. You do it with clocks.

What's 3 hours after 10 o'clock?

1 o'clock. You hit 12 and then "wrapped around"

"13 and 1 are the same, mod 12" "-11 and 1 are the same, mod 12"

We don't just want to do math for clocks – what about if we need to talk about parity (even vs. odd) or ignore higher-order-bits (mod by 16, for example)

Modular Arithmetic

1%12

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

We'll write $13 \equiv 1 (\mathbf{mod}\ 12)$

$\equiv$ 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.

Modular Arithmetic

$a \equiv b \pmod{n}$

We need a definition! We can't just say "it's like a clock"

$a \% n = b \% n$

Pause what do you expect the definition to be?

Is it related to % ?

Modular Arithmetic

We need a definition! We can't just say "it's like a clock"

Pause what do you expect the definition to be?

Equivalence in modular arithmetic

Let a, b, n be integers with $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

Huh?

Long Pause

It's easy to read something with a bunch of symbols and say "yep, those are symbols." and keep going

STOP Go Back.

You have to *fight* the symbols they're probably trying to pull a fast one on you.

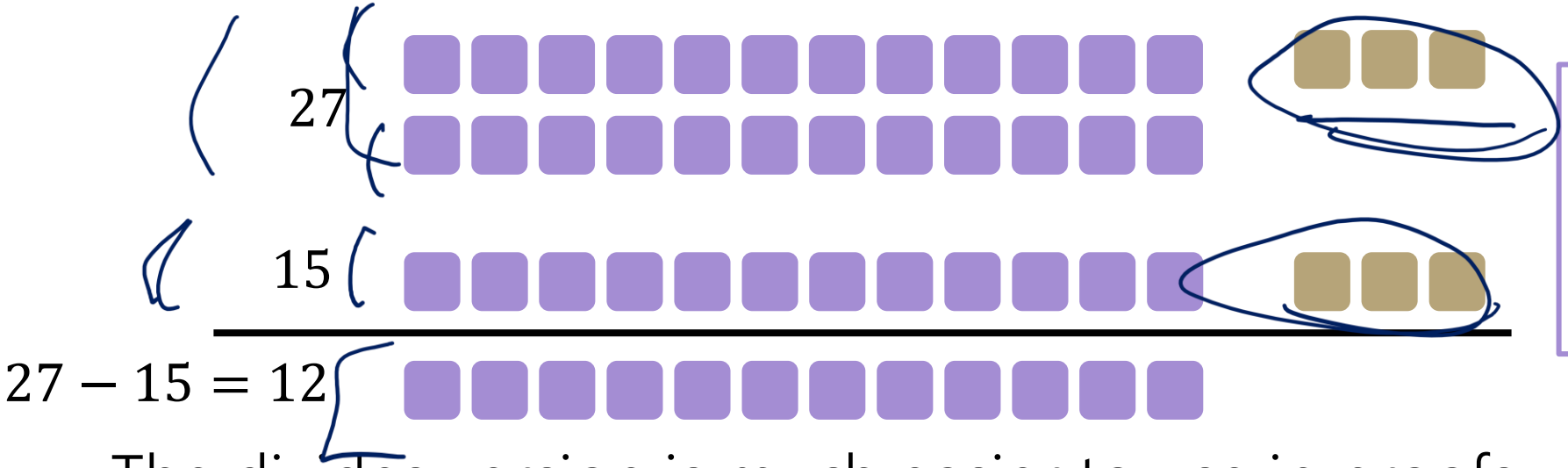
Same goes for when I'm presenting a proof – you shouldn't just believe me – I'm wrong all the time!

You should be *trying* to do the proof with me. Where do you think we're going next?

Why?

Here's the short version:

It really is equivalent to "what we expected"
`a%n=b%n` if and only if $n|(b-a)$



When you subtract, the remainders cancel. What you're left with is a multiple of 12.

The divides version is much easier to use in proofs…

Proof Practice

Over the next few weeks:

Practice direct proofs in English (formatting details, doing more examples)

See a few other proof techniques

Proof by contrapositive, proving an exists statement, proof by contradiction

All while learning some number theory.

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

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

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, n be integers with $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

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

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

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$,
and suppose $a \equiv b \pmod{n}$.

$a + c \equiv b + c \pmod{n}$

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

A proof

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

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

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$,
and suppose $a \equiv b \pmod{n}$.

By definition of mod, $\mathrm{n}|(b - a)$

By definition of divides, $nk = (b - a)$ for some integer k.

Adding and subtracting c, we have $nk = ([b + c] - [\mathrm{a} + \mathrm{c}])$.

Since k is an integer $n|([b + c] - [a + c])$

By definition of mod, $a + c \equiv b + c \pmod{n}$. Since a, b, c, n were arbitrary, the claim holds for all integers a, b, c and positive integers n.

You Try!

Claim: for all integers a, b, c, n with $n > 0$:
If $a \equiv b \ (mod\ n)$ then $ac \equiv bc \ (mod\ n)$

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 $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b - a)$

You try---skeleton

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

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

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$
and suppose $a \equiv b(mod\ n)$.

$ac \equiv bc\ (mod\ n)$

You try---the full proof

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

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

Proof:

Let a, b, c, n be arbitrary integers with $n > 0$
and suppose $a \equiv b (mod\ n)$.

By definition of mod $n|(b - a)$

By definition of divides, $nk = b - a$ for some integer k

Multiplying both sides by c, we have $n(ck) = bc - ac$.

Since c and k are integers, $n|(bc - ac)$ by definition of divides.

So, $ac \equiv bc\ (mod\ n)$, by the definition of mod. Since a, b, c, n were arbitrary, the claim holds for all integers a, b, c and positive integers n.

Don’t lose your intuition!

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

$x \equiv 0 \pmod 2$

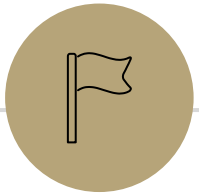
“x is even” Note that negative (even) x values also make this true.

$-1 \equiv 19 \pmod 5$

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



Small Techniques

Proof By [Counter]Example

To prove an existential statement (or disprove a universal statement), provide an example, and demonstrate that it is the needed example.

You don't have to explain where it came from! (In fact, you **shouldn't)**

Computer scientists and mathematicians like to keep an air of mystery around our proofs.

(or more charitably, we want to focus on just enough to believe the claim)

Skeleton of an Exists Proof

To show $\exists x(P(x))$

Consider x =[the value that will work]

[Show that x does cause $P(x)$ to be true.]

So [value] is the desired x.

You'll probably need some "scratch work" to determine what to set x to. That might not end up in the final proof!

Exists proofs

Suppose I claim that for all integers, if x is even then $8|x^2$.

That…doesn't look right.

How do you prove me wrong?

Want to show: $\exists x(Even(x) \wedge \neg[8|x\text{^}2])$

Consider $x = 6$. Then x is even (since $6 = 3 \cdot 2$), but 8 does not divide 36 (as $36\%8 = 4$).

Proof By Cases

If x is prime then x^2 is odd or $2|x$.

We need two different arguments – one for 2 and one for all the other primes…

Proof By Cases

Let x be an arbitrary prime number

We divide into two cases.

Case 1: x is even

If x is even then $x = 2k$ for some integer k, this is the definitions of $2|x$.

Case 2: x is odd

If x is odd, then $x = 2j + 1$ for some integer j. Squaring, we get
$x^2 = 4j^2 + 4j + 1 = 2(2j^2 + 2j) + 1.$
Since j is an integer $2j^2 + 2j$ is as well, so x^2 is odd by definition.

In either case, x met the condition of $2|x$ or x^2 is odd, so the claim is true.

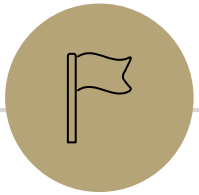
Proof By Cases

Make it clear how you decide which case your in.

It should be obvious your cases are “exhaustive”

Reach the same conclusion in each of the cases, and you can say you’ve got that conclusion no matter what (outside the cases).

Advanced version: sometimes you end up arguing a certain case “can’t happen”



(Optional) equivalence of % and $\equiv (mod\ n)$

The full proof

% and Mod

Other resources use mod to mean an operation (takes in an integer, outputs an integer). We will not in this course. mod only describes $\equiv$. It's not "just on the right hand side"

Define $a\%b$ to be "the r you get from the division theorem"
i.e. the integer r such that $0 \leq r < d$ and $a = bq + r$ for some integer q.

This is the "mod function"

I claim $a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$.

How do we show and if-and-only-if?

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Backward direction:

Suppose $a \equiv b(mod\ n)$

$a\%n = (b - nk)\%n = b\%n$

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Backward direction:

Suppose $a \equiv b(mod\ n)$

$n|b - a$ so $nk = b - a$ for some integer k. (by definitions of mod and divides).

So $a = b - nk$

Taking each side $\%n$ we get:

$a\%n = (b - nk)\%n = b\%n$

Where the last equality follows from k being an integer and doing k applications of the identity we proved in the warm-up.

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Show the forward direction:

If $a\%n = b\%n$ then $a \equiv b(mod\ n)$.

This proof is a bit different than the other direction.

Remember to work from top and bottom!!

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b\ (mod\ n)$ if and only if $n|(b - a)$

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
There exist ***unique*** integers q, r with $0 \leq r < d$ Such that $a = dq + r$

$a\%n = b\%n$ if and only if $a \equiv b(mod\ n)$

Forward direction:

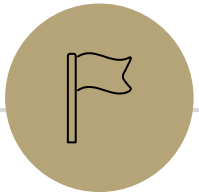
Suppose $a\%n = b\%n$.

By definition of $\%, a = kn + (a\%n)$ and $b = jn + (b\%n)$ for integers k, j

Isolating $a\%n$ we have $a\%n = a - kn$. Since $a\%n = b\%n$, we can plug into the second equation to get: $b = jn + (a - kn)$

Rearranging, we have $b - a = (j - k)n$. Since k, j are integers we have $n|(b - a)$.

By definition of mod we have $a \equiv b(mod\ n)$.



Extra Practice

Does Order matter?

Show that if $a \equiv b(mod\ n)$ then $b \equiv a\ (mod\ n)$.

Now that we've proven this, we aren't going to care whether you write $n|(b-a)$ or $n|(a-b)$ when you write the definition.

We can't remember the right order either.

Order doesn't matter!

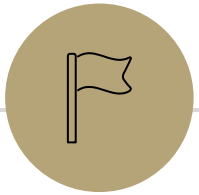
Show that if $a \equiv b(mod\ n)$ then $b \equiv a\ (mod\ n)$.

Let a, b be arbitrary integers and let n be an arbitrary integer > 0, and suppose $a \equiv b(mod\ n)$.

By definition of equivalence mod n, $n|(b - a)$. By definition of divides, $nk = b - a$ for some integer k. Multiplying by -1, we get

$$n(-k) = a - b$$

Since k was an integer, so is $-k$. Thus $n|(a - b)$, and by definition of mod, $b \equiv a(mod\ n)$.



Even more Extra Practice!

Even more practice

Equivalence in modular arithmetic

Let $a \in \mathbb{Z}, b \in \mathbb{Z}, n \in \mathbb{Z}$ and $n > 0$.
We say $a \equiv b \ (mod\ n)$ if and only if $n|(b-a)$

Show that $a \equiv b \ (mod\ n)$ if and only if $b \equiv a (mod\ n)$

Show that $a\%n=(a-n)\%n$ Where $b\%c$ is the unique r such that $b = kc + r$ for some integer k.

The Division Theorem

For every $a \in \mathbb{Z}$, $\boldsymbol{d} \in \mathbb{Z}$ with $\boldsymbol{d > 0}$
There exist ***unique*** integers q, r with $0 \leq r < d$ Such that $a = dq + r$

Even more practice

Show that $a \equiv b\ (mod\ n)$ if and only if $b \equiv a(mod\ n)$

$a \equiv b(mod\ n) \leftrightarrow n|(b-a) \leftrightarrow nk = b - a(\text{for } k \in \mathbb{Z}) \leftrightarrow$

$n(-k) = a - b(\text{for } -\text{k} \in \mathbb{Z}) \leftrightarrow n|(a-b) \leftrightarrow b \equiv a(mod\ n)$

Show that $a\%n=(a-n)\%n$ Where $b\%c$ is the unique r such that $b = kc + r$ for some integer k.

By definition of %, $a = qn + (a\%n)$ for some integer q. Subtracting n,

$a - n = (q-1)n + (a\%n)$. Observe that $q-1$ is an integer, and that this is the form of the division theorem for $(a-n)\%n$. Since the division theorem guarantees a unique integer, $(a-n)\%n = (a\%n)$