Sets and Number Theory

CSE 311 Autumn 2023
Lecture 11

Announcements

HW3 due tonight, HW4 released tonight, due Friday Oct. 27.

HW4 tends to take students by surprise

Same number of problems, but English proofs often take longer.

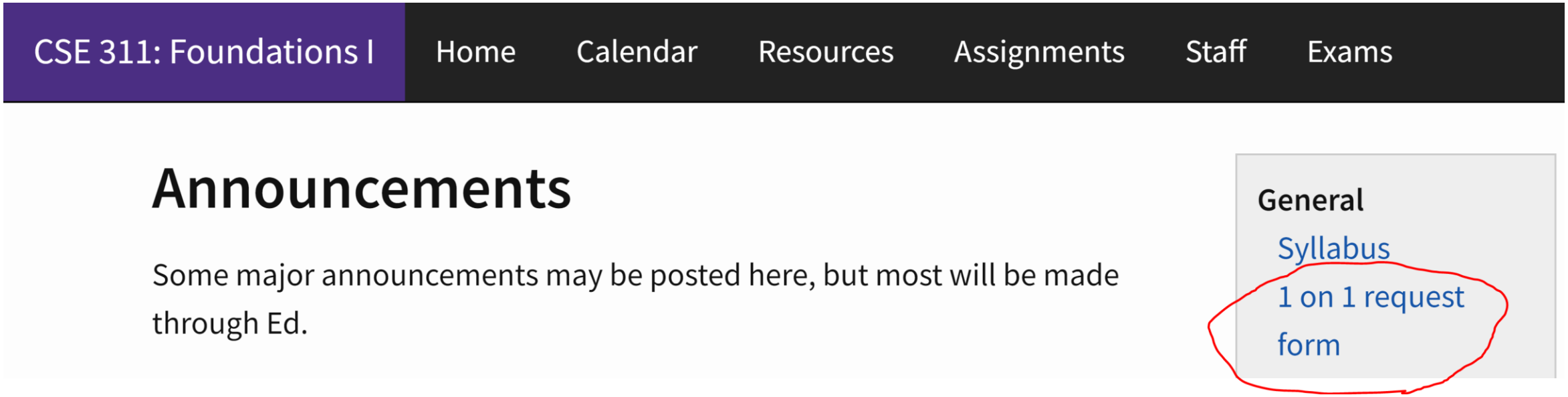
More spots to get stuck; more editing to do.

Please start early!

Still struggling with domain restriction?

You're not alone! There's an optional reading on the webpage.

Announcements



1:1 request form on the webpage.

Schedule a time to talk to a TA for 30 minutes.

NOT for current homework.

But can talk about concepts, section problems, old homeworks, etc.

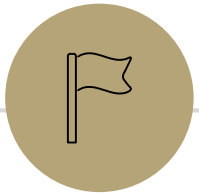
Today

Now that we've done the laundry list of definitions, let's do a set proof!

Two other proof techniques

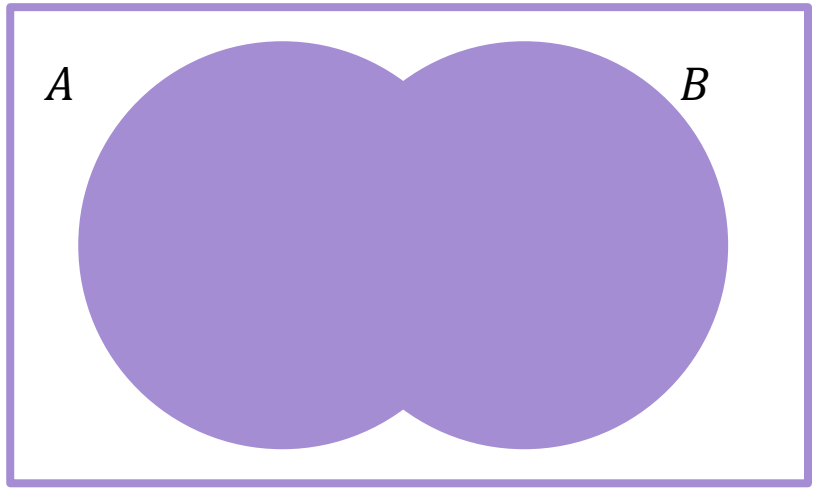
- Proving an exists
- Proof by cases

Start on Number theory definitions

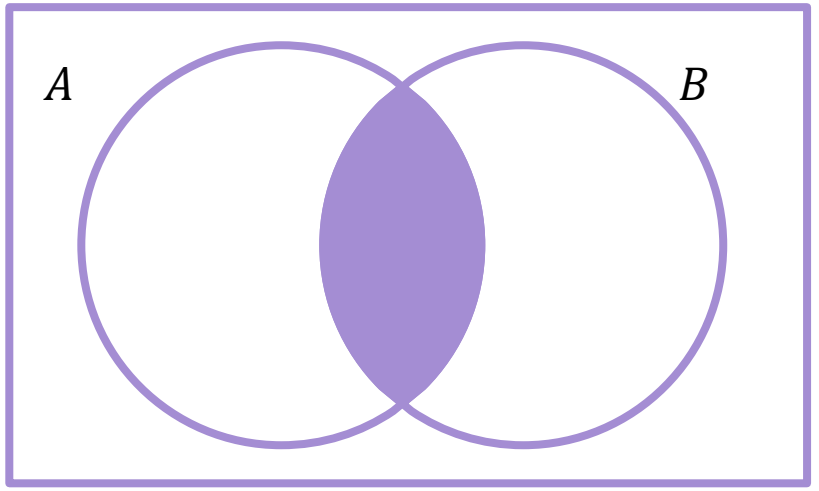


Proofs with sets

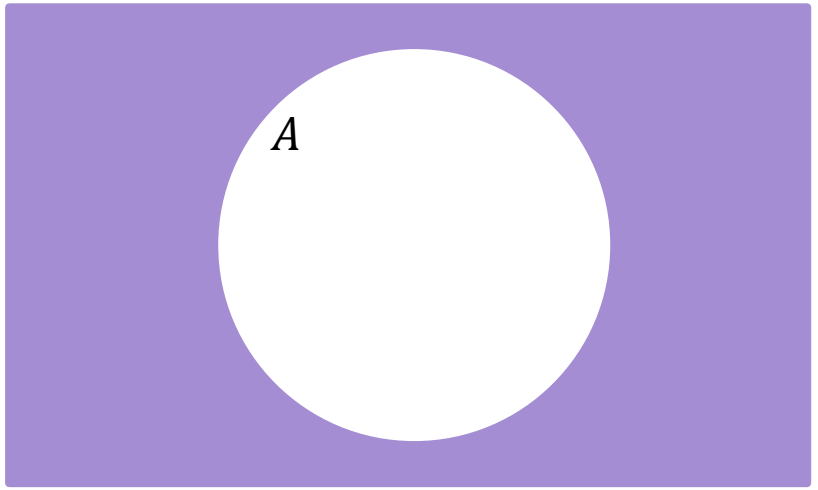
$A \cup B$



$A \cap B$



$\bar{A}$



A proof!

What's the analogue of DeMorgan's Laws…

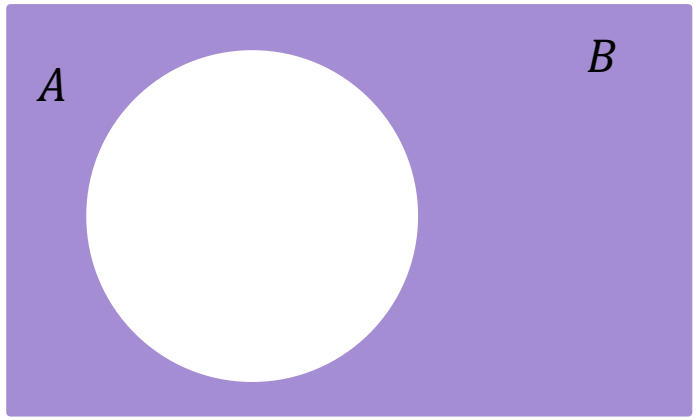
$\bar{A} \cap \bar{B} = \overline{A \cup B}$

$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$

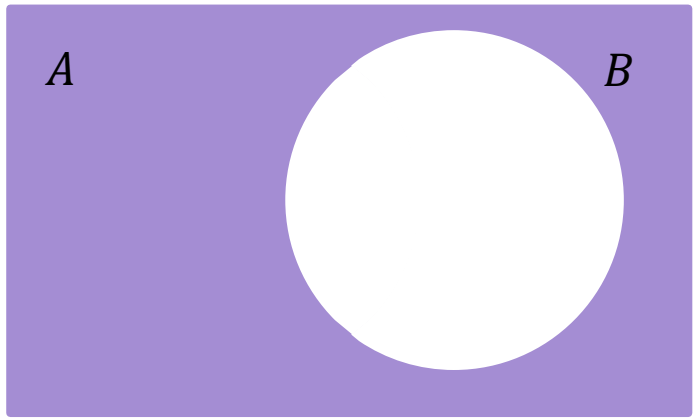
$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

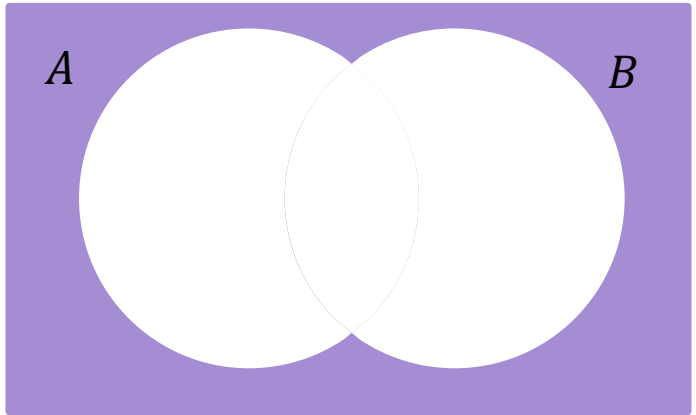
$\bar{A}$



$\bar{B}$



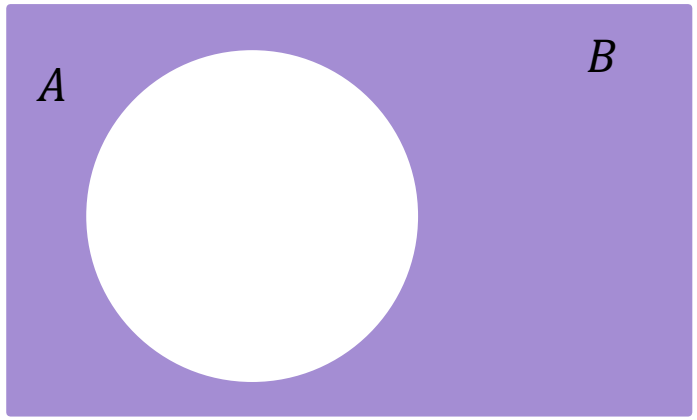
$\bar{A} \cap \bar{B}$



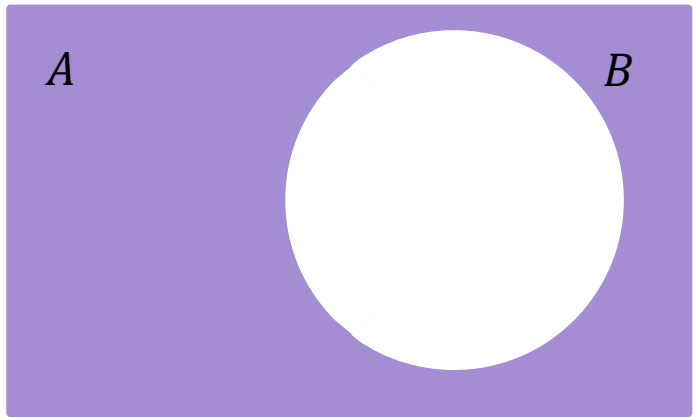
Try to find the diagram for $\overline{A \cup B}$

Is it the same?

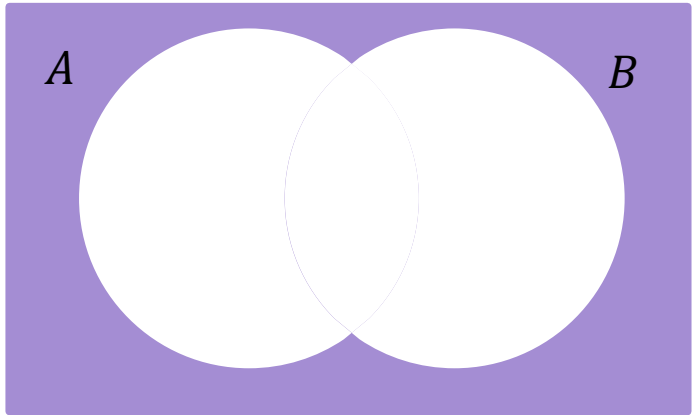
$\bar{A}$



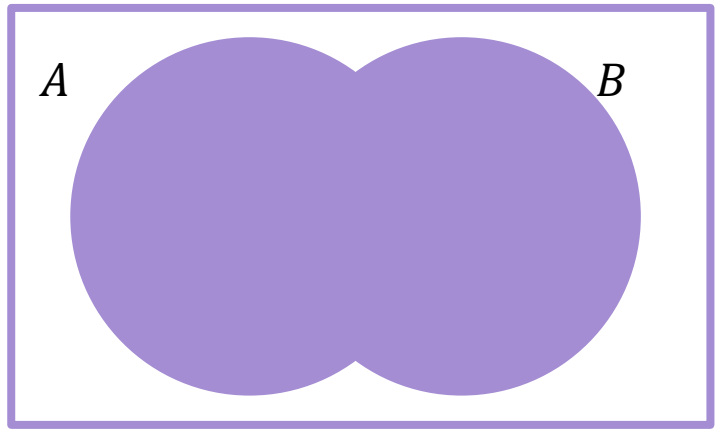
$\bar{B}$



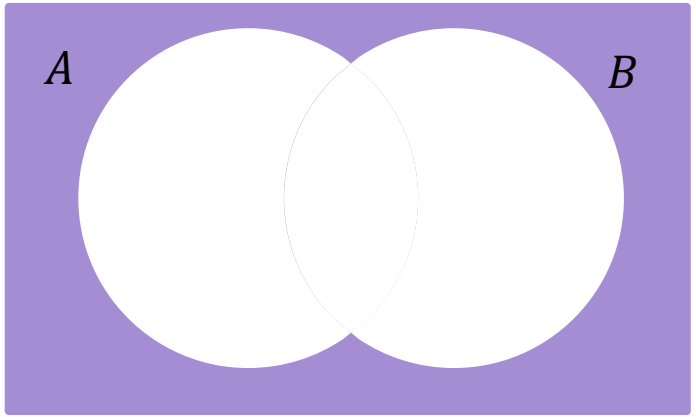
$\bar{A} \cap \bar{B}$



$A \cup B$



$\overline{A \cup B}$



A proof!

What's the analogue of DeMorgan's Laws…

$\bar{A} \cap \bar{B} = \overline{A \cup B}$

$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$

$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$
Let x be an arbitrary element of $\bar{A} \cap \bar{B}$.
…
That is, x is in the complement of $A \cup B$, as required.
Since x was arbitrary $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$
Let x be an arbitrary element of $\overline{A \cup B}$.
…
we get $x \in \bar{A} \cap \bar{B}$
Since x was arbitrary $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

Since the subset relation holds in both directions, we have $\bar{A} \cap \bar{B} = \overline{A \cup B}$

A proof!

What's the analogue of DeMorgan's Laws…

$\bar{A} \cap \bar{B} = \overline{A \cup B}$

$A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \wedge B \subseteq A$

$\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$
Let x be an arbitrary element of $\bar{A} \cap \bar{B}$.
By definition of $\cap$ $x \in \bar{A}$ and $x \in \bar{B}$. By definition of complement, $x \notin A \wedge x \notin B$.
Applying DeMorgan's Law, we get $\neg(x \in A \vee x \in B)$.
Applying the definition of union, we get:$\neg(x \in A \cup B)$.
From the definition of complement, we get $x \in \overline{A \cup B}$, as required.
Since x was arbitrary $\bar{A} \cap \bar{B} \subseteq \overline{A \cup B}$

$\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$
Let x be an arbitrary element of $\overline{A \cup B}$.
By definition of complement, x is not an element of $A \cup B$. Applying the definition of union, we get, $\neg(x \in A \vee x \in B)$
Applying DeMorgan's Law, we get: $x \notin A \wedge x \notin B$
By definition of complement, $x \in \bar{A} \wedge x \in \bar{B}$. So by definition of intersection, we get $x \in \bar{A} \cap \bar{B}$
Since x was arbitrary $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$

Since the subset relation holds in both directions, we have $\bar{A} \cap \bar{B} = \overline{A \cup B}$

Proof-writing advice

When you're writing a set equality proof, often the two directions are nearly identical, just reversed.

It's very tempting to use that $x \in A \leftrightarrow x \in B$ definition.

Be VERY VERY careful. It's easy to mess that up, at every step you need to be saying "if and only if."

Summary: How to show an if and only if

To show $p \leftrightarrow q$ you have two options:

Option A (STRONGLY recommended)

(1) $p \rightarrow q$

(2) $q \rightarrow p$

Option B (discouraged, but allowed)

p if-and-only-if p' if-and-only-if p'' if-and-only-if … if-and-only-if q

EVERY step must be an if-and-only if (in your justification AND explicitly written).

Two More Set Operations

Set-Builder Notation

Build your own set!

$\{x : \texttt{Conditions}(x)\}$

"The set of all x such that $\texttt{Conditions}(x)$"

In general
$\{ variable : conditions \}$
Will also see | instead of :

Everything that meets the conditions (causes the expression after the : to be true) is in the set. Nothing else is.

$\{x : \texttt{Even}(x)\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$

$\{y : \texttt{Prime}(y) \wedge \texttt{Even}(y)\} = \{2\}$

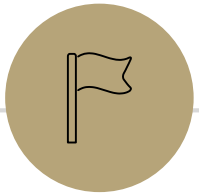
Two More Set Operations

Given a set, let's talk about it's powerset.

$\mathcal{P}(A) = \{\mathrm{X}: \mathrm{X} \text{ is a subset of } A\}$

The powerset of A is the **set** of all subsets of A.

$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$



More Proof Techniques

Proving an exists statement

How do I convince you $\exists x(P(x))$?

Show me the x! And convince me that $P(x)$ is true for that x.

Domain: Integers

Claim $\exists x\ \mathbf{Even}(x)$

Proof: Consider $x = 2$. We see that $2 = 2 \cdot 1$. Since 1 is an integer $2 = 2k$ for an integer k, which means 2 is even by definition, as required.

Two claims, two proof techniques

Suppose I claim that for all sets A, B, C: $A \cap B \subseteq C$

That…doesn't look right.

How do you prove me wrong?

What am I trying to prove? First write symbols for "¬(for all sets A, B, C …)"

Then 'distribute' the negation sign.

Two claims, two proof techniques

Suppose I claim that for all sets A, B, C: $A \cap B \subseteq C$

That…doesn't look right.

How do you prove me wrong?

Want to show: $\exists A, B, C: A \cap B \nsubseteq C$

Consider $A = \{1,2,3\}$, $B = \{1,2\}$, $C = \{2,3\}$, then $A \cap B = \{1,2\}$, which is not a subset of C.

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!

Proof By Cases

Let $A = \{x : \texttt{Prime}(x)\}$, $B = \{x : \texttt{Odd}(x) \vee \texttt{PowerOfTwo}(x)\}$

Where $\texttt{PowerOfTwo}(x) \coloneqq \exists c(\texttt{Integer}(c) \wedge x = 2\texttt{\^}c)$

Prove $A \subseteq B$

Proof By Cases

Let $A = \{x : \texttt{Prime}(x)\}$, $B = \{x: \texttt{Odd}(x) \vee \texttt{PowerOfTwo}(x)\}$

Where $\texttt{PowerOfTwo}(x) \coloneqq \exists c(\texttt{Integer}(c) \wedge x = 2\texttt{\^}c)$

Prove $A \subseteq B$

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

Proof By Cases

Let x be an arbitrary element of A.

We divide into two cases.

Case 1: x is even

If x is even and an element of A (i.e. both even and prime) it must be 2.
So it equals $2\text{^}c$ for $c = 1$, and thus is in B by definition of B.

Case 2: x is odd

Then $x \in B$ by satisfying the first requirement in the definition of B.

In either case, $x \in B$. Since an arbitrary element of A is also in B, we have $A \subseteq B$.

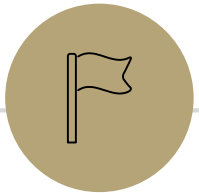
Proof By Cases

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”



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.

Divides

Divides

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

"x is a divisor of y" or "x is a factor of y" means (essentially) the same thing as x divides y.

("essentially" because of edge cases like when a number is negative or $y = 0$)

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

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

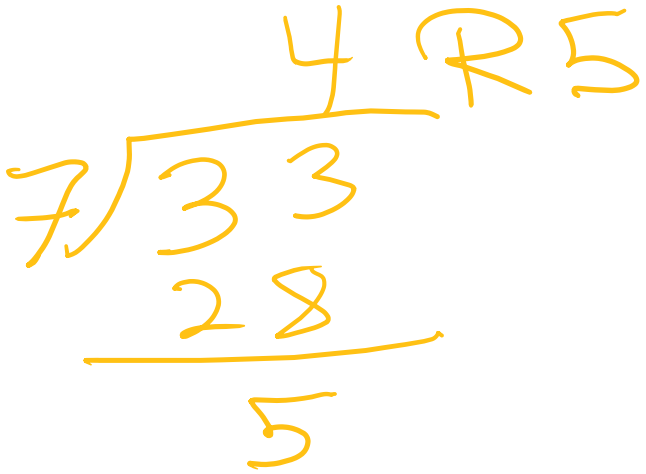
$1|5$ True

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 $a = dq + r$

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

"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

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

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

We need a definition! We can’t just say “it’s like a clock”

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

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!

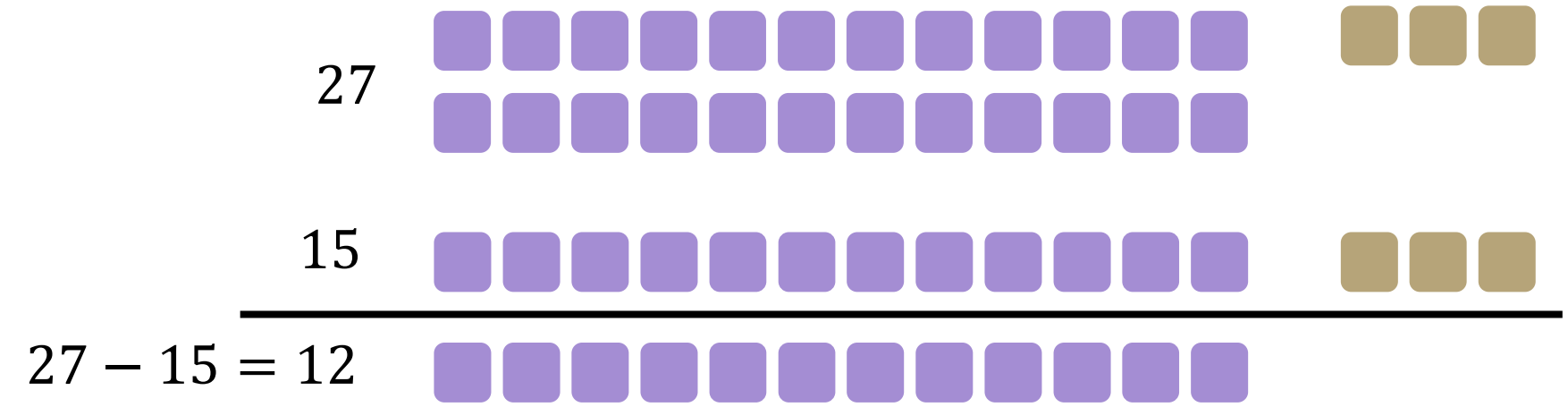
You should be *trying* to do the proof with me. Where do you think we're going next?

Why?

We'll post an optional (15-minute-ish) video over the weekend with why.

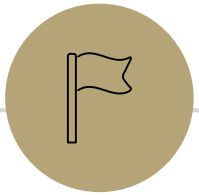
Here's the short version:

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…



Extra Set Practice

Extra Set Practice

Show $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
Proof:
Firse, we'll show: $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$
Let x be an arbitrary element of$A \cup (B \cap C)$.
Then by definition of ∪,∩ we have:
$x \in A \vee (x \in B \wedge x \in C)$
Applying the distributive law, we get
$(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
Applying the definition of union, we have:
$x \in (A \cup B)$ and $x \in (A \cup C)$
By definition of intersection we have $x \in (A \cup B) \cap (A \cup C)$.
So $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Now we show $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$
Let x be an arbitrary element of $(A \cup B) \cap (A \cup C)$.
By definition of intersection and union, $(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$
Applying the distributive law, we have $x \in A \vee (x \ \in B \wedge x \in C)$
Applying the definitions of union and intersection, we have $x \in A \cup (B \cap C)$
So $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.
Combining the two directions, since both sets are subsets of each other, we have $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

Extra Set Practice

Suppose $A \subseteq B$. Show that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Let A, B be arbitrary sets such that $A \subseteq B$.

Let X be an arbitrary element of $\mathcal{P}(A)$.

By definition of powerset, $X \subseteq A$.

Since $X \subseteq A$, every element of X is also in A. And since $A \subseteq B$, we also have that every element of X is also in B.

Thus $X \in \mathcal{P}(B)$ by definition of powerset.

Since an arbitrary element of $\mathcal{P}(A)$ is also in $\mathcal{P}(B)$, we have $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Extra Set Practice

Disprove: If $A \subseteq (B \cup C)$ then $A \subseteq B$ or $A \subseteq C$

Consider $A = \{1,2,3\}, B = \{1,2\}, C = \{3,4\}$.

$B \cup C = \{1,2,3,4\}$ so we do have $A \subseteq (B \cup C)$, but $A \nsubseteq B$ and $A \nsubseteq C$.

When you disprove a ∀, you're just providing a counterexample (you're showing ∃) – your proof won't have "let x be an arbitrary element of A."