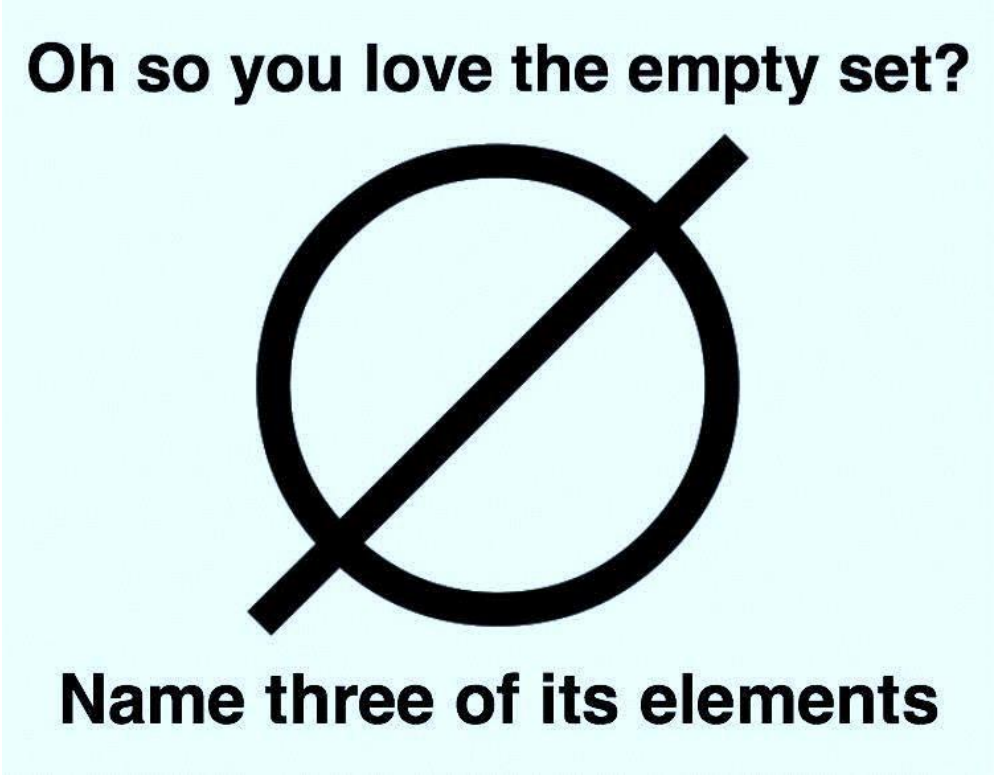
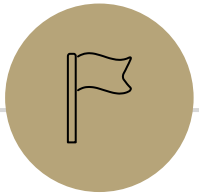


Set Theory

CSE 311 Summer 25
Lecture 10

Announcements

- HW3 is due tonight!
- HW2 Feedback is out
- HW2 Resubmission is out and due Friday
- HW4 will be released today!



Review

The Properties of Congruence We've Proven

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

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

Prime and Composite

Definition:

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

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

Least Common Multiple

Definition:

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

For Example:

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

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

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

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

Greatest Common Divisor

Definition:

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

For Example:

$\gcd(99,18) = 9$

$\gcd(100, 125) = 25$

$\gcd(7,11) = 1$

$\gcd(13,0) = 13$

Calculating the GCD: Approach 1

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

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

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

GCD facts

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

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

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

For example:

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

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

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

Why should you care?

Calculating the GCD: Approach 2

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

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

For Example:

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

Euclid's Algorithm in Java

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

So…what's it good for?

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

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

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

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

What number can we pick?

Solving in Modular Arithmetic

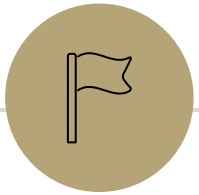
Solve: $7x \equiv 1 \pmod{10}$

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

None of our properties so far help us solve this.

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

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



Warm Up: Proving Another Mod Property

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv b \pmod{m}$.

[Unroll definitions]

[Manipulate towards goal]

[Reroll definitions]

Thus, $b \,\%\, m = a \,\%\, m$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv b \pmod{m}$.

Then $m \mid (a - b)$. So there exists some integer k such that $a - b = km$.

[Manipulate towards goal]

[Reroll definitions]

Thus, $b \,\%\, m = a \,\%\, m$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

⇒ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv b \pmod{m}$.

Then $m \mid (a - b)$. So there exists some integer k such that $a - b = km$.

Starting Point: $a - b = km \rightarrow a = km + b$

Goal: Show that $a \,\%\, m = b \,\%\, m$
(we'll need someway to get $a \,\%\, m$ and $b \,\%\, m$ from our starting point)

Available Facts & Theorems: $a \equiv b \,(mod\, m)$, The Division Theorem,
Definition of Divides, Definition of Congruence (mod m)

[Reroll definitions]

Thus, $b \,\%\, m = a \,\%\, m$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv b \pmod{m}$.

Then $m \mid (a - b)$. So there exists some integer k such that $a - b = km$.

So $a = km + b$. By the Division Theorem, $a = qm + (a \,\%\, m)$ for some integer q, where $0 \leq a \,\%\, m < m$.

Goal: Show that $a \,\%\, m = b \,\%\, m$

[Reroll definitions]

Thus, $b \,\%\, m = a \,\%\, m$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv b \pmod{m}$.

Then $m \mid (a - b)$. So there exists some integer k such that $a - b = km$.

So $a = km + b$. By the Division Theorem, $a = qm + (a \,\%\, m)$ for some integer q, where $0 \leq a \,\%\, m < m$. Thus:

$$km + b = qm + (a \,\%\, m)$$

$$b = qm - km + (a \,\%\, m)$$

$$b = (q - k)\, m + (a \,\%\, m)$$

[Reroll definitions]

Thus, $b \,\%\, m = a \,\%\, m$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Rightarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \equiv b \pmod{m}$.

Then $m \mid (a - b)$. So there exists some integer k such that $a - b = km$.

So $a = km + b$. By the Division Theorem, $a = qm + (a \,\%\, m)$ for some integer q, where $0 \leq a \,\%\, m < m$. Thus:

$$km + b = qm + (a \,\%\, m)$$

$$b = qm - km + (a \,\%\, m)$$

$$b = (q - k)\, m + (a \,\%\, m)$$

By the Division Theorem again, $a \,\%\, m$ is the remainder of b when divided by m.

Thus, $b \,\%\, m = a \,\%\, m$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$.

[Unroll definitions]

[Manipulate towards goal]

[Reroll definitions]

So $a \equiv b \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$.

(There are no definitions to unwind, but we'll use the fact that $a \,\%\, m = b \,\%\, m$)

[Manipulate towards goal]

[Reroll definitions]

So $a \equiv b \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$.

[Manipulate towards goal]

[Reroll definitions]

So $a \equiv b \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$.

Starting Point: $a \,\%\, m = b \,\%\, m$

Goal: Show that $m \mid (a - b)$. i.e. find an integer x such that $a - b = mx$
(we'll need someway to find values for a and b from our starting point)

Available Facts & Theorems: $a \,\%\, m = b \,\%\, m$, The Division Theorem, Definition of Divides

[Reroll definitions]

So $a \equiv b \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$.

By the Division Theorem, $a = mq + (a \,\%\, m)$ for some integer q, and $b = ms + (b \,\%\, m)$ for some integer s.

Goal: Show that $m \mid (a - b)$. i.e. find an integer x such that $a - b = mx$

[Reroll definitions]

So $a \equiv b \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$.

By the Division Theorem, $a = mq + (a \,\%\, m)$ for some integer q, and $b = ms + (b \,\%\, m)$ for some integer s. Thus:

$$a - b = (mq + (a \,\%\, m)) - (ms + b \,\%\, m)$$

$$a - b = mq - ms + (a \,\%\, m) - (b \,\%\, m)$$

$$a - b = m\mathrm{x}$$

Goal: Show that $m \mid (a - b)$. i.e. find an integer x such that $a - b = mx$

[Reroll definitions]

So $a \equiv b \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$.

By the Division Theorem, $a = mq + (a \,\%\, m)$ for some integer q, and $b = ms + (b \,\%\, m)$ for some integer s. Thus:

$$a - b = (mq + (a \,\%\, m)) - (ms + b \,\%\, m)$$

$$a - b = mq - ms + (a \,\%\, m) - (b \,\%\, m)$$

$$a - b = m(q - s)$$

Goal: Show that $m \mid (a - b)$. i.e. find an integer x such that $a - b = mx$

[Reroll definitions]

So $a \equiv b \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Warm Up: Claim 5

Definitions:

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

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

Claim 5: For integers a, b and $m > 0$, $a \equiv b \pmod{m}$ if and only if $a \,\%\, m = b \,\%\, m$.

$\Leftarrow$ Let $a, b, m > 0$ be arbitrary integers, and suppose $a \,\%\, m = b \,\%\, m$.

By the Division Theorem, $a = mq + (a \,\%\, m)$ for some integer q, and $b = ms + (b \,\%\, m)$ for some integer s. Thus:

$$a - b = (mq + (a \,\%\, m)) - (ms + b \,\%\, m)$$

$$a - b = mq - ms + (a \,\%\, m) - (b \,\%\, m)$$

$$a - b = m(q - s)$$

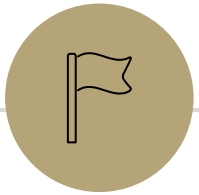
Since q, s are integers, $q - s$ is an integer. So $m \mid (a - b)$.

So $a \equiv b \pmod{m}$. Since a, b, m were arbitrary, the claim holds.

Summary: Properties of Mod

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

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



Bézout’s Theorem

Bézout's Theorem

Bézout's Theorem

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

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

So…what's it good for?

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

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

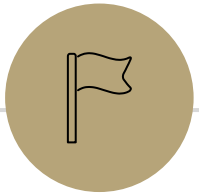
We once again want to find the multiplicative inverse of 8 (mod n).

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

Ok…how am I supposed to find s, t?

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

This is called the "Extended Euclidian algorithm"



Extended Euclidean Algorithm

Extended Euclidean Algorithm

Let's use the Extended Euclidean Algorithm to find the multiplicative inverse of $27 \pmod{35}$, i.e. the integer x such that $27 \cdot x \equiv 1 \pmod{35}$

Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

gcd(35,27)

Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

gcd(35,27) = gcd(27, 35%27) = gcd(27,8)

= gcd(8, 27%8) = gcd(8, 3)

= gcd(3, 8%3) = gcd(3, 2)

= gcd(2, 3%2) = gcd(2,1)

= gcd(1, 2%1) = gcd(1,0)

Tablaeu

$$35 = 1 \cdot 27 + 8$$

$$27 = 3 \cdot 8 + 3$$

$$8 = 2 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
35 &= 1 \cdot 27 + 8 \\
27 &= 3 \cdot 8 + 3 \\
8 &= 2 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{aligned}
$$

Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$\begin{aligned} 35 &= 1 \cdot 27 + 8 \\ 27 &= 3 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

$$\begin{aligned} 8 &= 35 - 1 \cdot 27 \\ 3 &= 27 - 3 \cdot 8 \\ 2 &= 8 - 2 \cdot 3 \\ 1 &= 3 - 1 \cdot 2 \end{aligned}$$

Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (8 - 2 \cdot 3) \\
&= -1 \cdot 8 + 3 \cdot 3
\end{aligned}
$$

Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (8 - 2 \cdot 3) \\
&= -1 \cdot 8 + 3 \cdot 3 \\
&= -1 \cdot 8 + 3 \cdot (27 - 3 \cdot 8) \\
&= 3 \cdot 27 - 10 \cdot 8
\end{aligned}
$$

Extended Euclidian Algorithm

Step 1 compute gcd(a,b); keep tableau information.

Step 2 solve all equations for the remainder.

Step 3 substitute backward

$$
\begin{aligned}
8 &= 35 - 1 \cdot 27 \\
3 &= 27 - 3 \cdot 8 \\
2 &= 8 - 2 \cdot 3 \\
1 &= 3 - 1 \cdot 2
\end{aligned}
$$

$$\gcd(27,35) = 13 \cdot 27 + (-10) \cdot 35 = 1$$

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (8 - 2 \cdot 3) \\
&= -1 \cdot 8 + 3 \cdot 3 \\
&= -1 \cdot 8 + 3 \cdot (27 - 3 \cdot 8) \\
&= 3 \cdot 27 - 10 \cdot 8 \\
&= 3 \cdot 27 - 10 \cdot (35 - 1 \cdot 27) \\
&= 13 \cdot 27 - 10 \cdot 35
\end{aligned}
$$

When substituting back, you keep the larger of m, n and the number you just substituted. Don't simplify further! (or you lose the form you need)

Extended Euclidian Algorithm

Bézout's Theorem

If a and b are positive integers, then there exist integers s and t such that
gcd(a,b)= $sa + tb$

$$\gcd(27,35) = 1 = s \cdot 27 + t \cdot 35$$
$$= 13 \cdot 27 + (-10) \cdot 35$$

We've found our s and t! $s = 13$ and $t = -10$

Extended Euclidian Algorithm

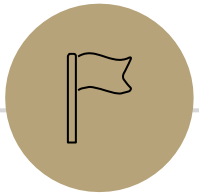
$$\gcd(27,35) = 1 = s \cdot 27 + t \cdot 35$$
$$= 13 \cdot 27 + (-10) \cdot 35$$

We've found our s and t! $s = 13$ and $t = -10$

This means the multiplicative inverse of $27 \pmod{35}$ is 13:

$$1 = 13 \cdot 27 + (-10) \cdot 35$$
$$1 - 13 \cdot 27 = (-10) \cdot 35$$

So $1 - 13 \cdot 27 \mid 35$ and $1 \equiv 13 \cdot 27 \pmod{35}$



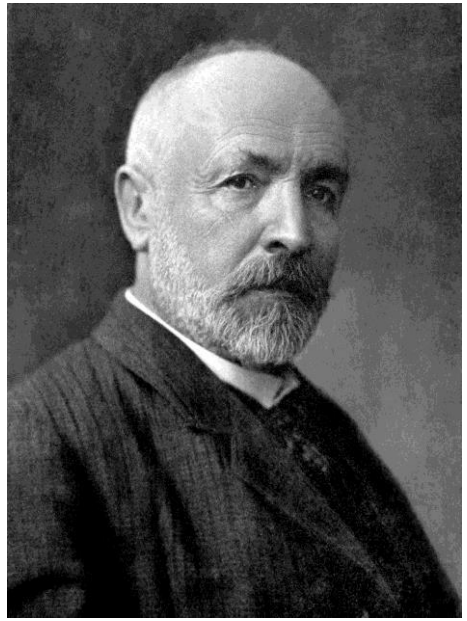
Set Theory

Motivation

Set theory is widely regarded as the foundation for all of mathematics.

In computing, there are applications in:

- Data Structures
- Databases
- Programming Languages



Father of Modern Set Theory
Georg Cantor
(1845 – 1918)

Sets

Definition:

A set is an unordered collection of distinct objects, called elements.

- We write $x \in A$ to say that x is an element of the set A.
- We write $x \notin A$ to say that x is not an element of the set A.

Set Notation

We'll write a set as a collection of elements inside curly braces {}.

Sets are often given variable names with capital letters.

$A = \{0,5,8,10\} = \{5,8,0,10\}$

$B = \{\text{watermelon}, \text{apple}, \text{pineapple}\}$

$C = \{a, b, c, c, b, a\} = \{a, b, c\}$

$D = \{0,1,2,3,4,5, \dots\}$

Sets are unordered

Sets can contain any type of object

Repeat elements are listed once

Sets can be finite or infinite

Common Sets

$\mathbb{R}$ is the set of Real Numbers.

E.g. $1, -17, \pi, \sqrt{2}$

$\mathbb{Z}$ is the set of Integers.

$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{N}$ is the set of Natural Numbers.

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$

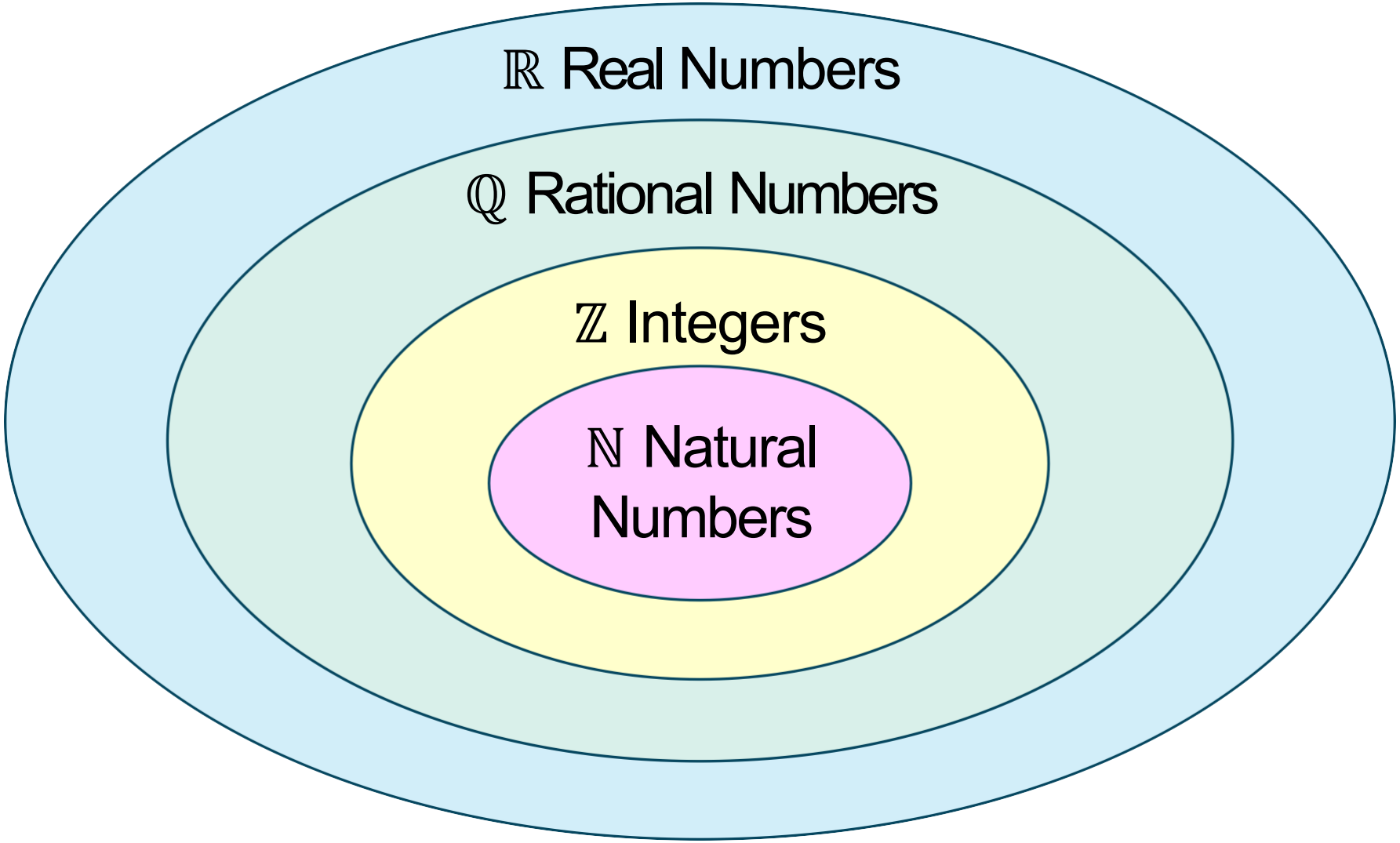
$\mathbb{Q}$ is the set of Rational Numbers (fractions)

E.g. $\frac{1}{2}, -\frac{11}{3}, 17$

$\emptyset = \{\}$ is the Empty Set

$\emptyset$ has no elements

Common Sets


ℝ Real Numbers
ℚ Rational Numbers
ℤ Integers
ℕ Natural Numbers

Sets can be elements of other sets

For example:

$A = \{\{1\}, \{2\}, \{1,2\}, \emptyset\}$

$B = \{1, 2\}$

Then $1 \in B, 2 \in B$. And $\emptyset \in A, B \in A$.

Sets Builder Notation

Another way to describe a set is using set-builder notation.

$S = \{x : \mathrm{P}(x)\}$ means S is the set of all x for which $\mathrm{P}(x)$ is true.

For example:

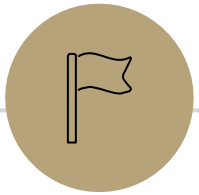
- $\{x \in \mathbb{Z} : x > 0\}$ is the set of all positive integers.
- $\{x \in \mathbb{N} : x \equiv 2 \pmod 3\}$ is the set $\{2, 5, 8, 11, 14, \dots\}$.
- $\{\frac{a}{b} : a, b \in \mathbb{Z}, \mathrm{b} \neq 0\}$ is the set of rational numbers

Set Cardinality

The cardinality of a set is the number of elements in a set (its size). The cardinality of a set A is often denoted $|A|$.

What is the cardinality of the following sets?

- $A = \{x \in \mathbb{Z} \ : \ x \equiv 1 \ (\mathrm{mod}\ 4) \ \mathrm{and} - 10 \leq x \leq 10\}$ $= \{-7, -3, 1, 5, 9\}$
  $|\mathrm{A}| = 5$
- $B = \emptyset$
  $|\mathrm{B}| = 0$
- $C = \{\emptyset\}$
  $|C| = 1$



Relationships Between Sets

Set Equality

Sets A and B are equal iff they have the same elements.

In predicate logic, $A = B$ is defined as:

$$\forall x \, (x \in A \leftrightarrow x \in B)$$

A = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}
D = {4, 3, 3}
E = {3, 4, 3}
F = {4, {3}}

Which sets are equal?

$$C = D = E$$

Subset

Set A is a subset of B if every element of A is also in B.

In predicate logic, $A \subseteq B$ is defined as:

$$\forall x(x \in A \rightarrow x \in B)$$

A = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}
D = {4, 3, 3}
E = {3, 4, 3}
F = {4, {3}}

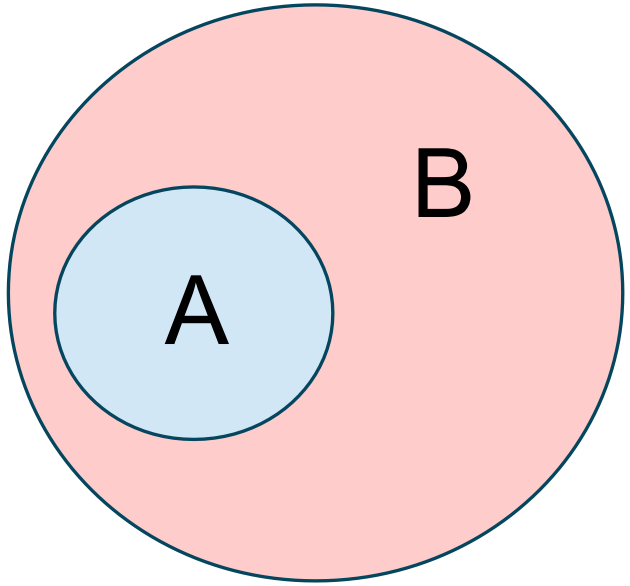
Which sets are subsets?

$C \subseteq B$, $D \subseteq E$, $E \subseteq D$, etc.

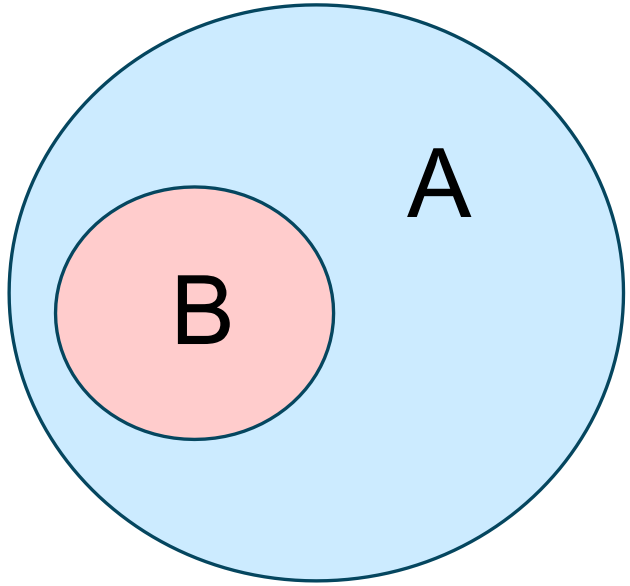
Set Equality and Subsets

$$A = B \equiv A \subseteq B \wedge B \subseteq A$$

A is a subset of B



B is a subset of A



$\in$ vs. $\subseteq$

$A = \{1, 2, 3\}$ $B = \{2\}$ $C = \{\emptyset, \{2\}\}$

- $\emptyset \subseteq A$? Yes.
- $\emptyset \in A$? No. $\emptyset \in C$ though!
- $2 \subseteq B$? No. $\{2\} \subseteq B$ though!
- $2 \in B$? Yes.
- $B \in A$? No. $B \subseteq A$ though!
- $B \in C$? Yes.

Proof Skeleton

How would we show $A \subseteq B$?

$$A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B)$$

Let x be an arbitrary element of A

…

So x is also in B.

Since x was an arbitrary element of A, we have that $A \subseteq B$.

Proof Skeleton

That wasn't a "new" skeleton! It's exactly what we always do when we want to prove $\forall x(P(x) \to Q(x))$!

What about $A = B$?

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

Just do two subset proofs!

i.e. $\forall x(x \in A \to x \in B)$ and $\forall x(x \in B \to x \in A)$

Proof-writing advice

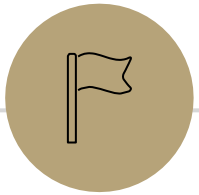
When you're writing a set equality proof, often the two directions are nearly identical, just reversed.

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."

Review : 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).



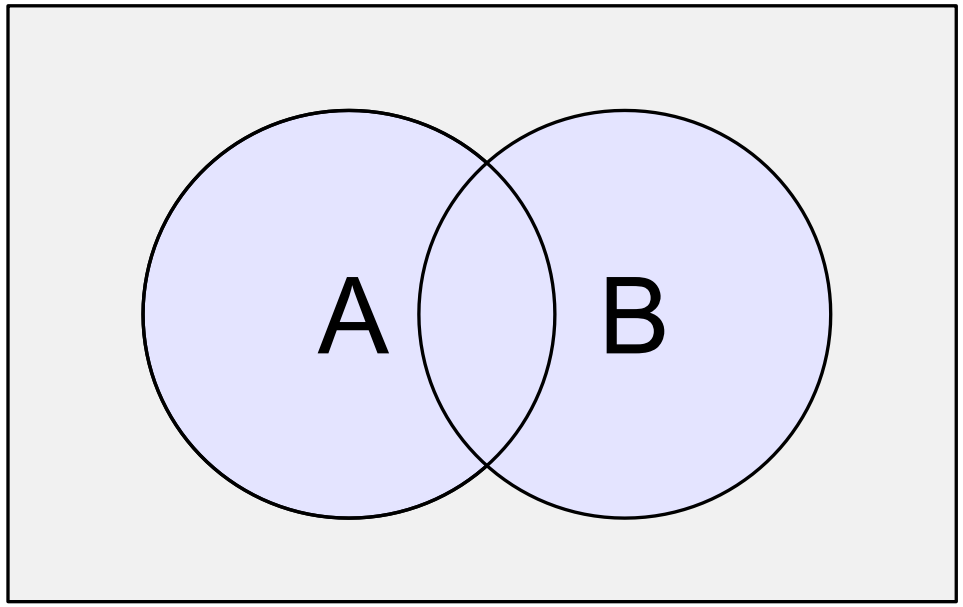
Set Operations

Combining Sets

Set Operations

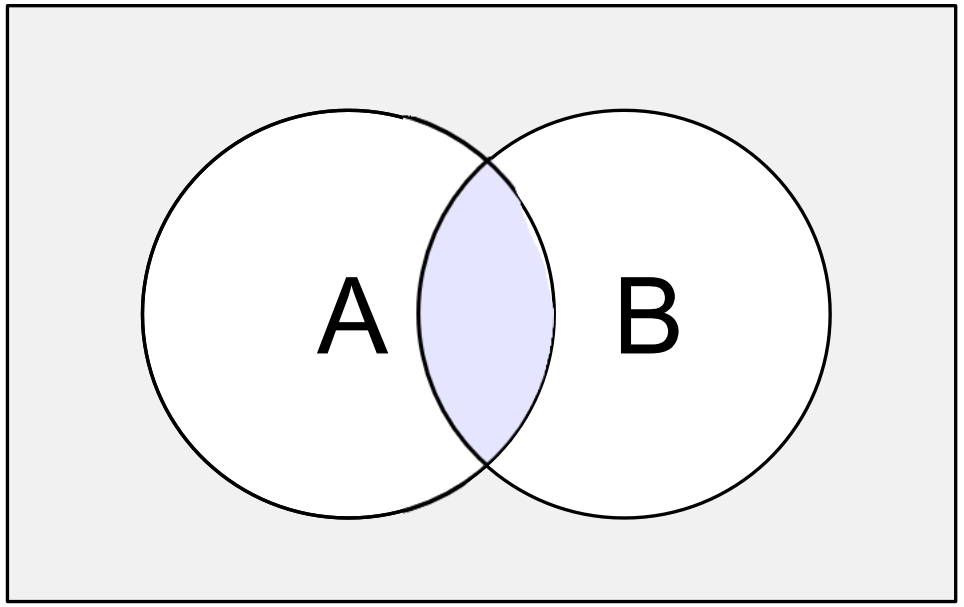
Union: $A \cup B$

$$A \cup B = \{x : x \in A \vee x \in B\}$$



Intersection: $A \cap B$

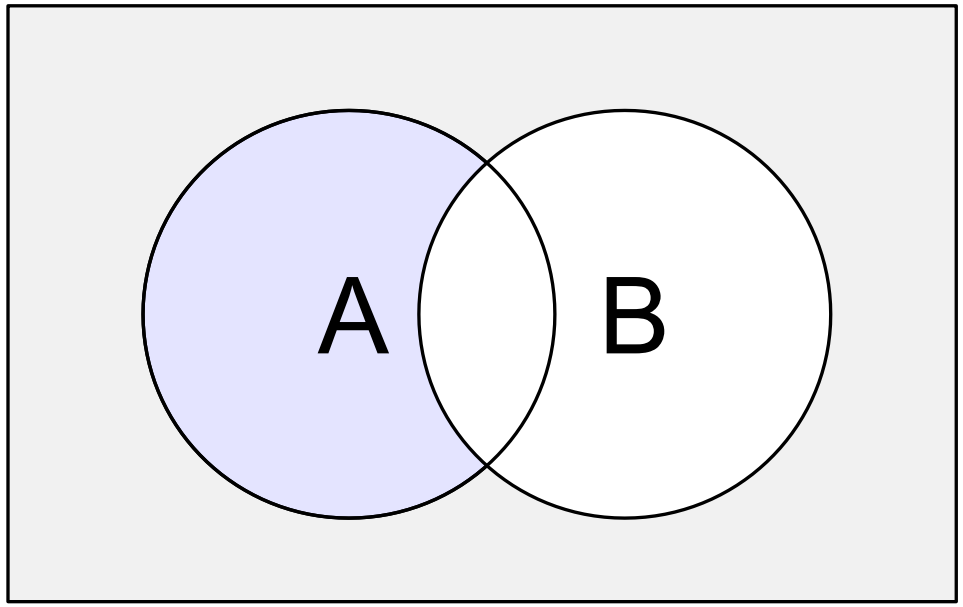
$$A \cap B = \{x : x \in A \wedge x \in B\}$$



Set Operations

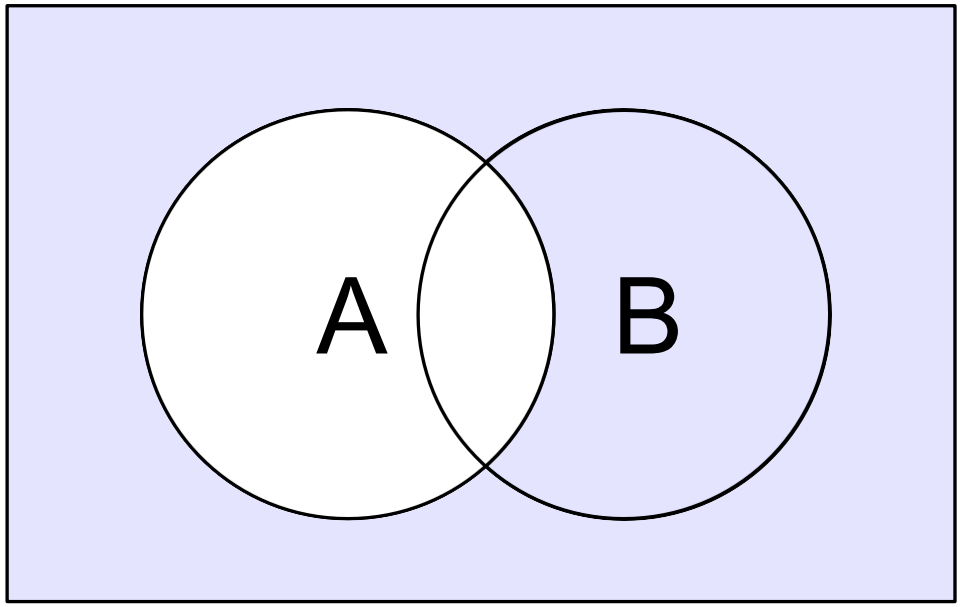
Set Difference: $A \setminus B$

$$A \setminus B = \{x : x \in A \wedge x \notin B\}$$

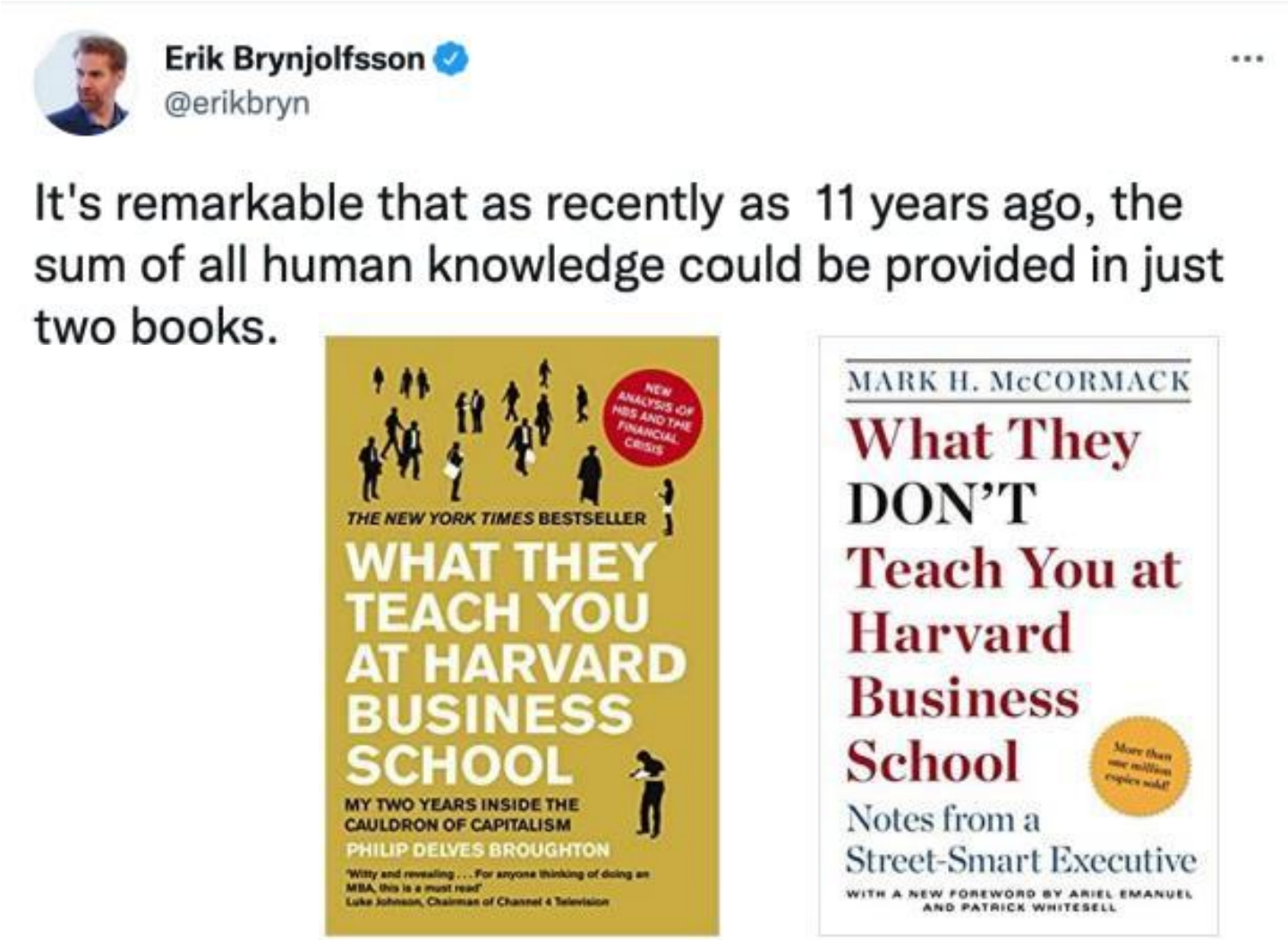


Set Complement: $\bar{A} = A^c$
(with respect to the universe $\mathcal{U}$)

$$\bar{A} = \{x \in \mathcal{U} : x \notin A\}$$



Set Operations



Exercises

Definitions

$A \cup B = \{x : x \in A \vee x \in B\}$

$A \cap B = \{x : x \in A \wedge x \in B\}$

$A \setminus B = \{x : x \in A \wedge x \notin B\}$

$\bar{A} = \{x : x \notin A\}$

$A = \{1, 2, 3\}$ $B = \{3, 5, 6\}$ $C = \{3, 4\}$

Using only A, B, C and set operations, make the following sets. The universe is all integers.

- $\{1, 2, 3, 4, 5, 6\} =$ $A \cup B \cup C$
- $\{3\} =$ $A \cap B$
- $\{1, 2\} =$ $A \setminus B = A \cap \bar{B}$

Powerset

Powerset: $\mathcal{P}\{A\}$

$\mathcal{P}(A) = \{X : X \subseteq A\}$

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

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

$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

Cartesian Product

Cartesian Product: $A \times B$

$A \times B = \{(a, b) : a \in A,\ b \in B\}$

The cartesian product of A with B is the set of ordered pairs of the form (a, b), where $a \in A$ and $b \in B$.

If $A = \{1,2\}$ and $B = \{a, b, c\}$ then:

$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$

$\mathbb{R} \times \mathbb{R} =$ the real plane. This is often denoted $\mathbb{R}^2$.

Exercises

Compute the following:

$\{1,2\} \times \emptyset =$ $\emptyset$

$\mathcal{P}(\{2\} \times \{1,3\}) =$ $\mathcal{P}(\{(2,1),(2,3)\}) = \{\emptyset, \{(2,1)\}, \{(2,3)\}, \{(2,1),(2,3)\}\}$

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

$|\mathcal{P}(\{1,2\}) \times \mathcal{P}(\{3,4,5\})| =$ 32

Todo

Tonight:

HW3 is due tonight!

Friday:

CC 10 due Friday at noon

HW2 Resubmission is due Friday!