CSE 311 Section 5

Number Theory & Set Theory

Announcements & Reminders

- 390z practice midterm on April 30th, 12:30pm - 2:20pm and 2:30pm - 4:20pm

- HW4 due tomorrow @ 11:00PM on Gradescope
  - Make sure you **tagged pages** on gradescope **correctly**
- HW5
  - Due Friday 5/3 @11:00 PM
- Midterm Review
  - Monday, May 6th 5:00-8:00PM SIG 134
- Midterm
  - Wednesday, May 8th, regular class periods
- Book One-on-Ones on the course homepage!

Problem 4 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of $7 \text{ mod } 33$. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

Problem 5 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

First, we find the gcd:

```
gcd(33,7)   = gcd(7,5)      33 = 4 • 7 + 5
            = gcd(5,2)      7  = 1 • 5 + 2
            = gcd(2,1)      5  = 2 • 2 + 1
            = gcd(1,0)      2  = 2 • 1 + 0
```

Problem 5 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

First, we find the gcd:

```
gcd(33,7)   = gcd(7,5)
            = gcd(5,2)
            = gcd(2,1)
            = gcd(1,0)
```

```
33 = 4 • 7 + 5
7  = 1 • 5 + 2
5  = 2 • 2 + 1
2  = 2 • 1 + 0
```

Next, we re-arrange the equations by solving for the remainder:

```
1 = 5 - 2 • 2
2 = 7 - 1 • 5
5 = 33 - 4 • 7
```

Problem 5 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of $7 \bmod 33$. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

b) Now, solve $7z \equiv 2 \pmod{33}$ for all of its integer solutions z.

Try this problem with the people around you, and then we'll go over it together!

Problem 5 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \ (mod\ 33)$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \leq y < 33$.

First, we find the gcd:

gcd(33,7) = gcd(7,5)	$33 = 4 \cdot 7 + 5$
= gcd(5,2)	$7 = 1 \cdot 5 + 2$
= gcd(2,**1**)	$5 = 2 \cdot 2 + \mathbf{1}$
= gcd(**1**,0)	$2 = 2 \cdot \mathbf{1} + 0$

Next, we re-arrange the equations by solving for the remainder:

$\mathbf{1} = 5 - 2 \cdot 2$

$2 = 7 - 1 \cdot 5$

$5 = 33 - 4 \cdot 7$

Now, we backward substitute into the boxed numbers using the equations:

$$
\begin{aligned}
\mathbf{1} &= 5 - 2 \cdot 2 \\
&= 5 - 2 \cdot (7 - 1 \cdot 5) \\
&= 3 \cdot 5 - 2 \cdot 7 \\
&= 3 \cdot (33 - 4 \cdot 7) - 2 \cdot 7 \\
&= 3 \cdot 33 + -14 \cdot 7
\end{aligned}
$$

Problem 5 – Extended Euclidean Algorithm

a) Find the multiplicative inverse y of 7 mod 33. That is, find y such that $7y \equiv 1 \pmod{33}$. You should use the extended Euclidean Algorithm. Your answer should be in the range $0 \le y < 33$.

First, we find the gcd:

$$\begin{aligned} \gcd(33,7) &= \gcd(7,5) \\ &= \gcd(5,2) \\ &= \gcd(2,\mathbf{1}) \\ &= \gcd(\mathbf{1},0) \end{aligned}$$

$$\begin{aligned} 33 &= 4 \cdot 7 + 5 \\ 7 &= 1 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + \mathbf{1} \\ 2 &= 2 \cdot \mathbf{1} + 0 \end{aligned}$$

Next, we re-arrange the equations by solving for the remainder:

$$\begin{aligned} \mathbf{1} &= 5 - 2 \cdot 2 \\ 2 &= 7 - 1 \cdot 5 \\ 5 &= 33 - 4 \cdot 7 \end{aligned}$$

Now, we backward substitute into the boxed numbers using the equations:

$$\begin{aligned} \mathbf{1} &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (7 - 1 \cdot 5) \\ &= 3 \cdot 5 - 2 \cdot 7 \\ &= 3 \cdot (33 - 4 \cdot 7) - 2 \cdot 7 \\ &= 3 \cdot 33 + -14 \cdot 7 \end{aligned}$$

So, $\mathbf{1} = \mathbf{3} \cdot 33 + \mathbf{-14} \cdot 7$. Thus, $33 \mathbf{- 14} = \mathbf{19}$ is the multiplicative inverse of 7 mod 33

Problem 5 – Extended Euclidean Algorithm

b) Now, solve $7z \equiv 2 \pmod{33}$ for all of its integer solutions z.

Problem 5 – Extended Euclidean Algorithm

b) Now, solve $7z \equiv 2 \pmod{33}$ for all of its integer solutions z.

If $7y \equiv 1 \pmod{33}$, then $2 \cdot 7y \equiv 2 \pmod{33}$.

Problem 5 – Extended Euclidean Algorithm

b) Now, solve $7z \equiv 2 \pmod{33}$ for all of its integer solutions z.

If we have $7z \equiv 2 \pmod{33}$, multiplying both sides by 19, we get:

$z \equiv 2 \cdot 19 \pmod{33} \equiv 5 \pmod{33}$.

This means that the set of solutions is $\{5 + 33k \mid k \in Z\}$

Sets

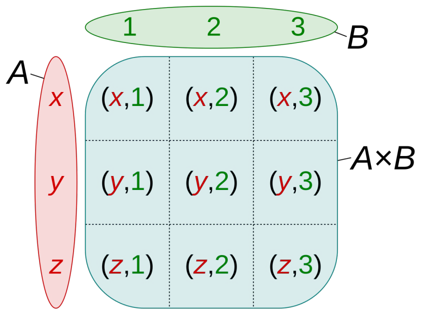
Sets

- A set is an **unordered** group of **distinct** elements
  - Set variable names are capital letters, with lower-case letters for elements

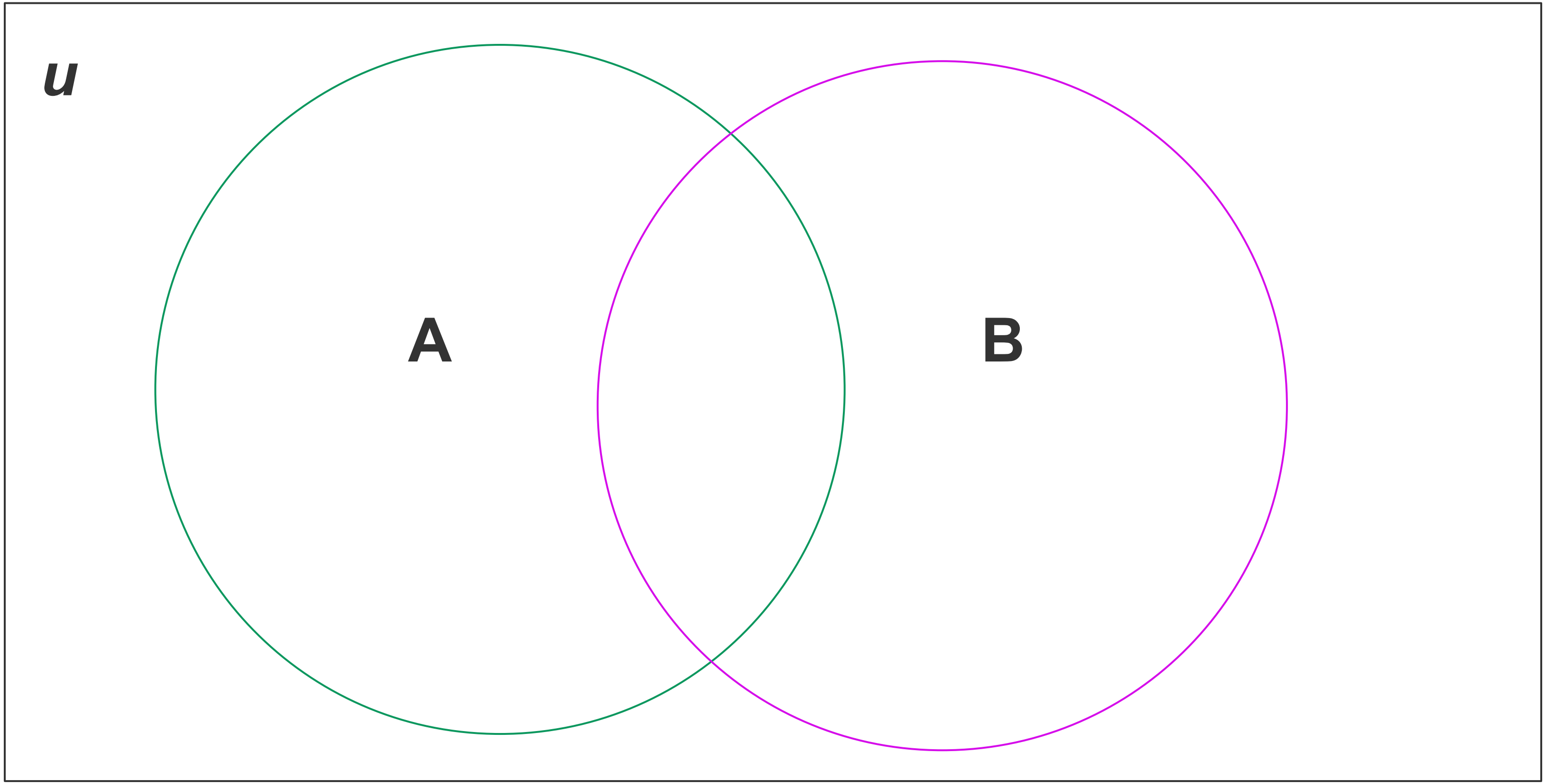
- Set Notation:
  - $a \in A$: "a is in A" or "a is an element of A"
  - $A \subseteq B$: "A is a subset of B", every element of A is also in B
  - $\emptyset$: "empty set", a unique set containing no elements
  - $\mathcal{P}(A)$: "power set of A", the set of all subsets of A including the empty set and A itself

Set Operators

- Subset: $A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B)$
- Equality: $A = B \equiv \forall x(x \in A \leftrightarrow x \in B) \equiv A \subseteq B \land B \subseteq A$
- Union: $A \cup B = \{x: x \in A \lor x \in B\}$
- Intersection: $A \cap B = \{x: x \in A \land x \in B\}$
- Complement: $\overline{A} = \{x: x \notin A\}$
- Difference: $A \setminus \mathrm{B} = \{x: x \in A \land x \notin B\}$
- Cartesian Product: $A \times B = \{(a, b): a \in A \land b \in B\}$

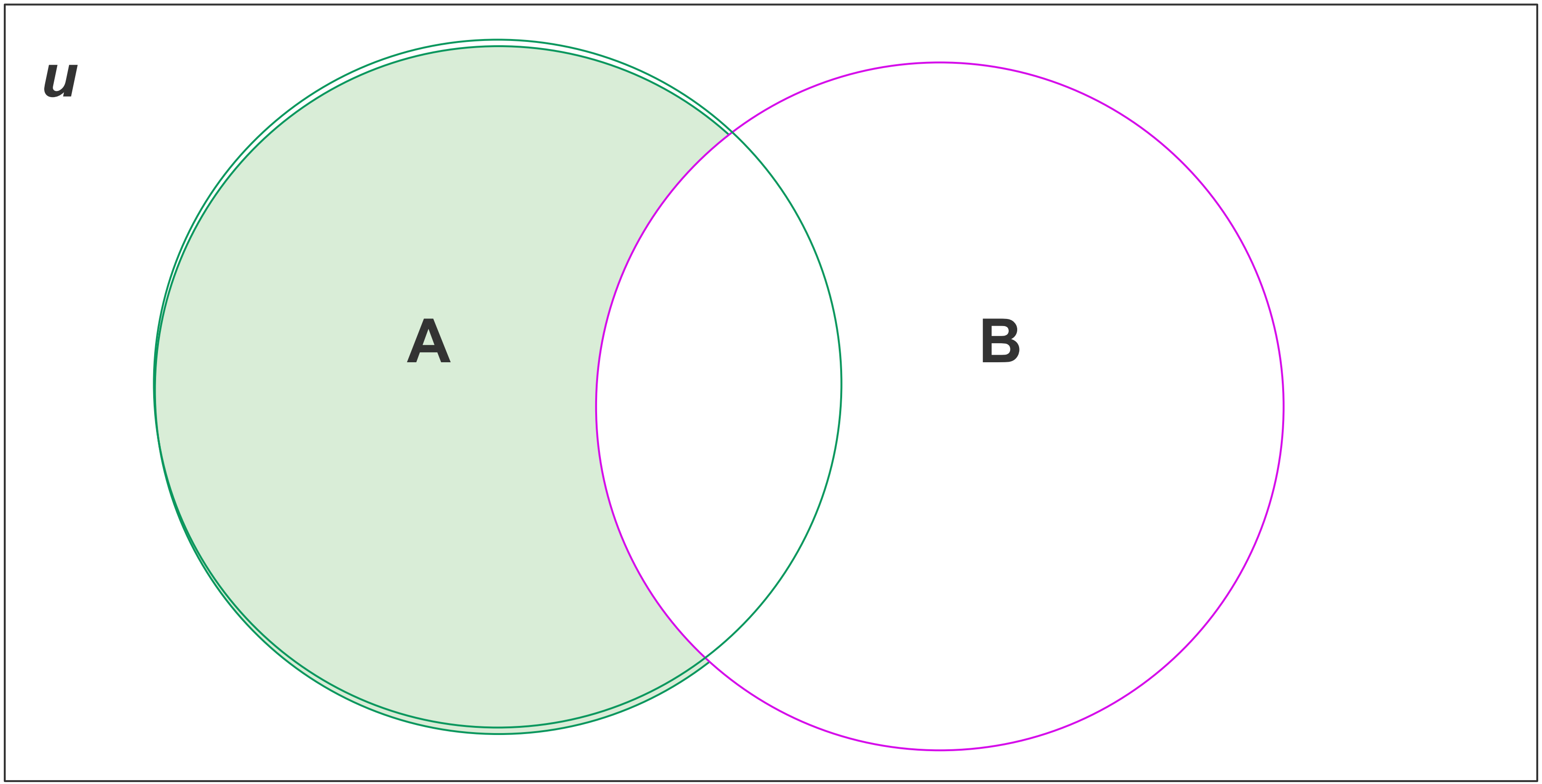


Understand Sets Visually!



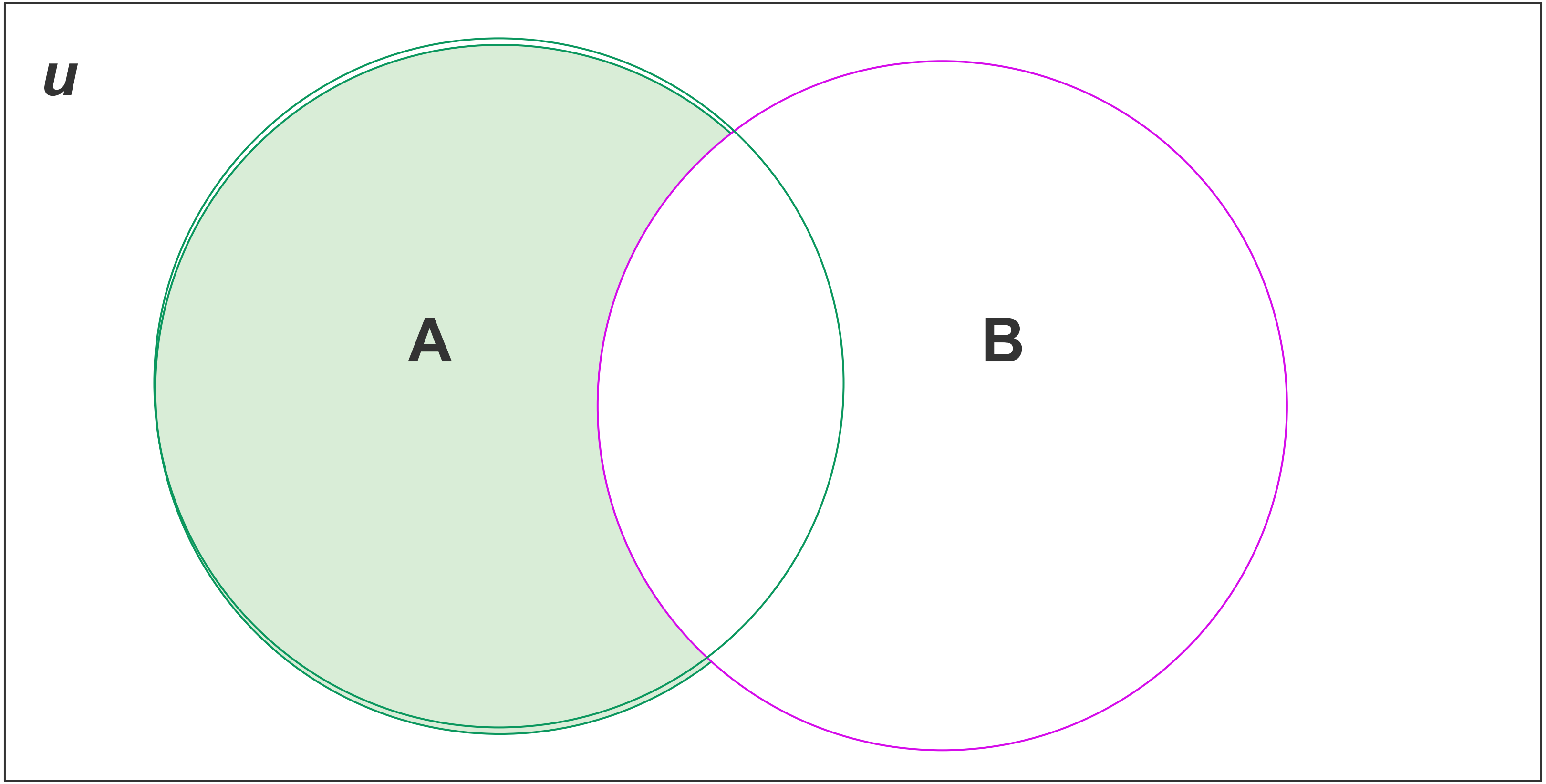
Understand Sets Visually!

What Set Operation is this?

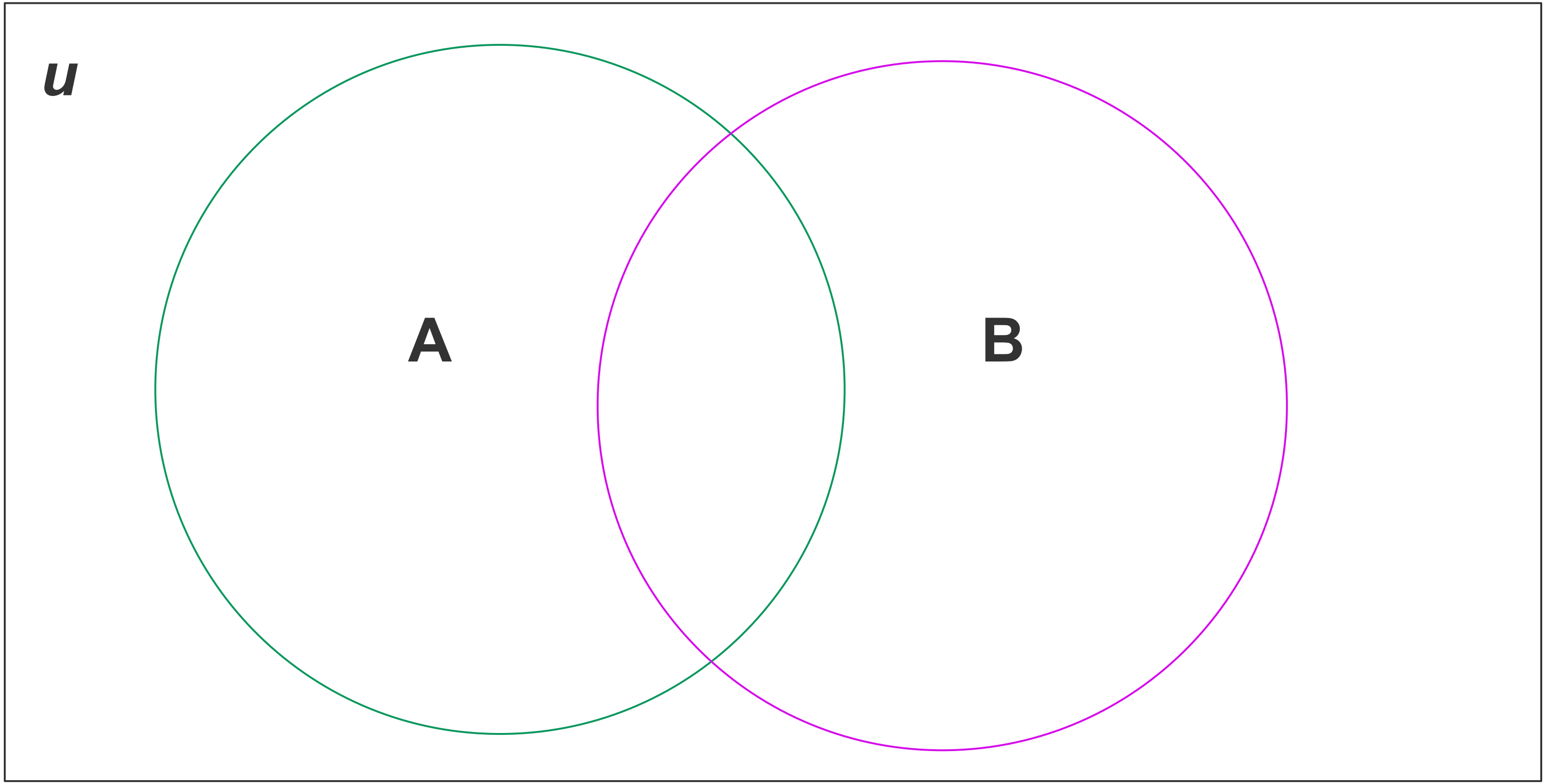


Understand Sets Visually!

What Set Operation is this?
Difference: A \ B

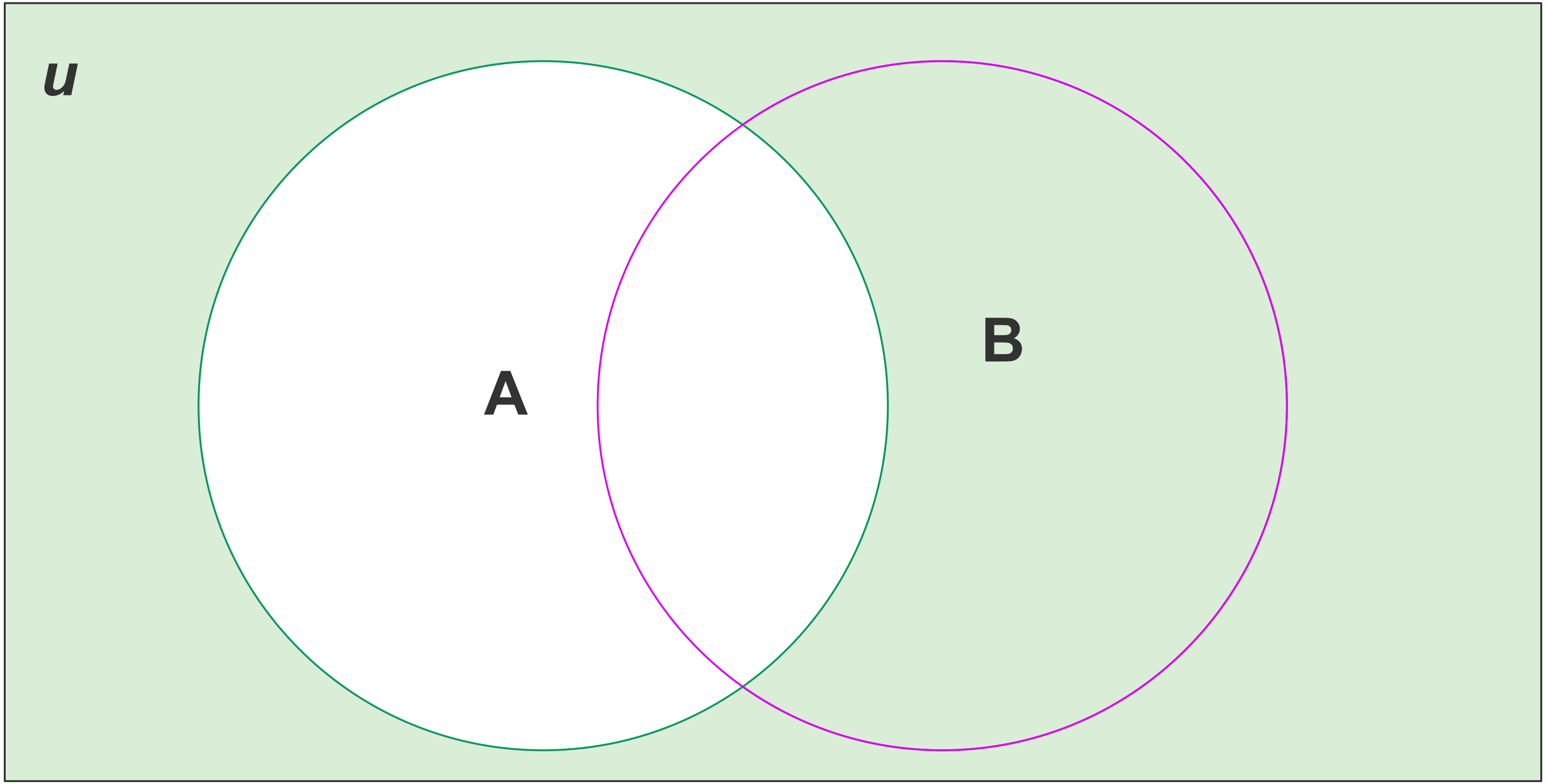


Understand Sets Visually!



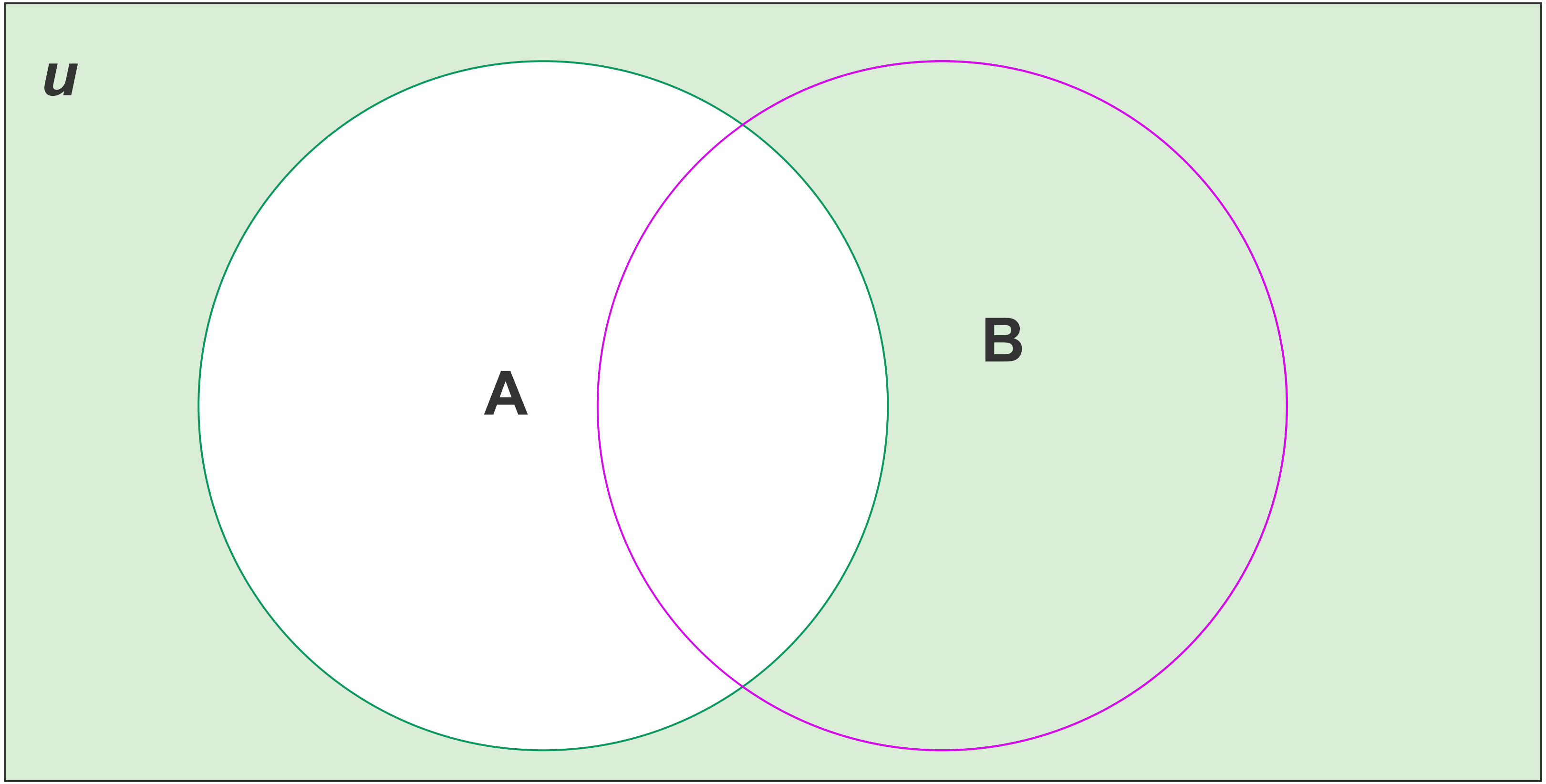
Understand Sets Visually!

What Set Operation is this?

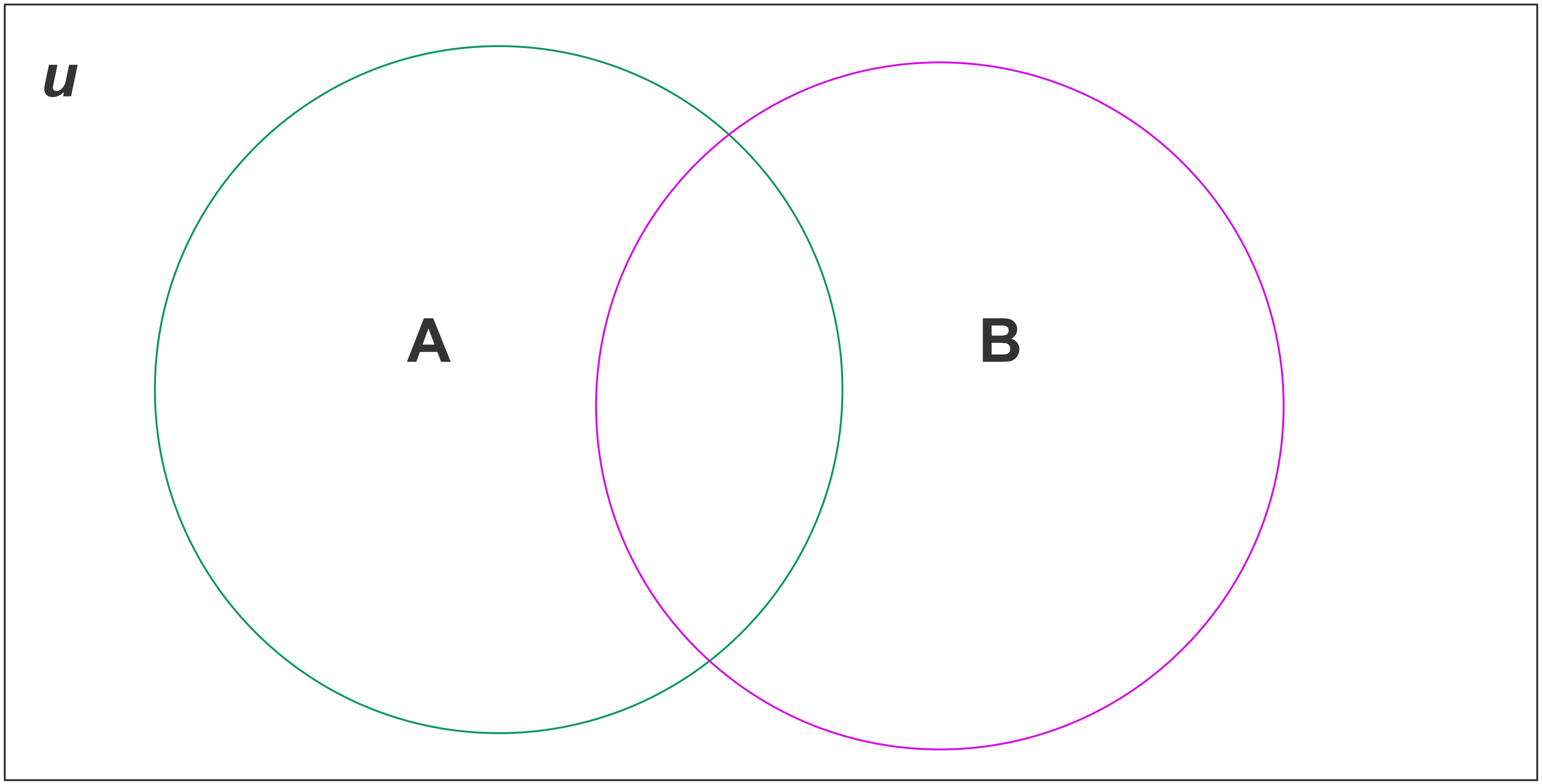


Understand Sets Visually!

What Set Operation is this?
A complement: $\overline{A}$

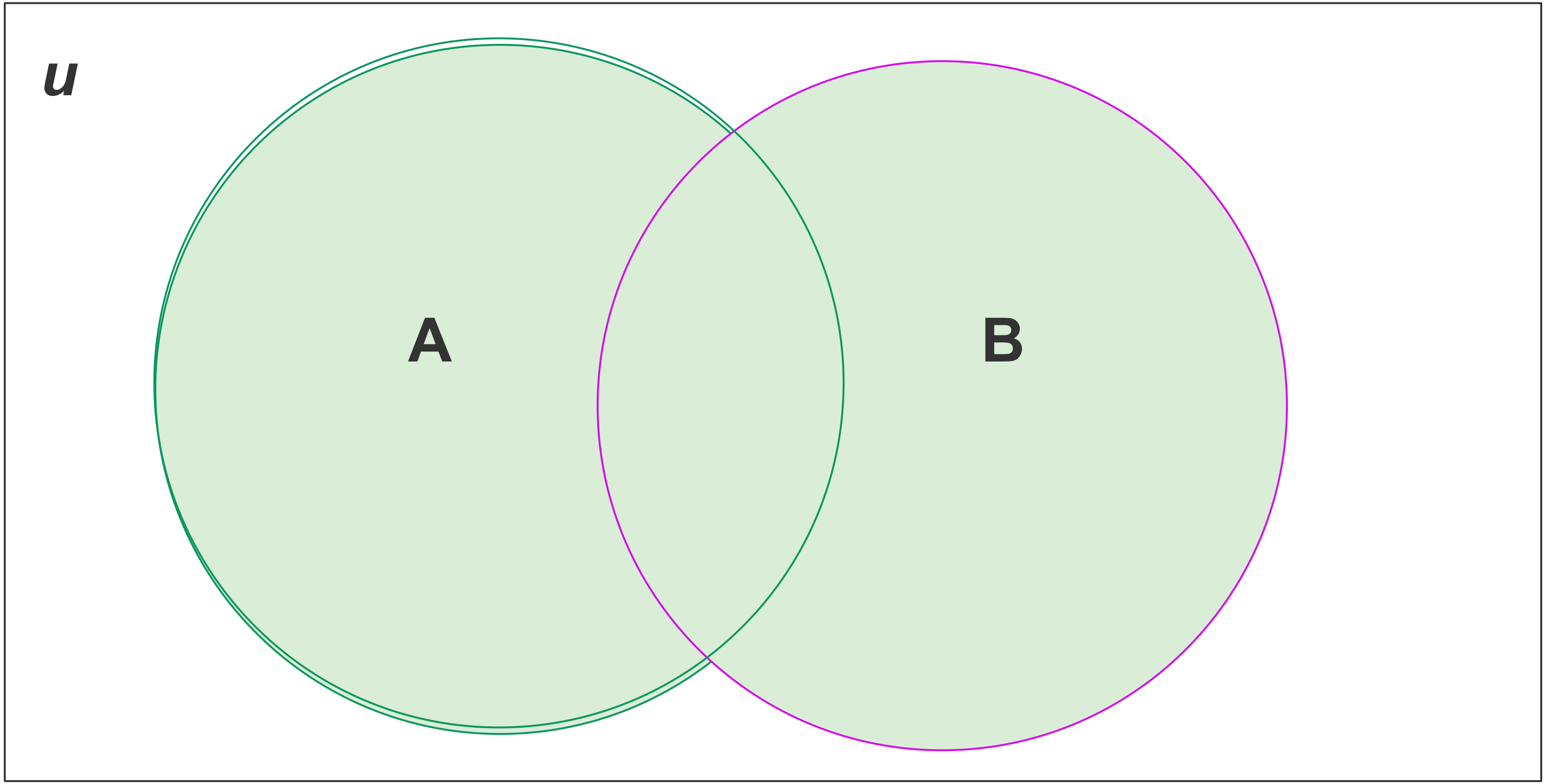


Understand Sets Visually!



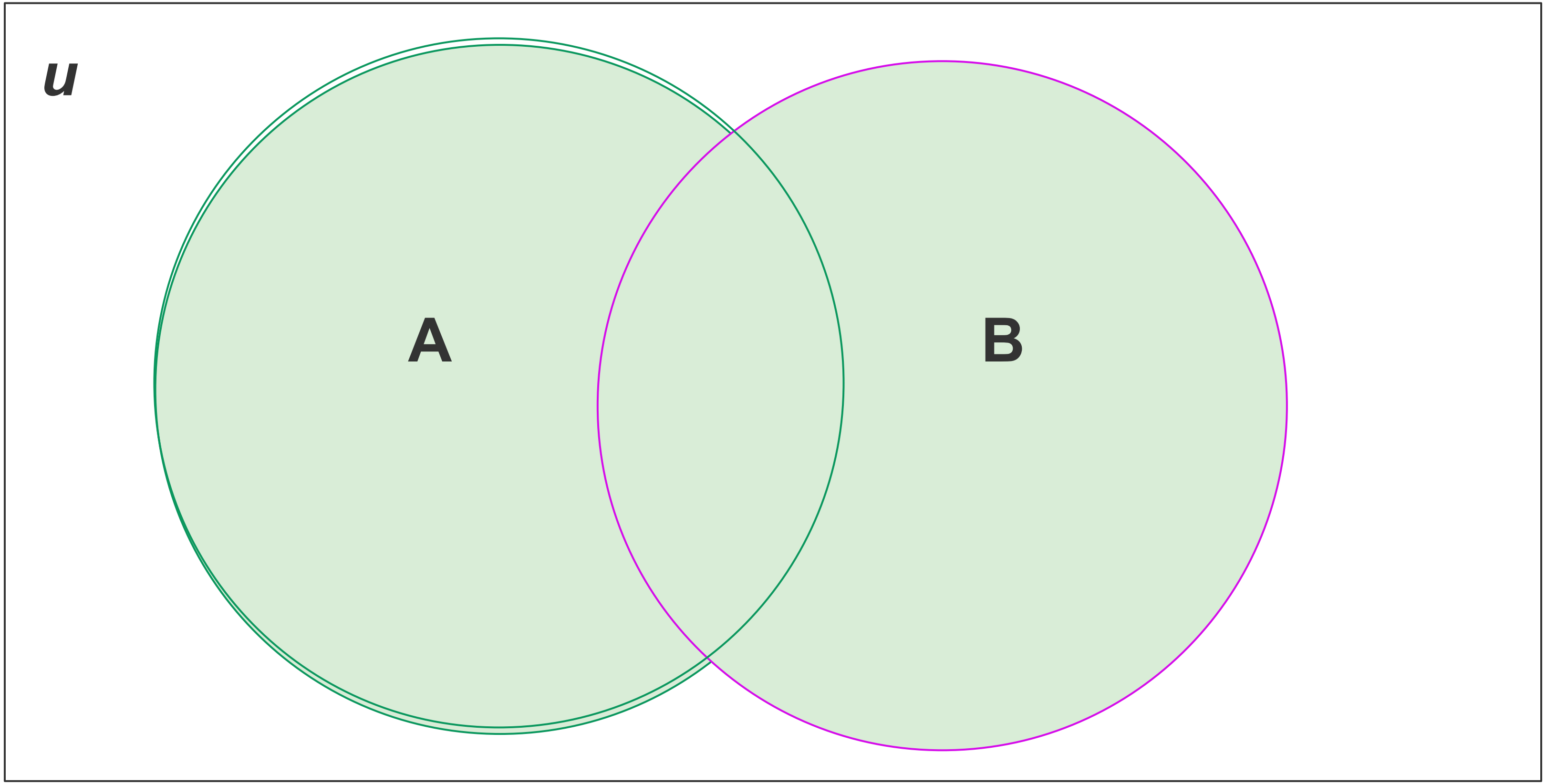
Understand Sets Visually!

What Set Operation is this?



Understand Sets Visually!

What Set Operation is this?
Union: A U B



Set Proofs

Subset Proofs

One of the most common types of proofs you will be asked to write involving sets is a subset proof. That is, you will be asked to prove that $A \subseteq B$. We always approach these proofs with the same proof skeleton:

Let x be an arbitrary element of A, so $x \in A$.
… some steps using set definitions to show that x must also be in B…
Thus, $x \in B$
Since x was arbitrary, $A \subseteq B$.

Using Cozy For Sets

- **A U B**: A Union B- “A cup B”
- **A ∩ B**: “A cap B”
- **A ∊ B**: “A in B”
- A \ B: “A \ B”
- B complement- “~B” (Only one Argument)
- A\B\C is implicitly (A\B)\C

New Feature: Use the **text** button to see what the text input for a proof should be

Problem 3a – Subsets

For any sets A, B, and C, show that it holds that $A \setminus B \subseteq A \cup C$

Try it on Cozy: bit.ly/S053A

Problem 3a – Cozy Solution

For any sets A, B, and C, show that it holds that $A \setminus B \subseteq A \cup C$

Let x be arbitrary.

1.1.1.	`x in A \ B`	`assumption`
1.1.2.	`x in A and not (x in B)`	`defof \ {A} {B} 1.1.1`
1.1.3.	`x in A`	`elim and 1.1.2 left`
1.1.4.	`x in A or x in B`	`intro or 1.1.3 (x in B) right`
1.1.5.	`x in A cup B`	`undef cup {A} {B} 1.1.4` ✖
1.1.	`x in A \ B -> x in A cup B`	`direct proof (x in A \ B -> x in A cup B)` ✖
1.	`forall x, x in A \ B -> x in A cup B`	`intro forall (forall x, x in A \ B -> x in A cup B) x`
2.	`A \ B subset A cup B`	`undef subset {A \ B} {A cup B} 1` ✖

Problem 3b- Subsets

For any sets A, B, and C, show that it holds that $(A \setminus B) \setminus C \subseteq A \setminus C$

Try it on Cozy: bit.ly/S053B

Problem 3b- Cozy Solution

Let x be arbitrary.

1.1.1.	`x in A \ B \ C`	`assumption`
1.1.2.	`x in A \ B and not (x in C)`	`defof \ {A \ B} {C} 1.1.1`
1.1.3.	`x in A and not (x in B) and not (x in C)`	`defof \ {A} {B} 1.1.2`
1.1.4.	`not (x in C)`	`elim and 1.1.3 right`
1.1.5.	`x in A and not (x in B)`	`elim and 1.1.3 left`
1.1.6.	`x in A`	`elim and 1.1.5 left`
1.1.7.	`x in A and not (x in C)`	`intro and 1.1.6 1.1.4`
1.1.8.	`x in A \ C`	`undef \ {A} {C} 1.1.7` ✖
1.1.	`x in A \ B \ C -> x in A \ C`	`direct proof (x in A \ B \ C -> x in A \ C)` ✖
1.	`forall x, x in A \ B \ C -> x in A \ C`	`intro forall (forall x, x in A \ B \ C -> x in A \ C) x`
2.	`A \ B \ C subset A \ C`	`undef subset {A \ B \ C} {A \ C} 1` ✖

Set Equality: Using Meta Theorem

Problem 4

Let A and B be sets. Consider the claim: $A\backslash(B \cup C) = (A\backslash B) \cap (A\backslash C)$.

Problem 4

Let A and B be sets. Consider the claim: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Let x be arbitrary.

Since x was arbitrary, we have shown that the two sets contain the same elements.

Problem 4

Let A and B be sets. Consider the claim: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Let x be arbitrary.

$x \in A \backslash (B \cup C) \equiv x \in A \wedge \neg(x \in (B \cup C))$ [Def of Set Difference]

Since x was arbitrary, we have shown that the two sets contain the same elements.

Problem 4

Let A and B be sets. Consider the claim: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Let x be arbitrary.

$$
\begin{aligned}
x \in A \backslash (B \cup C) &\equiv x \in A \land \neg(x \in (B \cup C)) && \text{[Def of Set Difference]} \\
&\equiv x \in A \land \neg(x \in B \lor x \in C) && \text{[Def of Union]}
\end{aligned}
$$

Since x was arbitrary, we have shown that the two sets contain the same elements.

Problem 4

Let A and B be sets. Consider the claim: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Let x be arbitrary.

$$
\begin{aligned}
x \in A \backslash (B \cup C) &\equiv x \in A \wedge \neg(x \in (B \cup C)) && \text{[Def of Set Difference]} \\
&\equiv x \in A \wedge \neg(x \in B \vee x \in C) && \text{[Def of Union]} \\
&\equiv x \in A \wedge (x \notin B \wedge x \notin C) && \text{[De Morgan]}
\end{aligned}
$$

Since x was arbitrary, we have shown that the two sets contain the same elements.

Problem 4

Let A and B be sets. Consider the claim: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Let x be arbitrary.

$$
\begin{aligned}
x \in A \backslash (B \cup C) &\equiv x \in A \wedge \neg(x \in (B \cup C)) && \text{[Def of Set Difference]} \\
&\equiv x \in A \wedge \neg(x \in B \vee x \in C) && \text{[Def of Union]} \\
&\equiv x \in A \wedge (x \notin B \wedge x \notin C) && \text{[De Morgan]} \\
&\equiv (x \in A \wedge x \in A) \wedge (x \notin B \wedge x \notin C) && \text{[Idempotency]}
\end{aligned}
$$

Since x was arbitrary, we have shown that the two sets contain the same elements.

Problem 4

Let A and B be sets. Consider the claim: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Let x be arbitrary.

$$
\begin{aligned}
x \in A \backslash (B \cup C) &\equiv x \in A \wedge \neg(x \in (B \cup C)) && \text{[Def of Set Difference]} \\
&\equiv x \in A \wedge \neg(x \in B \vee x \in C) && \text{[Def of Union]} \\
&\equiv x \in A \wedge (x \notin B \wedge x \notin C) && \text{[De Morgan]} \\
&\equiv (x \in A \wedge x \in A) \wedge (x \notin B \wedge x \notin C) && \text{[Idempotency]} \\
&\equiv (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) && \text{[Associativity/Commutativity]}
\end{aligned}
$$

Since x was arbitrary, we have shown that the two sets contain the same elements.

Problem 4

Let A and B be sets. Consider the claim: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Let x be arbitrary.

$$
\begin{aligned}
x \in A \backslash (B \cup C) &\equiv x \in A \wedge \neg(x \in (B \cup C)) && \text{[Def of Set Difference]} \\
&\equiv x \in A \wedge \neg(x \in B \vee x \in C) && \text{[Def of Union]} \\
&\equiv x \in A \wedge (x \notin B \wedge x \notin C) && \text{[De Morgan]} \\
&\equiv (x \in A \wedge x \in A) \wedge (x \notin B \wedge x \notin C) && \text{[Idempotency]} \\
&\equiv (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) && \text{[Associativity/Commutativity]} \\
&\equiv (x \in (A \backslash B)) \wedge (x \in (A \backslash C)) && \text{[Def of Set Difference]}
\end{aligned}
$$

Since x was arbitrary, we have shown that the two sets contain the same elements.

Problem 4

Let A and B be sets. Consider the claim: $A \backslash (B \cup C) = (A \backslash B) \cap (A \backslash C)$.

Let x be arbitrary.

$$
\begin{aligned}
x \in A \backslash (B \cup C) &\equiv x \in A \land \neg(x \in (B \cup C)) && \text{[Def of Set Difference]} \\
&\equiv x \in A \land \neg(x \in B \lor x \in C) && \text{[Def of Union]} \\
&\equiv x \in A \land (x \notin B \land x \notin C) && \text{[De Morgan]} \\
&\equiv (x \in A \land x \in A) \land (x \notin B \land x \notin C) && \text{[Idempotency]} \\
&\equiv (x \in A \land x \notin B) \land (x \in A \land x \notin C) && \text{[Associativity/Commutativity]} \\
&\equiv (x \in (A \backslash B)) \land (x \in (A \backslash C)) && \text{[Def of Set Difference]} \\
&\equiv (x \in (A \backslash B) \cap (A \backslash C)) && \text{[Def of Intersection]}
\end{aligned}
$$

Since x was arbitrary, we have shown that the two sets contain the same elements.

Number Theory (optional)

Problem

Prove that given a|b and b|a that a=b

Try it on Cozy: bit.ly/311S05

That's all Folks!

By: Aruna