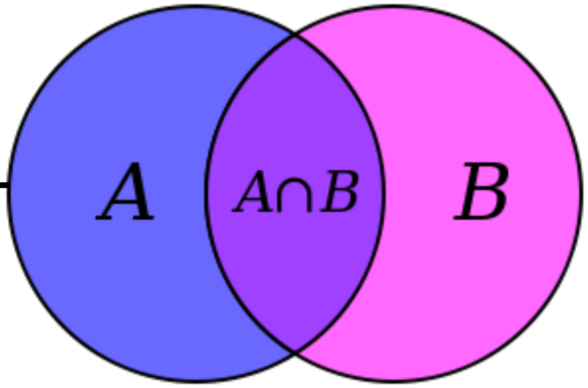
CSE 311: Foundations of Computing

Lecture 10: Set Operations & Representation, Modular Arithmetic

Last Time: Set Theory



Sets are collections of objects called **elements.**

Write a ∈ B to say that a is an element of set B,
and a ∉ B to say that it is not.

Some simple examples
A = {1}
B = {1, 3, 2}
C = {□, 1}
D = {{17}, 17}
E = {1, 2, 7, cat, dog, ∅, α}

Last Time: Operations on Sets

- **Definition for $\cup$ based on $\vee$**

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

- **Definition for $\cap$ based on $\wedge$**

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

- **Complement works like $\neg$**

$$\overline{A} = \{ x : \neg(x \in A) \}$$

Last Time: De Morgan's Laws

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

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

Last Time: De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall \mathrm{x}\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$. Then, by definition of complement, we have $\neg(x \in A \cup B)$. The latter is equivalent to $\neg(x \in A \vee x \in B)$, which is equivalent to $\neg(x \in A) \wedge \neg(x \in B)$ by De Morgan's law. We then have $x \in A^C$ and $x \in B^C$, by the definition of complement, so we have $x \in A^C \cap B^C$ by the definition of intersection.

Proof technique:
To show C = D show
$x \in C \rightarrow x \in D$ and
$x \in D \rightarrow x \in C$

Last Time: De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

Suppose $x \in (A \cup B)^C$.... Then, $x \in A^C \cap B^C$.

Suppose $x \in A^C \cap B^C$. Then, by definition of intersection, we have $x \in A^C$ and $x \in B^C$. That is, we have $\neg(x \in A) \wedge \neg(x \in B)$, which is equivalent to $\neg(x \in A \vee x \in B)$ by De Morgan's law. The last is equivalent to $\neg(x \in A \cup B)$, by the definition of union, so we have shown $x \in (A \cup B)^C$, by the definition of complement. ■

Last Time: De Morgan's Laws

Prove that $(A \cup B)^C = A^C \cap B^C$

Formally, prove $\forall x\ (x \in (A \cup B)^C \leftrightarrow x \in A^C \cap B^C)$

Proof: Let x be an arbitrary object.

The stated bi-condition holds since:

$x \in (A \cup B)^C$	$\equiv \neg(x \in A \cup B)$	def of -^{C}
	$\equiv \neg(x \in A \lor x \in B)$	def of ∪
	$\equiv \neg(x \in A) \land \neg(x \in B)$	De Morgan
	$\equiv x \in A^C \land x \in B^C$	def of -^{C}
	$\equiv x \in A^C \cap B^C$	def of ∩

Chains of equivalences are often easier to read like this rather than as English text

…bitrary, we have shown the sets are equal. ■

It’s Boolean Algebra Again!

Meta-Theorem: Translate any Propositional Logic equivalence into “=” relationship between sets by replacing ∪ with ∨, ∩ with ∧, and $\cdot^C$ with ¬.

“Proof”: Let x be an arbitrary object.

The stated bi-condition holds since:

$x \in$ left side ≡ replace set ops with propositional logic

≡ apply Propositional Logic equivalence

≡ replace propositional logic with set ops

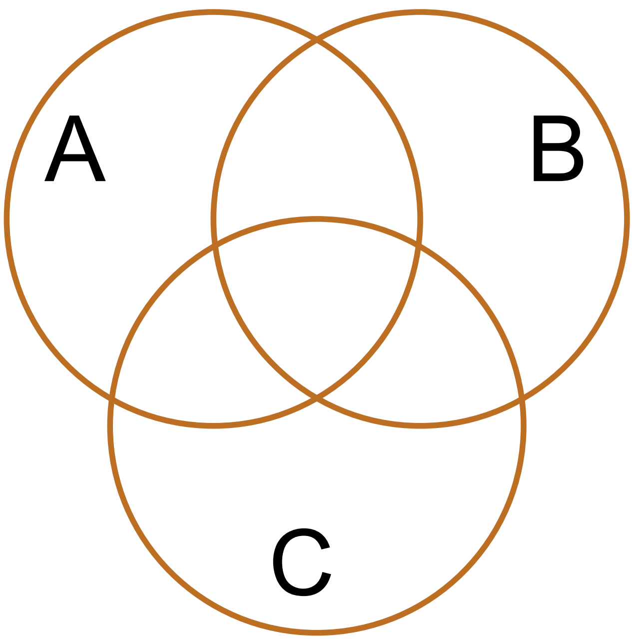
≡ $x \in$ right side

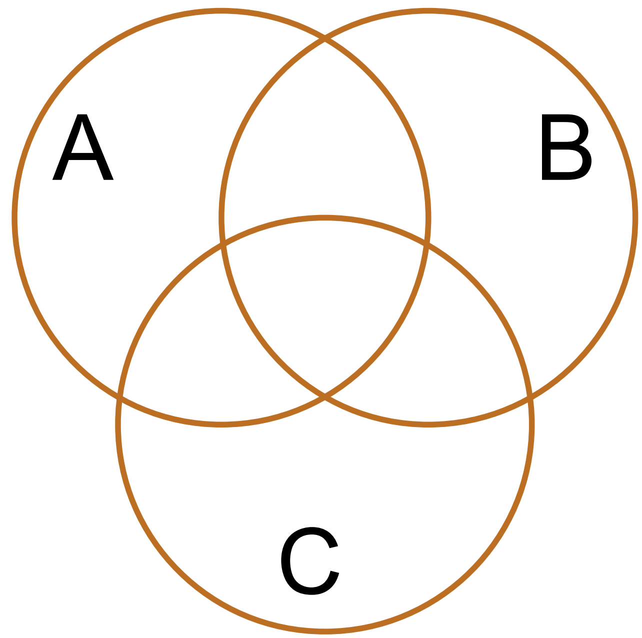
Since x was arbitrary, we have shown the sets are equal.

■

Distributive Laws

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$





Power Set

- Power Set of a set A = set of all subsets of A

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

- e.g., let Days={M,W,F} and consider all the possible sets of days in a week you could ask a question in class

$\mathcal{P}$(Days)=?

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

Power Set

- **Power Set of a set A = set of all subsets of A**

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

- **e.g., let Days={M,W,F} and consider all the possible sets of days in a week you could ask a question in class**

$\mathcal{P}$(Days)=$\{\{M, W, F\}, \{M, W\}, \{M, F\}, \{W, F\}, \{M\}, \{W\}, \{F\}, \varnothing\}$

$\mathcal{P}(\varnothing)=\{\varnothing\} \neq \varnothing$

Cartesian Product

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

$\mathbb{R} \times \mathbb{R}$ is the real plane. You've seen ordered pairs before.

These are just for arbitrary sets.

$\mathbb{Z} \times \mathbb{Z}$ is "the set of all pairs of integers"

If A = {1, 2}, B = {a, b, c}, then A × B = {(1,a), (1,b), (1,c),
(2,a), (2,b), (2,c)}.

Cartesian Product

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

$\mathbb{R} \times \mathbb{R}$ is the real plane. You've seen ordered pairs before.

These are just for arbitrary sets.

$\mathbb{Z} \times \mathbb{Z}$ is "the set of all pairs of integers"

If A = {1, 2}, B = {a, b, c}, then A × B = {(1,a), (1,b), (1,c),
(2,a), (2,b), (2,c)}.

What is $A \times \emptyset$?

Cartesian Product

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

$\mathbb{R} \times \mathbb{R}$ is the real plane. You've seen ordered pairs before.

These are just for arbitrary sets.

$\mathbb{Z} \times \mathbb{Z}$ is "the set of all pairs of integers"

If A = {1, 2}, B = {a, b, c}, then A × B = {(1,a), (1,b), (1,c), (2,a), (2,b), (2,c)}.

$$\boldsymbol{A} \times \emptyset = \{(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a} \in \boldsymbol{A} \wedge \boldsymbol{b} \in \emptyset\} = \{(\boldsymbol{a}, \boldsymbol{b}) : \boldsymbol{a} \in \boldsymbol{A} \wedge \mathbf{F}\} = \emptyset$$

Representing Sets Using Bits

- Suppose universe U is $\{1,2,\ldots,n\}$
- Can represent set $B \subseteq U$ as a vector of bits:

  $b_1 b_2 \ldots b_n$ where $b_i = 1$ when $i \in B$

  $b_i = 0$ when $i \notin B$

  – Called the *characteristic vector* of set B

- Given characteristic vectors for A and B
  – What is characteristic vector for $A \cup B$? $A \cap B$?

Bitwise Operations

$$
\begin{array}{rl}
 & 01101101 \\
\vee & \underline{00110111} \\
 & 01111111
\end{array}
$$

Java: `z=x|y`

$$
\begin{array}{rl}
 & 00101010 \\
\wedge & \underline{00001111} \\
 & 00001010
\end{array}
$$

Java: `z=x&y`

$$
\begin{array}{rl}
 & 01101101 \\
\oplus & \underline{00110111} \\
 & 01011010
\end{array}
$$

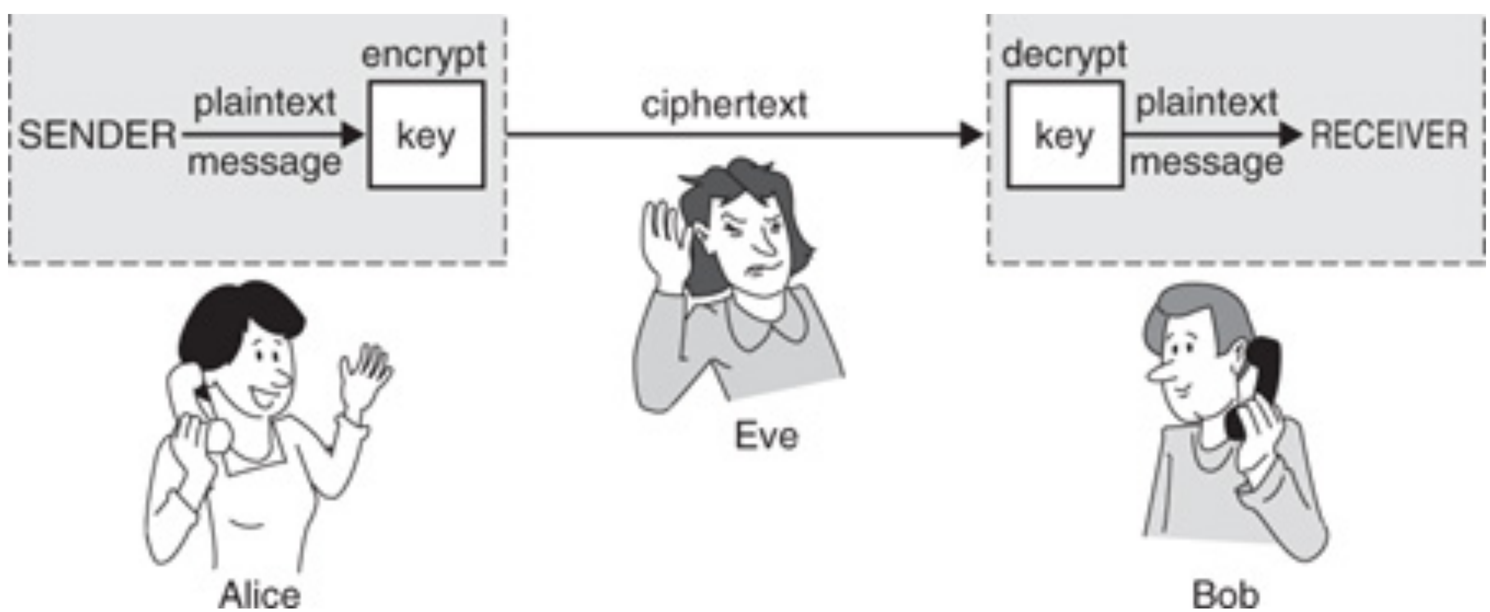
Java: `z=x^y`

A Useful Identity

- If x and y are bits: $(x \oplus y) \oplus y = ?$
- What if x and y are bit-vectors?

Private Key Cryptography

- **Alice** wants to communicate message secretly to **Bob** so that eavesdropper **Eve** who hears their conversation cannot tell what **Alice**'s message is.
- **Alice** and **Bob** can get together and privately share a secret key K ahead of time.



One-Time Pad

- Alice and Bob privately share random n-bit vector K
  - Eve does not know K
- Later, Alice has n-bit message m to send to Bob
  - Alice computes $C = m \oplus K$
  - Alice sends C to Bob
  - Bob computes $m = C \oplus K$ which is $(m \oplus K) \oplus K$
- Eve cannot figure out m from C unless she can guess K

Russell's Paradox

$$S = \{ x : x \notin x \}$$

Suppose for contradiction that $S \in S$...

Russell's Paradox

$$S = \{ x : x \notin x \}$$

Suppose for contradiction that $S \in S$. Then, by definition of S, $S \notin S$, but that's a contradiction.

Suppose for contradiction that $S \notin S$. Then, by definition of the set S, $S \in S$, but that's a contradiction, too.

This is reminiscent of the truth value of the statement "This statement is false."

Number Theory (and applications to computing)

- Branch of Mathematics with direct relevance to computing
- Many significant applications
  - Cryptography
  - Hashing
  - Security
- Important tool set

Modular Arithmetic

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

I’m ALIVE!

```
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println(
            “I will be alive for at least ” +
            SEC_IN_YEAR * 101 + “ seconds.”
        );
    }
}
```

I'm ALIVE!

```
public class Test {
    final static int SEC_IN_YEAR = 364*24*60*60*100;
    public static void main(String args[]) {
        System.out.println(
            "I will be alive for at least " +
            SEC_IN_YEAR * 101 + " seconds."
        );
    }
}
```

```
 ----jGRASP exec: java Test
I will be alive for at least -186619904 seconds.

 ----jGRASP: operation complete.
```

Divisibility

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
1 | 5	5 | 25	0 | 5	2 | 3

Divisibility

Definition: "a divides b"

For $a \in \mathbb{Z}, b \in \mathbb{Z}$ with $a \neq 0$:

$$a \mid b \leftrightarrow \exists k \in \mathbb{Z}\ (b = ka)$$

Check Your Understanding. Which of the following are true?

5 | 1	25 | 5	5 | 0	3 | 2
5 | 1 iff 1 = 5k	25 | 5 iff 5 = 25k	5 | 0 iff 0 = 5k	3 | 2 iff 2 = 3k
1 | 5	5 | 25	0 | 5	2 | 3
1 | 5 iff 5 = 1k	5 | 25 iff 25 = 5k	0 | 5 iff 5 = 0k	2 | 3 iff 3 = 2k

Division Theorem

Division Theorem

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

To put it another way, if we divide *d* into *a*, we get a unique quotient *q* = *a* **div** *d*
and non-negative remainder *r* = *a* **mod** *d*

Note: r ≥ 0 even if a < 0.
Not quite the same as `a%d`.

Division Theorem

Division Theorem

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

To put it another way, if we divide *d* into *a*, we get a unique quotient ***q* = *a* div *d***
and non-negative remainder ***r* = *a* mod *d***

```
public class Test2 {
    public static void main(String args[]) {
        int a = -5;
        int d = 2;
        System.out.println(a % d);
    }
}
```

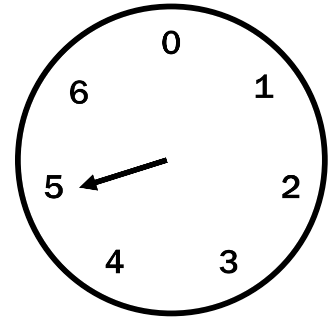
```
 ----jGRASP exec: java Test2
-1

 ----jGRASP: operation complete.
```

Note: r ≥ 0 even if a < 0.
Not quite the same as `a%d`.

Arithmetic, mod 7

$$a +_7 b = (a + b) \bmod 7$$

$$a \times_7 b = (a \times b) \bmod 7$$



+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

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

Check Your Understanding. What do each of these mean? When are they true?

x ≡ 0 (mod 2)

-1 ≡ 19 (mod 5)

y ≡ 2 (mod 7)

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a, b, m \in \mathbb{Z}$ with $m > 0$

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

Check Your Understanding. What do each of these mean? When are they true?

x ≡ 0 (mod 2)

This statement is the same as saying "x is even"; so, any x that is even (including negative even numbers) will work.

-1 ≡ 19 (mod 5)

This statement is true. 19 - (-1) = 20 which is divisible by 5

y ≡ 2 (mod 7)

This statement is true for y in { ..., -12, -5, 2, 9, 16, ...}. In other words, all y of the form 2+7k for k an integer.

Modular Arithmetic: A Property

Let a, b, m be integers with $m > 0$.
Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Suppose that $a \equiv b \pmod{m}$.

Suppose that $a \bmod m = b \bmod m$.

Modular Arithmetic: A Property

Let a, b, m be integers with $m > 0$.
Then, $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

Suppose that $a \equiv b \pmod{m}$.

Then, $m \mid (a - b)$ by definition of congruence.

So, $a - b = km$ for some integer k by definition of divides.

Therefore, $a = b + km$.

Taking both sides modulo m we get:

$$a \bmod m = (b + km) \bmod m = b \bmod m.$$

Suppose that $a \bmod m = b \bmod m$.

By the division theorem, $a = mq + (a \bmod m)$ and
$b = ms + (b \bmod m)$ for some integers q, s.

Then, $a - b = (mq + (a \bmod m)) - (ms + (b \bmod m))$
$= m(q - s) + (a \bmod m - b \bmod m)$
$= m(q - s)$ since $a \bmod m = b \bmod m$

Therefore, $m \mid (a - b)$ and so $a \equiv b \pmod{m}$.