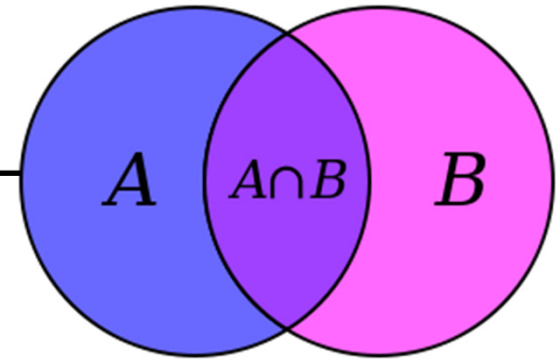


CSE 311: Foundations of Computing

Lecture 10: Set Operations & Representation, Modular Arithmetic



Last Class: Set Theory



Sets are collections of objects called elements.

Write $a \in B$ to say that a is an element of set B ,
and $a \notin B$ to say that it is not.

Some simple examples

$$A = \{1\}$$

$$B = \{1, 3, 2\}$$

$$C = \{\square, 1\}$$

$$D = \{\{17\}, 17\}$$

$$E = \{1, 2, 7, \text{cat}, \text{dog}, \emptyset, \alpha\}$$

Last Class: Definitions

- A and B are *equal* if they have the same elements

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

- A is a *subset* of B if every element of A is also in B

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

- Note: $(A = B) \equiv (A \subseteq B) \wedge (B \subseteq A)$

Last Class: Building Sets from Predicates

S = the set of all x for which $P(x)$ is true

$$S = \{x : P(x)\}$$

S = the set of all x in A for which $P(x)$ is true

$$S = \{x \in A : P(x)\}$$

*in the domain of P , usually called the “universe” U

Last Class: It's Boolean algebra again

- 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

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

Last Class: De Morgan's Laws

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

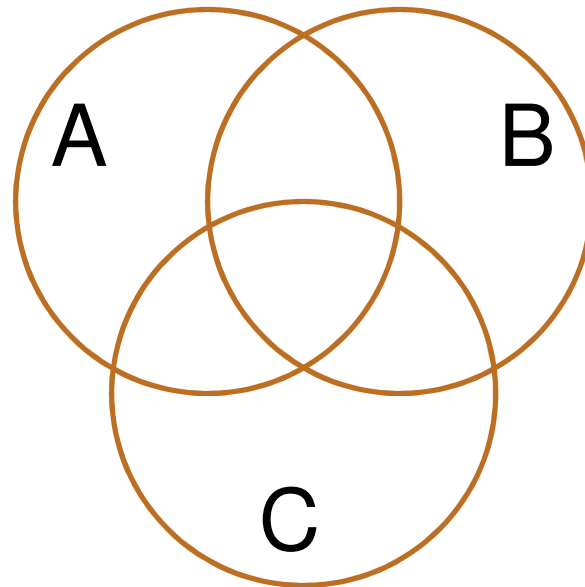
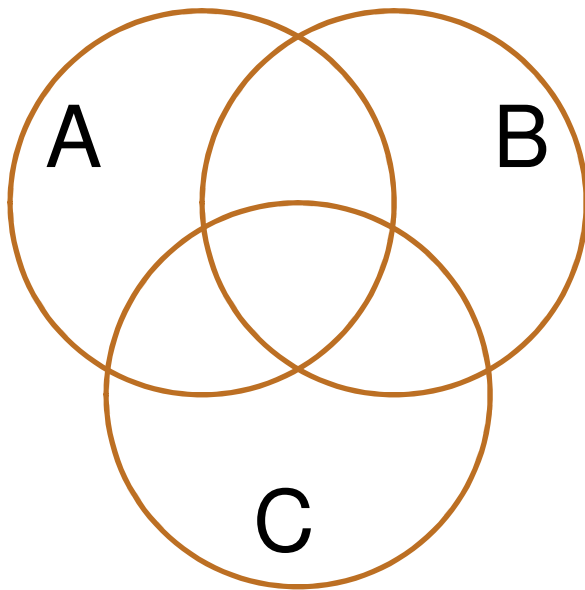
$$\begin{aligned} x \in \overline{A \cup B} &\equiv \neg(x \in A \cup B) \quad \text{Definition of } \bar{} \\ &\equiv \neg((x \in A) \vee (x \in B)) \quad \text{Definition of } \cup \\ &\equiv \neg(x \in A) \wedge \neg(x \in B) \quad \text{De Morgan} \\ &\equiv (x \in \bar{A}) \wedge (x \in \bar{B}) \quad \text{Definition of } \bar{} \\ &\equiv x \in \bar{A} \cap \bar{B} \quad \text{Definition of } \cap \end{aligned}$$

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

Similar

Last Class: Distributive Laws

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



A Simple Set Proof

Prove that for any sets A and B we have $(A \cap B) \subseteq A$

Remember the definition of subset?

$$X \subseteq Y \equiv \forall x (x \in X \rightarrow x \in Y)$$

A Simple Set Proof

Prove that for any sets A and B we have $(A \cap B) \subseteq A$

Remember the definition of subset?

$$X \subseteq Y \equiv \forall x (x \in X \rightarrow x \in Y)$$

Proof: Let A and B be arbitrary sets and x be an arbitrary element of $A \cap B$.

Then, by definition of $A \cap B$, $x \in A$ and $x \in B$.

It follows that $x \in A$, as required. ■

Power Set

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

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

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

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

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

Power Set

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

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

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

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

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

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

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

Representing Sets Using Bits

- Suppose universe U is $\{1, 2, \dots, n\}$
- Can represent set $B \subseteq U$ as a vector of bits:
 $b_1 b_2 \dots b_n$ 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 $A \cup B$? $A \cap B$?

UNIX/Linux File Permissions

- `ls -l`

```
drwxr-xr-x ... Documents/
```

```
-rw-r--r-- ... file1
```

- Permissions maintained as bit vectors
 - Letter means bit is 1
 - “-” means bit is 0.

Bitwise Operations

$$\begin{array}{r} 01101101 \\ \vee \ 00110111 \\ \hline 01111111 \end{array}$$

Java: $z = x | y$

$$\begin{array}{r} 00101010 \\ \wedge \ 00001111 \\ \hline 00001010 \end{array}$$

Java: $z = x \& y$

$$\begin{array}{r} 01101101 \\ \oplus \ 00110111 \\ \hline 01011010 \end{array}$$

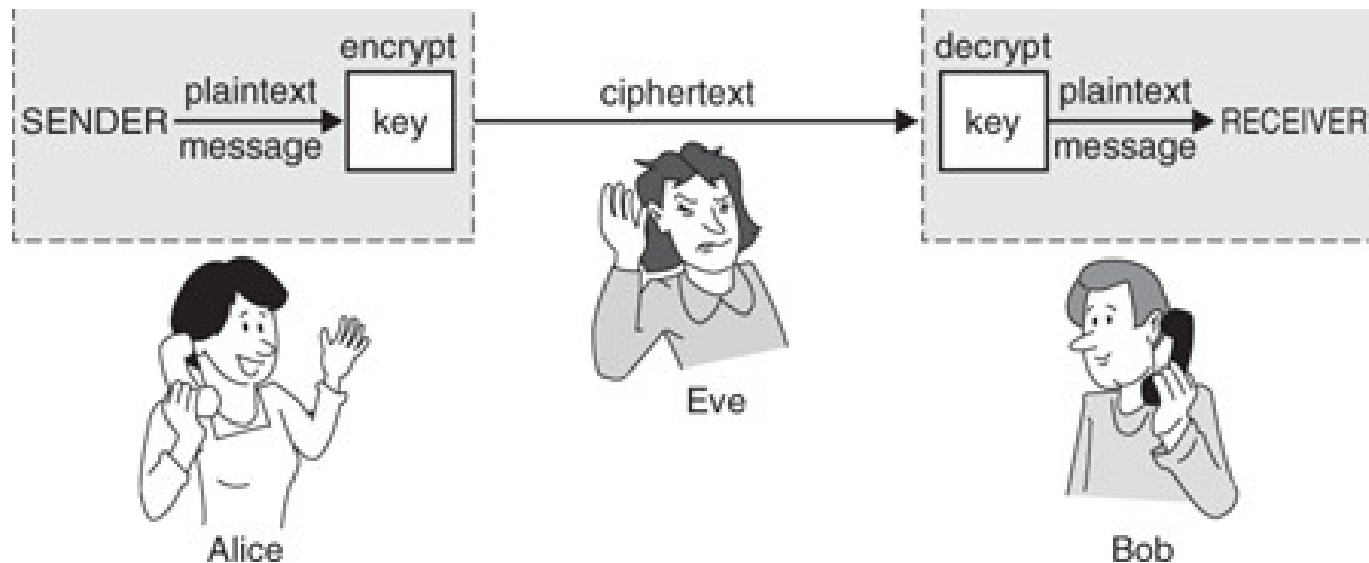
Java: $z = x \wedge y$

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 that $S \in S$...

Russell's Paradox

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

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

Suppose 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?

$5 \mid 1$

$25 \mid 5$

$5 \mid 0$

$3 \mid 2$

$1 \mid 5$

$5 \mid 25$

$0 \mid 5$

$2 \mid 3$

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?

$$5 \mid 1$$

$$5 \mid 1 \text{ iff } 1 = 5k$$

$$25 \mid 5$$

$$25 \mid 5 \text{ iff } 5 = 25k$$

$$5 \mid 0$$

$$5 \mid 0 \text{ iff } 0 = 5k$$

$$3 \mid 2$$

$$3 \mid 2 \text{ iff } 2 = 3k$$

$$1 \mid 5$$

$$1 \mid 5 \text{ iff } 5 = 1k$$

$$5 \mid 25$$

$$5 \mid 25 \text{ iff } 25 = 5k$$

$$0 \mid 5$$

$$0 \mid 5 \text{ iff } 5 = 0k$$

$$2 \mid 3$$

$$2 \mid 3 \text{ iff } 3 = 2k$$

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 $q = a \text{ div } d$
and non-negative remainder $r = a \text{ mod } d$

Note: $r \geq 0$ 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 $q = a \text{ div } d$
and non-negative remainder $r = a \text{ mod } d$

```
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: $r \geq 0$ 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?**

$$x \equiv 0 \pmod{2}$$

$$-1 \equiv 19 \pmod{5}$$

$$y \equiv 2 \pmod{7}$$

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?**

$$x \equiv 0 \pmod{2}$$

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

$$-1 \equiv 19 \pmod{5}$$

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

$$y \equiv 2 \pmod{7}$$

This statement is true for y in $\{ \dots, -12, -5, 2, 9, 16, \dots \}$. 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

$$b = ms + (b \bmod m) \text{ for some integers } q, s.$$

$$\begin{aligned} \text{Then, } a - b &= (mq + (a \bmod m)) - (ms + (b \bmod m)) \\ &= m(q - s) + (a \bmod m - b \bmod m) \\ &= m(q - s) \text{ since } a \bmod m = b \bmod m \end{aligned}$$

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