CSE 311: Foundations of Computing

Lecture 10: Set Operations & Representation, Modular Arithmetic

A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI, A'LA'IH, A'LA'IH, DO'NEH'LINI, A'LA'IH, DO'NEH'LINI, DO'NEH'LINI, DO'NEH'LINI . . .
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
...IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

Definitions

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

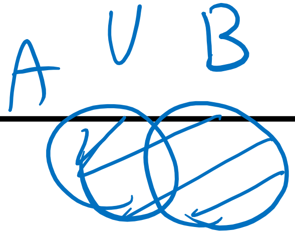
$$A = B \equiv \forall x\,(x \in A \leftrightarrow x \in B)$$

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

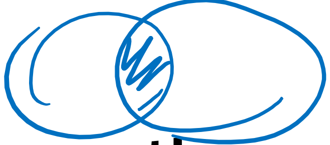
$$A \subseteq B \equiv \forall x\,(x \in A \rightarrow x \in B)$$

- Note: $(\boldsymbol{A} = \boldsymbol{B}) \equiv (\boldsymbol{A} \subseteq \boldsymbol{B}) \land (\boldsymbol{B} \subseteq \boldsymbol{A})$

Set Operations

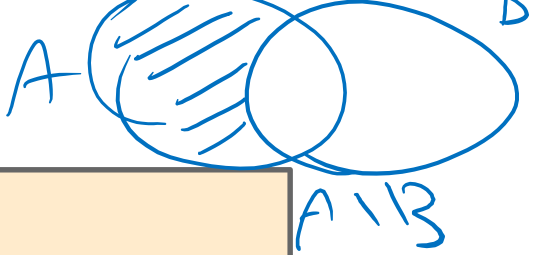


$$A \cup B = \{\, x : (x \in A) \vee (x \in B) \}$$ **Union**



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

$$A \setminus B = \{\, x : (x \in A) \wedge (x \notin B) \}$$ **Set Difference**



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

QUESTIONS

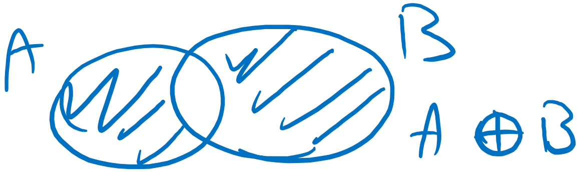
Using A, B, C and set operations, make…

[6] = A ⋃ B ⋃ C

{3} = A ⋂ B = A ⋂ C

{1,2} = A \ B = A \ C

More Set Operations



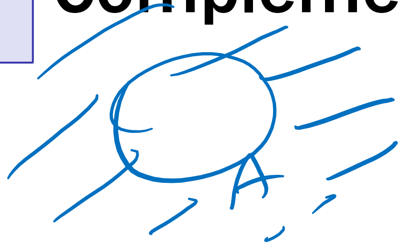
$$A \oplus B = \{\, x : (x \in A) \oplus (x \in B)\}$$

Symmetric Difference

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

(with respect to universe U)

Complement



A = {1, 2, 3}
B = {1, 2, 4, 6}
Universe:
U = {1, 2, 3, 4, 5, 6}

$A \oplus B$ = {3, 4, 6}
$\overline{A}$ = {4,5,6}

It’s Boolean algebra again

- Definition for ∪ based on ∨

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

- Definition for ∩ based on ∧

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

- Complement works like ¬

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

De Morgan's Laws

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

Informal.

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

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

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

let x arbitrary in $\overline{A \cup B}$. This means $\neg(x \in A \cup B)$. Therefore $\neg(x \in A \vee x \in B)$ is true. By demorgan's $x \notin A$ and $x \notin B$. This implies that $x \in \bar{A} \cap \bar{B}$. Since x was arbitrary $\overline{A \cup B} \subseteq \bar{A} \cap \bar{B}$.

$\supseteq$

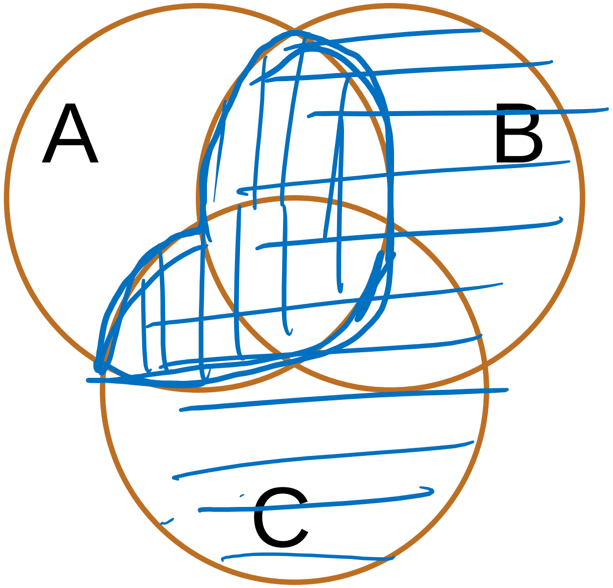
$\Rightarrow \overline{A \cup B} = \bar{A} \cap \bar{B}$

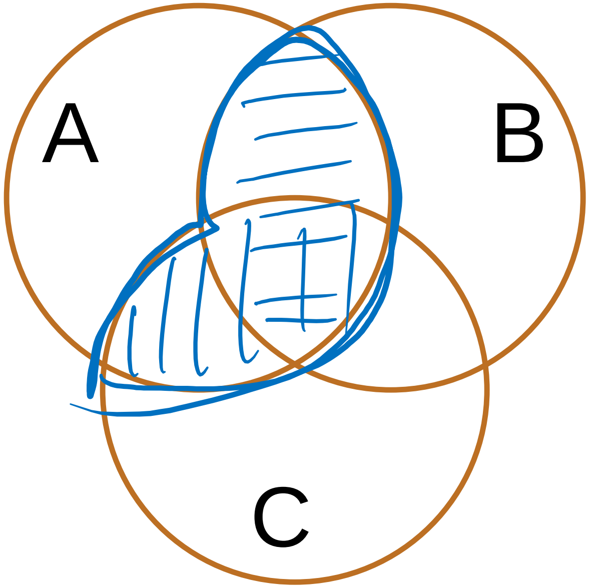
$$\overline{A \cap B} = \bar{A} \cup \bar{B}$$

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

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?

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

Pf. Let x be arbitrary in $A \cap B$.

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

Therefore $x \in A$. Since x was arbitrary

$\forall x \quad x \in A \cap B \rightarrow x \in A$. So $A \cap B \subseteq A$.

A Simple Set Proof

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

Remember the definition of subset?

$$X \subseteq Y \equiv \forall x\, (x \in X \to x \in Y)$$

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

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

- 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)=? $\{\{M\}, \emptyset, \{W\}, \{F\}, \{M,W\}, \{M,W,F\}, \{M,F\}, \{W,F\}\}.$

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

Power Set

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

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

If A has n, $\mathcal{P}(A)$ has 2^n elmts.

- 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

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

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

$P(\{\varnothing\})$

$P(P(\{\varnothing\}))$.

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"

$(a,1) \notin A \times B$

order matter

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

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

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 $\overset{a}{\frown}{A}$ and $\overset{b}{\frown}{B}$
  - What is characteristic vector for $\underset{a \vee b}{A \cup B}$? $\underset{a \wedge b}{A \cap B}$?

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

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

Java: `z=x|y`

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

Java: `z=x&y`

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

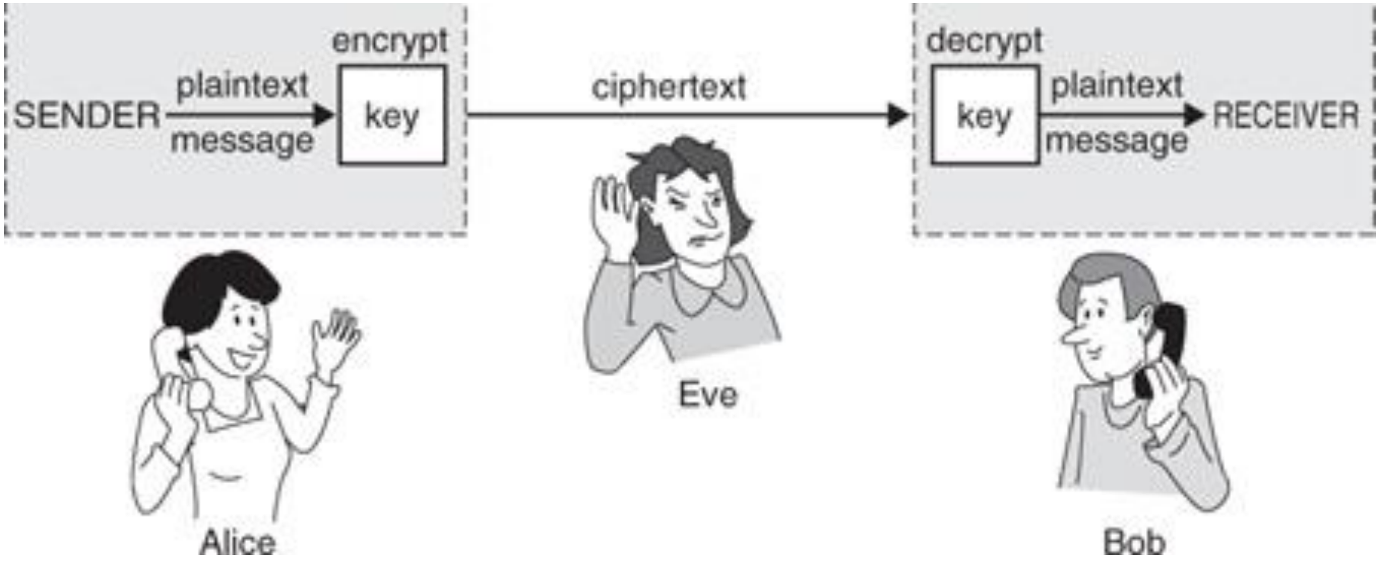
Java: `z=x^y`

A Useful Identity

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

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

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

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

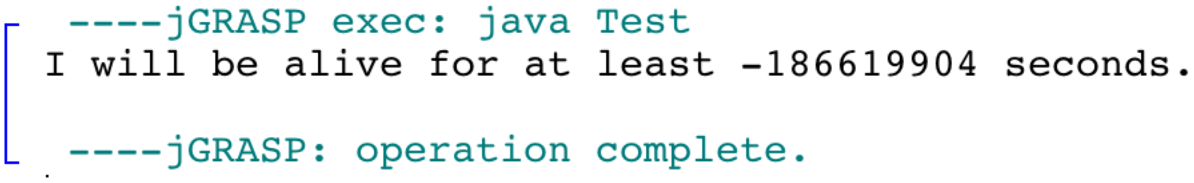
- In computing, almost all computations are over a finite domain

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 $\boxed{a \neq 0}$:

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

Check Your Understanding. Which of the following are true?

~~$5 \mid 1$~~

$1 = 5 \cdot k$

~~$25 \mid 5$~~

$5 = 25 \cdot k$

$5 \mid 0$ ✓

$0 = 5 \cdot \underbrace{k}_{0}$

~~$3 \mid 2$~~

$2 = 3 \cdot k$

$1 \mid 5$ ✓

$5 = 1 \cdot 5$

$5 \mid 25$ ✓

$25 = 5 \cdot 5$

$0 \mid 5$ ✗

$5 = 0 \cdot k$

$2 \mid 3$ ✗

$3 = 2 \cdot k$

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

$a = 13$ and $d = 4$

$q = 3$ $r = 1$ $13 = \underset{q}{3} \cdot 4 + \underset{r}{1}$

Division Theorem

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

there exist *unique* integers *q*, *r* with $\boxed{0 \leq r < d}$

such that $\boxed{a = dq + r.}$

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*

$a = -13$ $d = 4$

$q = -4$ $r = 3$

$-13 = \cancel{(-3)\cdot 4} - 1$

$-13 = (-4)\cdot 4 + 3$

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

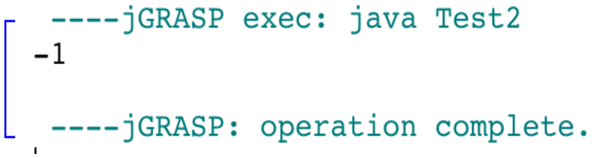
Division Theorem

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

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

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

$5 . 3 = 15$

$15 \bmod 7 = 1$

+	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 $a \equiv b \pmod m$.