CSE 311

Foundations of Computing I

Some Reminders/Hints for HW3

Style matters in proofs!

Do NOT manipulate large statements by equivalences! This is horrible style and will lose points if there is a significantly cleaner proof.

Our inference rules can only prove things true. Do not "prove the negation false"! It doesn't make sense.

After you're done writing your proof, you should proof-read (heh) it.

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 = {4, 5, 6}
C = {3, 4}

QUESTIONS

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

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

{3} = A ∩ C

{1,2} =

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 = {4, 5, 6}
C = {3, 4}

QUESTIONS

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

[6] = A ∪ B = A ∪ B ∪ C

{3} = C ∖ B = A ∖ B = A ∩ C

{1,2} = A ∖ C = (A ∪ B) ∖ C

More Set Operations

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

Symmetric Difference

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

(with respect to universe U)

Complement

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

QUESTIONS

Let S = {1, 2}.

If the universe is A, then $\overline{S}$ is... {3}

If the universe is B, then $\overline{S}$ is... {4, 6}

If the universe is C, then $\overline{S}$ is...

More Set Operations

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

Symmetric Difference

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

(with respect to universe U)

Complement

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

QUESTIONS

Let S = {1, 2}.

If the universe is A, then $\overline{S}$ is... **A \ S = {3}**

If the universe is B, then $\overline{S}$ is... **B \ S = {4, 6}**

If the universe is C, then $\overline{S}$ is... **C \ S = {3, 4}**

Power Set

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

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

$A \subseteq A$

$\emptyset \subseteq A$

- Let Days = {M, W, F}. Suppose we wanted to know the possible ways that we could allocate class days to be cancelled. Let's call this set $\mathcal{P}(\text{Days})$.

e.g. $\mathcal{P}(\text{Days}) = \{$

$\emptyset$, $\{M, W, F\}$

$\{M\}$, $\{W\}$, $\{F\}$, $\{M, W\}$

$\}$

e.g. $\mathcal{P}(\emptyset) = ?$

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

Power Set

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

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

- Let Days = {M, W, F}. Suppose we wanted to know the possible ways that we could allocate class days to be cancelled. Let's call this set $\mathcal{P}(\text{Days})$.

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

e.g. $\mathcal{P}(\emptyset) = \{\emptyset\}$

Cartesian Product

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

$A \times \{\emptyset\} = \{(a,b) : a \in A \wedge b \in \{\emptyset\}\}$ $(a, \emptyset)$ $(2, \emptyset)$ ...

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

$\emptyset \subseteq \emptyset$

These are just for arbitrary sets.

$\mathbb{Z} \times \mathbb{Z}$ is "the set of all pairs of integers" $(b, 1)$

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

$A \times \{\emptyset\}$

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

Russell's Paradox

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

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

S contains itself.

$S \notin S$

$S \notin S \rightarrow S \in S$

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 comprehension, S $\in$ S, but that's a contradiction.

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

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 ¬**

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

(with respect to universe U)

De Morgan's Laws

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

Let U be the universe.

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

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

$=$

$=$

$=$

$=$

$=$

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

De Morgan's Laws

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

Let U be the universe.

$$
\begin{aligned}
\overline{A \cup B} &= \{x : x \notin A \cup B\} \\
&= \{x : \neg(x \in A \cup B)\} \\
&= \{x : \neg((x \in A) \vee (x \in B))\} \\
&= \{x : (x \notin A) \wedge (x \notin B)\} \\
&= \{x : (x \in \overline{A}) \wedge (x \in \overline{B})\} \\
&= \{x : (x \in \overline{A})\} \cap \{x : (x \in \overline{B})\} \\
&= \overline{A} \cap \overline{B}
\end{aligned}
$$

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

De Morgan's Laws

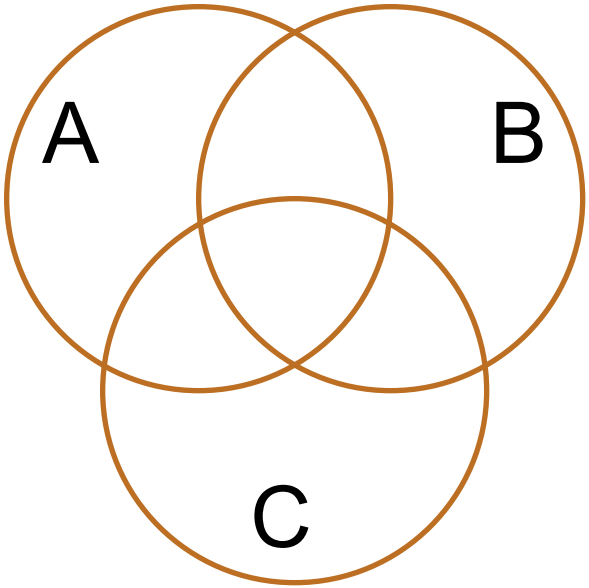
Prove $\overline{A \cap B} = \overline{A} \cup \overline{B}$

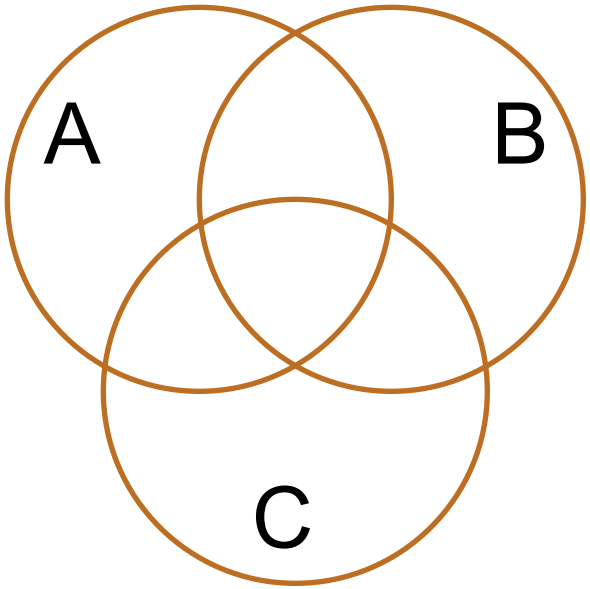
Let U be the universe.

$$
\begin{aligned}
\overline{A \cap B} &= \{x : x \notin A \cap B\} \\
&= \{x : \neg(x \in A \cap B)\} \\
&= \{x : \neg((x \in A) \wedge (x \in B))\} \\
&= \{x : (x \notin A) \vee (x \notin B)\} \\
&= \{x : (x \in \overline{A}) \vee (x \in \overline{B})\} \\
&= \{x : (x \in \overline{A})\} \cup \{x : (x \in \overline{B})\} \\
&= \overline{A} \cup \overline{B}
\end{aligned}
$$

Distributive Laws

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





One More

Prove $(A \cap B) \subseteq A$

Remember the definition of subset?

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

$A \cap B \subseteq A$

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

So,

One More

Prove $(A \cap B) \subseteq A$

Remember the definition of subset?

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

Let 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.**

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 $A \cup B$? $A \cap B$?

UNIX/Linux File Permissions

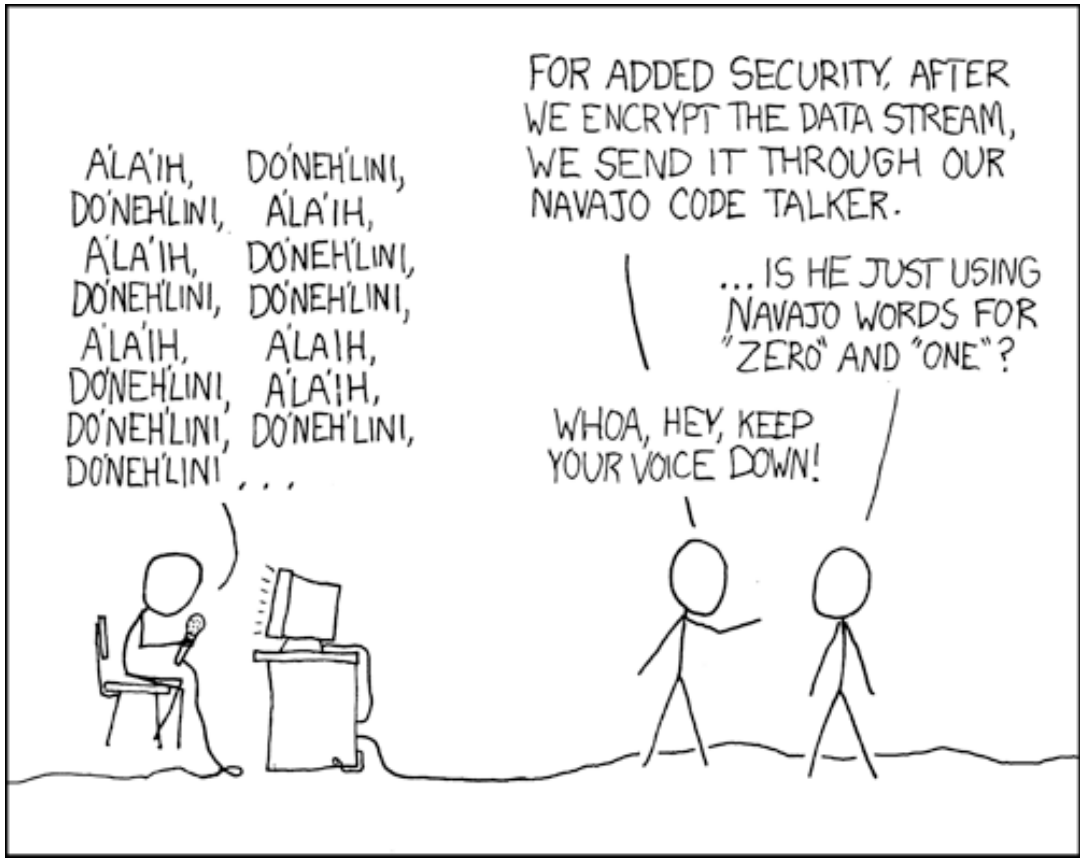
- `ls –l`

```
drwxr-xr-x ... Documents/
-rw-r--r-- ... file1
```

- Permissions maintained as bit vectors
  - Letter means bit is 1
  - "–" means bit is 0.

CSE 311: Foundations of Computing

Lecture 10: Modular Arithmetic



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

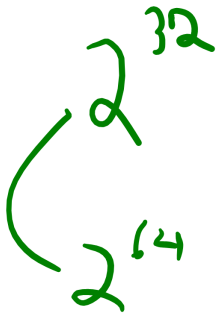
- In computing, almost all computations are over a finite domain

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 $a \neq 0$:

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

Check Your Understanding. Which of the following are true?

$5 \mid 25$

$5 \mid 1$ $\quad 1 = 5 \cdot k$

$25 \mid 5$

$5 \mid 5$

$3 \mid 2$

$1 \mid 5$

$5 \mid 25$

$0 \mid 1$

$2 \mid 3$

Divisibility

Definition: "a divides b"

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

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

Check Your Understanding. Which of the following are true?

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

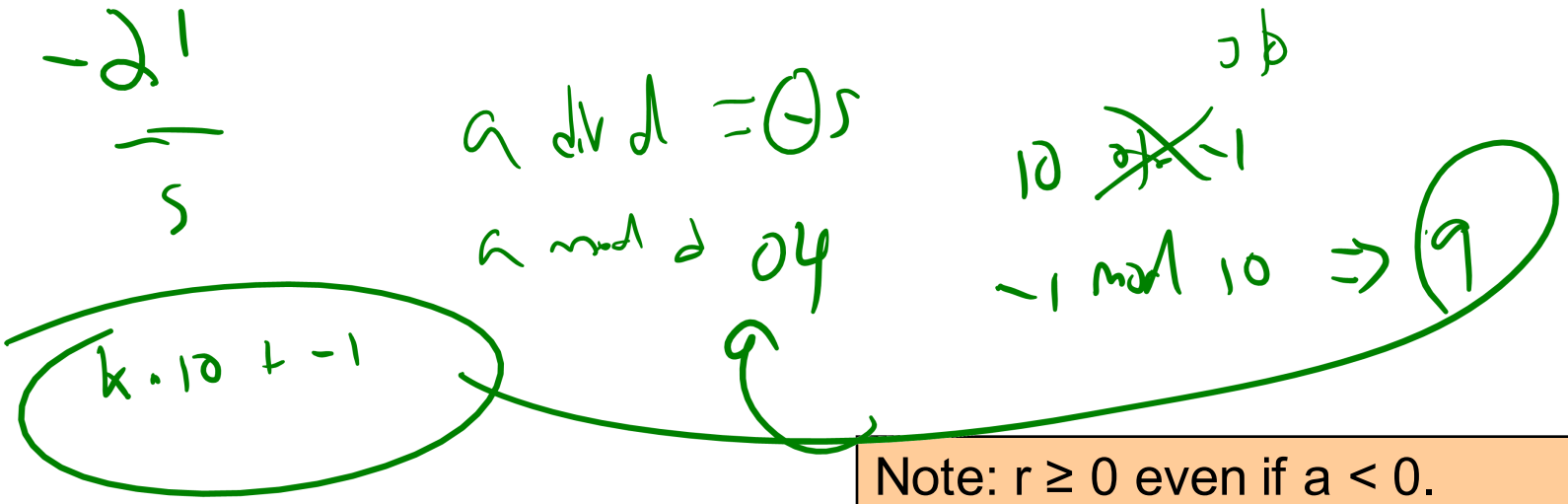
Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}^+$:

Then, there exists *unique* integers *q*, *r* with $0 \leq r < d$ such that $a = dq + r$.

To put it another way, if we take a/d, we get a dividend and a remainder: $q = a$ **div** d $\quad r = a$ **mod** d



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

Division Theorem

Division Theorem

For $a \in \mathbb{Z}, d \in \mathbb{Z}^+$:

Then, there exists *unique* integers *q*, *r* with $0 \leq r < d$ such that $a = dq + r$.

To put it another way, if we take a/d, we get a dividend and a remainder: $q = a \textbf{ div } d$ $\quad r = a \textbf{ mod } d$

```
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 $a \in \mathbb{Z}, b \in \mathbb{Z}, \mathrm{m} \in \mathbb{Z}$:

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

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

A ≡ 0 (mod 2)

1 ≡ 0 (mod 4)

A ≡ -1 (mod 17)

Modular Arithmetic

Definition: "a is congruent to b modulo m"

For $a \in \mathbb{Z}, b \in \mathbb{Z}, \mathrm{m} \in \mathbb{Z}$:

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

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

A ≡ 0 (mod 2)

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

1 ≡ 0 (mod 4)

This statement is false. If we take it mod 1 instead, then the statement is true.

A ≡ -1 (mod 17)

If A = 17x – 1 = 17x + 16, then it works.

Note that (m – 1) mod m = ((m mod m) + (-1 mod m)) mod m

= (0 + -1) mod m = -1 mod m

Modular Arithmetic: A Property

Let a and b be integers, and let m be a positive integer. 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 and b be integers, and let m be a positive integer. 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, $a - b = (mq + (a \bmod m)) - (mr + (b \bmod m))$

$= m(q - r) + (a \bmod m - b \bmod m)$

$= m(q - r)$ since $a \bmod m = b \bmod m$

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

Modular Arithmetic: Another Property

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then **$a + c \equiv b + d \pmod{m}$**

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Unrolling definitions gives us some k such that
$a - b = km$, and some j such that $c - d = jm$.

Adding the equations together gives us
$(a + c) - (b + d) = m(k + j)$. Now, re-applying the definition of mod gives us $a + c \equiv b + d \pmod{m}$.

Modular Arithmetic: Another-nother Property

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then **$ac \equiv bd \pmod{m}$**

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Unrolling definitions gives us some k such that
$a - b = km$, and some j such that $c - d = jm$.

Then, $a = km + b$ and $c = jm + d$. Multiplying both together gives us $ac = (km + b)(jm + d) = kjm^2 + kmd + jmb + bd$.

Re-arranging gives us $ac - bd = m(kjm + kd + jb)$. Using the definition of mod gives us $ac \equiv bd \pmod{m}$.

Example

Let n be an integer.
Prove that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$

Let's start by looking a a small example:

$0^2 = 0 \equiv 0 \pmod 4$
$1^2 = 1 \equiv 1 \pmod 4$
$2^2 = 4 \equiv 0 \pmod 4$
$3^2 = 9 \equiv 1 \pmod 4$
$4^2 = 16 \equiv 0 \pmod 4$

It looks like

$n \equiv 0 \pmod 2 \rightarrow n^2 \equiv 0 \pmod 4$, and
$n \equiv 1 \pmod 2 \rightarrow n^2 \equiv 1 \pmod 4$.

Case 1 (n is even):

Suppose $n \equiv 0 \pmod 2$.
Then, $n = 2k$ for some k.
So, $n^2 = (2k)^2 = 4k^2$. So, by definition of congruence, $n^2 \equiv 0 \pmod 4$.

Case 2 (n is odd):

Suppose $n \equiv 1 \pmod 2$.
Then, $n = 2k + 1$ for some k.
So, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. So, by definition of congruence, $n^2 \equiv 1 \pmod 4$.

Bitwise Operations

```
  01101101
∨ 00110111
  --------
  01111111
```

Java: `z=x|y`

```
  00101010
∧ 00001111
  --------
  00001010
```

Java: `z=x&y`

```
  01101101
⊕ 00110111
  --------
  01011010
```

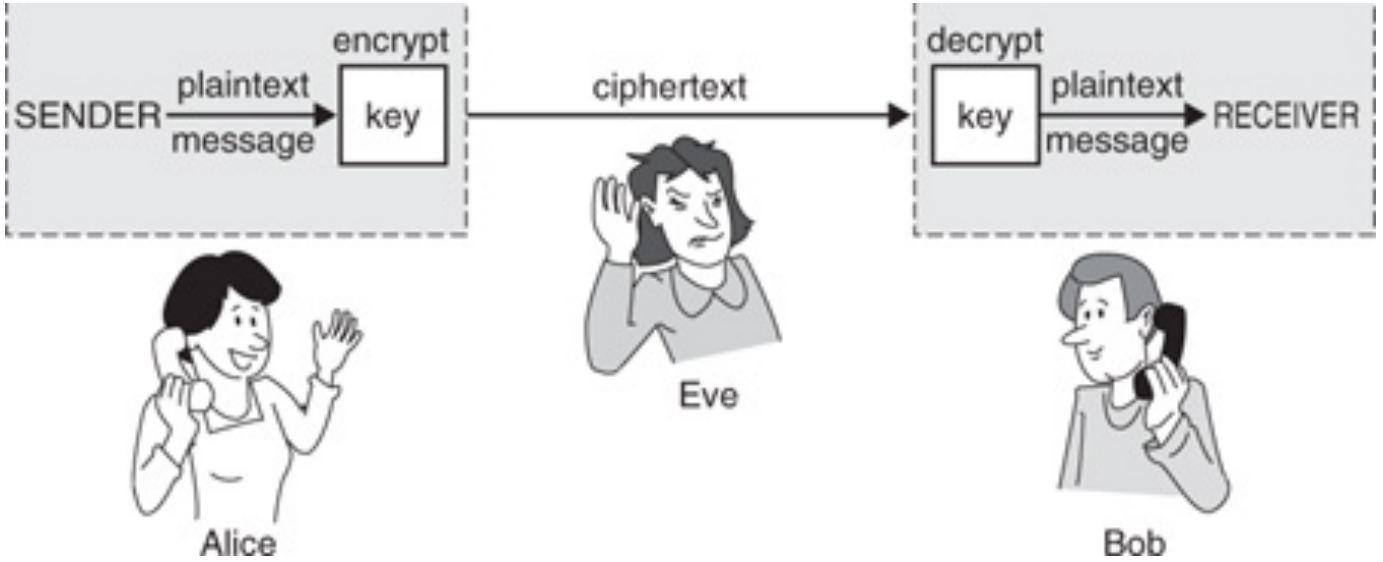
Java: `z=x^y`

A Useful Identity

- If x and y are bits: $(x \oplus y) \oplus y = ?$
  - $(x \oplus y) \oplus y = x \oplus (y \oplus y) = x \oplus 0 = x$

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