
# Lecture 27: Inclusion-exclusion Principle

Dr. Chengjiang Long
Computer Vision Researcher at Kitware Inc.
Adjunct Professor at SUNY at Albany.
Email: **clong2@albany.edu**

# Announcement

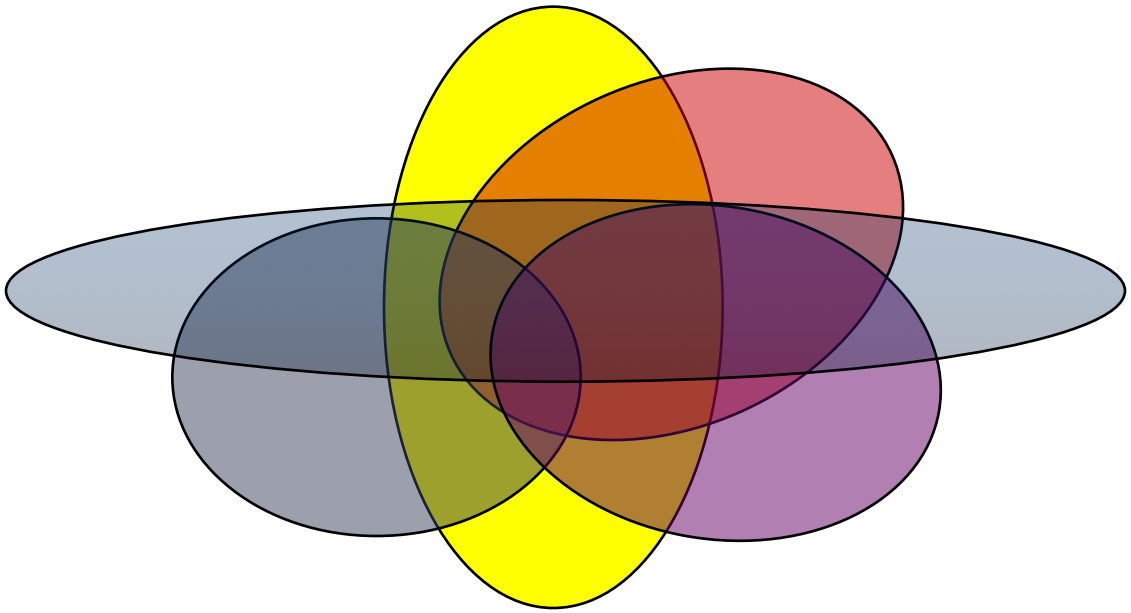
- Our last class is Dec 10th, 2018.
- Final Exam will be taken on Dec 17th, 2018 (Monday).
  - Two-hour exam from 3:30 pm to 5:30 pm at LC 25.
  - It will cover all the contents which we have talked in class.
  - Can be close book & close notes, or open book & open notes.

# Outline

- Inclusion-exclusion Principle
- Review on Modular Exponentiation Algorithm

# Outline

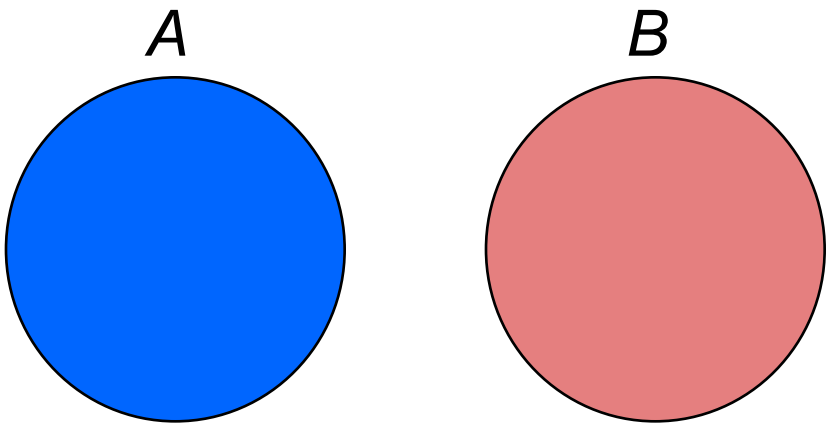
- **Inclusion-exclusion Principle**
- Review on Modular Exponentiation Algorithm



# Sum Rule

If sets $A$ and $B$ are disjoint, then

$$|A \cup B| = |A| + |B|$$

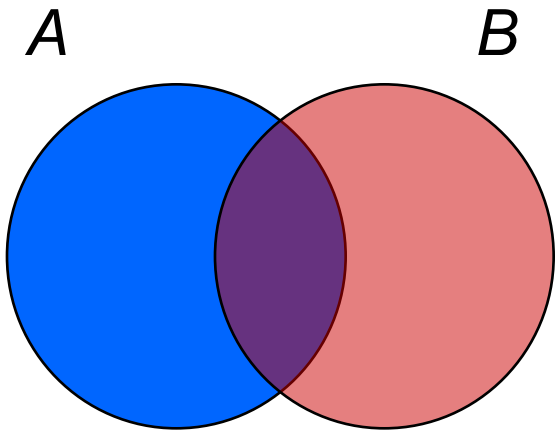



What if $A$ and $B$ are not disjoint?

# Inclusion-Exclusion (2 Sets)

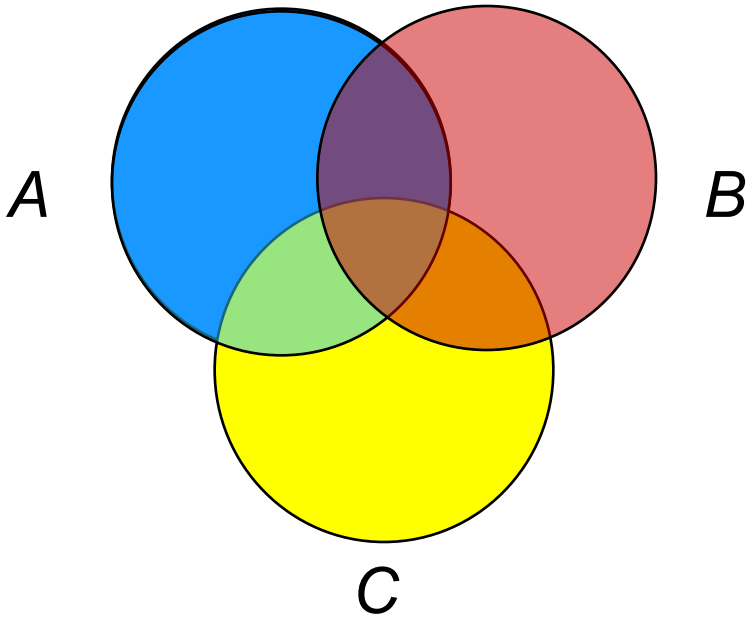
For two arbitrary sets $A$ and $B$

$$|A \cup B| = |A| + |B| - |A \cap B|$$



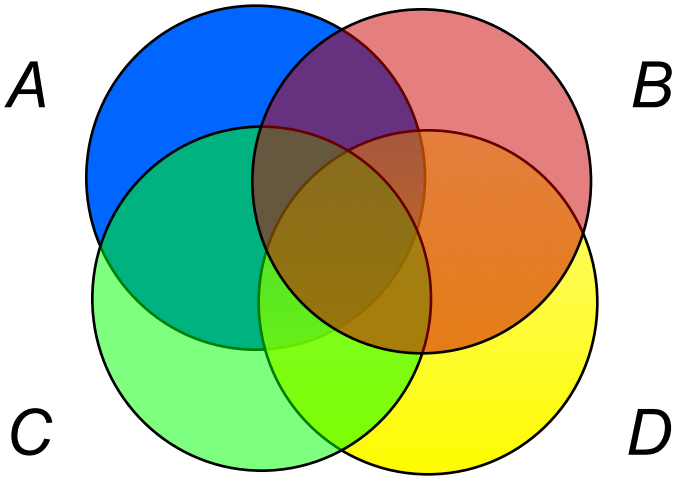
# Inclusion-Exclusion (3 Sets)

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$



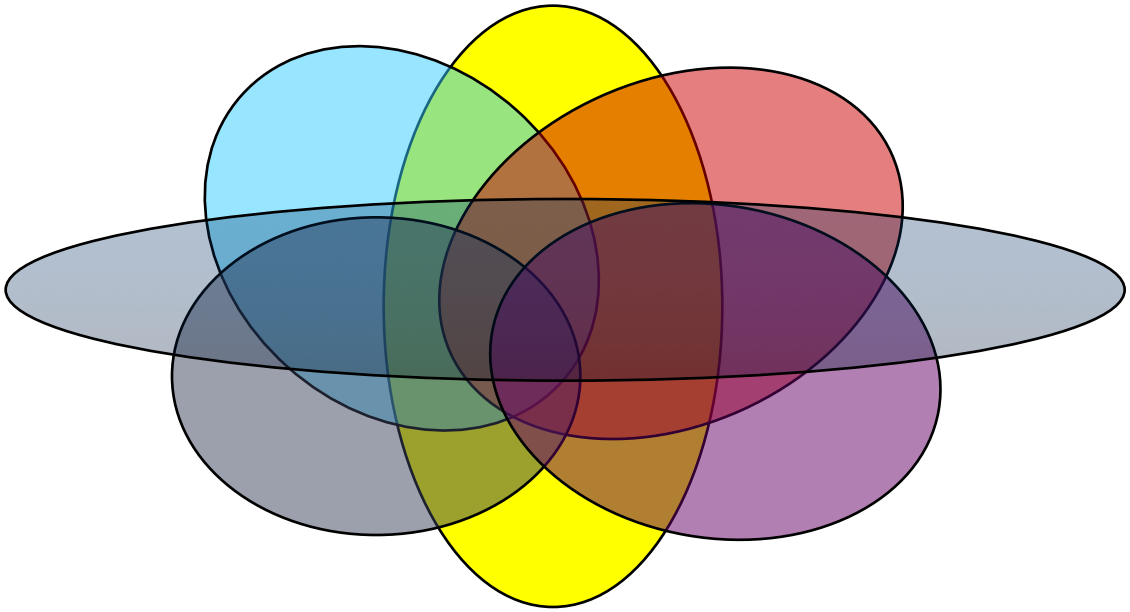
# Inclusion-Exclusion (4 Sets)

$$|A \cup B \cup C \cup D| = |A| + |B| + |C| + |D|$$
$$- |A \cap B| - |A \cap C| - |A \cap D| - |B \cap C| - |B \cap D| - |C \cap D|$$
$$+ |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D|$$
$$- |A \cap B \cap C \cap D|$$



# Inclusion-Exclusion (n Sets)

What is the inclusion-exclusion formula for the union of n sets?



# Inclusion-Exclusion (n Sets)

$$\left|A_1 \cup A_2 \cup \quad \cup A_n\right| =$$

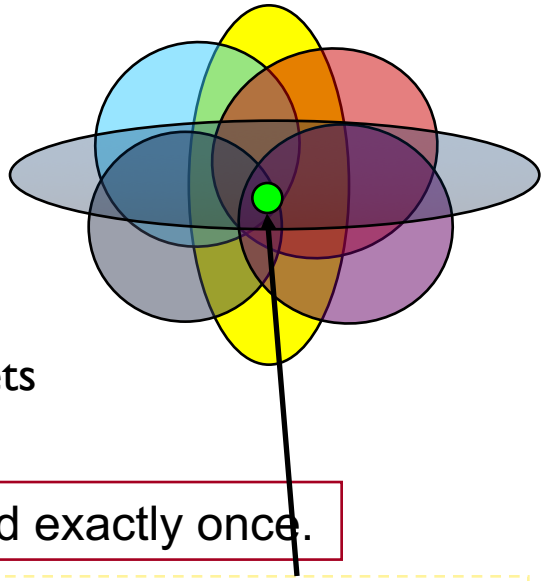
sum of sizes of all single sets
− sum of sizes of all 2-set intersections
+ sum of sizes of all 3-set intersections
− sum of sizes of all 4-set intersections
…
+ $(-1)^{n+1}$ × sum of sizes of intersections of all $n$ sets

$$= \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{S \subseteq \{1,2,\quad,n\} \\ |S|=k}} \left| \bigcap_{i \in S} A_i \right|$$

# Inclusion-Exclusion (n Sets)

$|A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n|$

sum of sizes of all single sets
– sum of sizes of all 2-set intersections
+ sum of sizes of all 3-set intersections
– sum of sizes of all 4-set intersections
…
+ $(-1)^{n+1} \times$ sum of sizes of intersections of all $n$ sets



We want to show that every element is counted exactly once.

Consider an element which belongs to exactly k sets, say $A_1$, $A_2$, $A_3$, …, $A_k$.

In the formula, such an element is counted the following number of times:

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} + \ldots + (-1)^{k+1}\binom{k}{k} = 1$$

Therefore each element is counted exactly once, and thus the formula is correct

# Inclusion-Exclusion (n Sets)

$$\binom{k}{1} - \binom{k}{2} + \binom{k}{3} - \binom{k}{4} + \ldots + (-1)^{k+1}\binom{k}{k} = 1$$

$$(x+y)^k = \sum_{k=0}^{n} \binom{k}{i} x^i y^{k-i}$$

Plug in x=1 and y=-1 in the above binomial theorem, we have

$$0 = \binom{k}{0} - \binom{k}{1} + \binom{k}{2} + \ldots + (-1)^i \binom{k}{i} + \ldots + (-1)^k \binom{k}{k}$$

$$\Rightarrow \quad \binom{k}{1} - \binom{k}{2} + \ldots + (-1)^{i+1}\binom{k}{i} + \ldots + (-1)^{k+1}\binom{k}{k} = \binom{k}{0} = 1$$

# Christmas Party

In a Christmas party, everyone brings his/her present.
There are n people and so there are totally n presents.
Suppose the host collects and shuffles all the presents.
Now everyone picks a random present.
What is the probability that no one picks his/her own present?

Let the n presents be {1, 2, 3, …, n}, where the present i is owned by person i.
Now a random ordering of the presents means a permutation of {1, 2, 3, …, n}.

e.g. (3,2,1) means the person 1 picks present 3, person 2 picks present 2, etc.

And the question whether someone picks his/her own present becomes

**whether there is a number i which is in position i of the permutation.**

# Fixed Points in a Permutation

Given a random permutation of {1, 2, 3, …, n},
what is the probability that a permutation has no fixed point
(i.e number i is not in position i for all i)?

e.g. {2, 3, 1, 5, 6, 4} has no fixed point,
{3, 4, 7, 5, 2, **6**, 1} has a fixed point,
{5, 4, **3**, 2, 1} has a fixed point.

You may wonder why we are suddenly asking a probability question.
Actually, this is equivalent to the following counting question:

What is the number of permutations of {1,2,3,…,n} with no fixed point?

# Fixed Points in a Permutation

What is the number of permutations of {1,2,3,…,n} with no fixed point?

For this question, it is more convenient to count the complement.

Let S be the set of permutations of {1,2,3…,n} with some fixed point(s).

Let $A_1$ be the set of permutations in which the number 1 is in position 1.
…
Let $A_j$ be the set of permutations in which the number j is in position j.
…
Let $A_n$ be the set of permutations in which the number n is in position n.

$S = A_1 \cup A_2 \cup \ldots \cup A_n$

Note that $A_i$ and $A_j$ are not disjoint, and so we need inclusion-exclusion.

# Fixed Points in a Permutation

Let S be the set of permutations of {1,2,3…,n} with some fixed point(s).

Let $A_j$ be the set of permutations in which the number j is in position j.

$$S = A_1 \cup A_2 \cup \ldots \cup A_n$$

How large is $|A_j|$?

Once we fixed j, we can have any permutation on the remaining n-1 elements.

Therefore, $|A_j| = (n-1)!$

How large is $|A_i \cap A_j|$?

Once we fixed i and j, we can have any permutation on the remaining n-2 elements.

Therefore, $|A_i \cap A_j| = (n-2)!$

# Fixed Points in a Permutation

Let S be the set of permutations of {1,2,3…,n} with some fixed point(s).

Let $A_j$ be the set of permutations in which the number j is in position j.

$$S = A_1 \cup A_2 \cup \ldots \cup A_n$$

How large is the intersection of k sets?

In the intersection of k sets, there are k positions being fixed.

Then we can have any permutation on the remaining n-k elements.

Therefore, |the intersection of k sets| = (n-k)!

# Fixed Points in a Permutation

Let S be the set of permutations of {1,2,3…,n} with some fixed point(s).

Let $A_j$ be the set of permutations in which the number j is in position j.

$$S = A_1 \cup A_2 \cup \ldots \cup A_n$$

|the intersection of k sets| = (n-k)!

$$|S| = |A_1 \cup A_2 \cup \ldots \cup A_n|$$
$$= \binom{n}{1}(n-1)!$$
$$-\binom{n}{2}(n-2)!$$
$$+\binom{n}{3}(n-3)!$$
$$\cdots$$
$$+(-1)^{n+1}\binom{n}{n}(n-n)!$$

$|A_1 \cup A_2 \cup A_3 \cup \ldots \cup A_n|$

sum of sizes of all single sets
– sum of sizes of all 2-set intersections
\+ sum of sizes of all 3-set intersections
– sum of sizes of all 4-set intersections
…
\+ $(-1)^{n+1}$ × sum of sizes of intersections of *n* sets

# Fixed Points in a Permutation

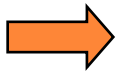
Let S be the set of permutations of {1,2,3…,n} with some fixed point(s).

Let $A_j$ be the set of permutations in which the number j is in position j.

$S = A_1 \cup A_2 \cup \ldots \cup A_n$

|the intersection of k sets| = (n-k)!

$$|S| = |A_1 \cup A_2 \cup \ldots \cup A_n|$$
$$= \binom{n}{1}(n-1)!$$
$$-\binom{n}{2}(n-2)!$$
$$+\binom{n}{3}(n-3)!$$
$$\ldots$$
$$+(-1)^{n+1}\binom{n}{n}(n-n)!$$



$$|S| = |A_1 \cup A_2 \cup \ldots \cup A_n|$$
$$= n! - n!/2! + n!/3! + \ldots (-1)^{i+1}\, n!/i! + \ldots + (-1)^{n+1}$$

# Fixed Points in a Permutation

Let S be the set of permutations of {1,2,3…,n} with some fixed point(s).

Let $A_j$ be the set of permutations in which the number j is in position j.

$$S = A_1 \cup A_2 \cup \ldots \cup A_n$$

$$|S| = n! - n!/2! + n!/3! + \ldots (-1)^{i+1}\, n!/i! + \ldots + (-1)^{n+1}$$

The number of permutations with no fixed points

$= n! - |S|$

$= n! - n! + n!/2! - n!/3! + \ldots (-1)^{i}\, n!/i! + \ldots + (-1)^{n}$

$= n!\,(1 - 1/1! + 1/2! - 1/3! + \ldots + (-1)^{i}\, 1/i! \ldots + (-1)^{n}\, 1/n!)$

-> n!/e (where e is the constant 2.71828…)

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = \sum_{n} \frac{x^n}{n!}$$

# Outline

- Inclusion-exclusion Principle
- **Review on Modular Exponentiation Algorithm**

# Binary Modular Exponentiation

- In general, to to compute $b^n$ we may use the binary expansion of $n$, $n = (a_{k-1},\ldots,a_1,a_0)_2$ . Than

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \ldots b^{a_1\cdot 2} \cdot b^{a_0}.$$

- Therefore, to compute $b^n$, we need only compute the values of $b$, $b^2$, $(b^2)^2 = b^4$, $(b^4)^2 = b^8$ , …, and the multiply the terms $b^{2^j}$ in this list, where $a_j = 1$.

$O((\log m)^2 \log n)$ bit operations are used to find $b^n$ mod $m$.

# Practice: $175^{235}$ mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j*** ***8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175$
- d: records the temporal result, starting from the rightmost factor.
- t: represents the next term $b^{2^j}$ where b = 175 in this example.

- j = 1, **$175 \bmod 257 = 175$**
  **$175^2 \bmod 257 = 42$**
  **d ← 175, t ← 42.**

# Practice: $175^{235} \bmod 257$

- $235 = 128 + 64 + 32 + 8 + 2 + 1 = (11101011)_2$.
- ***j  8  7  6  4  2  1  87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times \mathbf{175^2 \times 175}$

- j = 2, $175^2 \times 175 \bmod 257 = (175^2 \bmod 257) \times (175 \bmod 257) \bmod 257 = t \times d \bmod 257 = 42 \times 175 \bmod 257 = 154$
- $175^4 \bmod 257 = (175^2 \bmod 257)^2 \bmod 257$
- $= t \times t \bmod 257$
- $= 42 \times 42 \bmod 257 = 222$
- 
- **$d \leftarrow 175^2 \times 175 \bmod 257 = 154$**
- **$t \leftarrow 175^4 \bmod 257 = 222$**

# Practice: $175^{235}$ mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = (11101011)2.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times \mathbf{175^{2} \times 175}$

- j = 4, **no factor $175^{4}$.**
- $175^{8} \bmod 257 = (175^{4} \bmod 257)^{2} \bmod 257$
- $= t \times t \bmod 257$
- $= 222 \times 222 \bmod 257 = 197$
- 
- **d ← $175^{2} \times 175 \bmod 257 = 154$**
- **t ← $175^{8} \bmod 257 = 197$**

# Practice: $175^{235}$ mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times \mathbf{175^8 \times 175^2 \times 175}$

- j = 4, $\mathbf{175^8 \times 175^2 \times 175} \bmod 257 = (175^8 \bmod 257) \times (\mathbf{175^2 \times 175} \bmod 257) \bmod 257 = t \times d \bmod 257 = 197 \times 154 \bmod 257 = 12$
- $175^{16} \bmod 257 = (175^8 \bmod 257)^2 \bmod 257$
- $= t \times t \bmod 257$
- $= 197 \times 197 \bmod 257 = 2$
- **d ← $175^8 \times 175^2 \times 175$** mod 257 = 12
- **t ← $175^{16}$ mod 257 = 2**

# Practice: $175^{235}$ mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j  8  7  6  4  2  1  87654321***

- $175^{235} = 175^{128} \times 175^{64} \times 175^{32} \times \mathbf{175^8 \times 175^2 \times 175}$

- j = 5, no factor $\mathbf{175^{16}}$
- $175^{32}$ mod 257 = $(175^{16}$ mod 257$)^2$ mod 257
- = t x t mod 257
- = 2 x 2 mod 257 = 4
- **d ← $175^8$ x$175^2$ x175** mod 257 = 12
- **t ← $175^{32}$ mod 257 = 14**

# Practice: $175^{235}$ mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j  8  7  6  4  2  1  87654321***

- $175^{235} = 175^{128} \times 175^{64} \times \mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175}$

- j = 6, $\mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175}$ mod 257 = ($175^{32}$ mod 257) x ($\mathbf{175^{8} \times 175^{2} \times 175}$ mod 257) mod 257 = t x d mod 257 = 4 x 12 mod 257 = 48

- $175^{64}$ mod 257 = ($175^{32}$ mod 257)$^2$ mod 257
- = t x t mod 257
- = 4 x 4 mod 257 = 16
- **d ← $175^{32} \times 175^{8} \times 175^{2} \times 175$ mod 257 = 48**
- **t ← $175^{64}$ mod 257 = 16**

# Practice: $175^{235}$ mod 257

- 235 = 128 + 64 + 32 + 8 + 2 + 1 = $(11101011)_2$.
- ***j 8 7 6 4 2 1 87654321***

- $175^{235} = 175^{128} \times \mathbf{175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175}$

- j = 7, $\mathbf{175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175}$ mod 257 = ($175^{64}$ mod 257) x ($\mathbf{175^{32} \times 175^{8} \times 175^{2} \times 175}$ mod 257) mod 257 = t x d mod 257 = 16 x 48 mod 257 = 254

- $175^{128}$ mod 257 = ($175^{64}$ mod 257)$^2$ mod 257
- = t x t mod 257
- = 16 x 16 mod 257 = 256
- **d ← $175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175$ mod 257 = 48**
- **t ← $175^{128}$ mod 257 = 256**

# Practice: $175^{235} \bmod 257$

- $235 = 128 + 64 + 32 + 8 + 2 + 1 = (11101011)_2$.
- ***j  8  7  6  4  2  1  87654321***

- $175^{235} = \mathbf{175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175}$

- j = 8, $\mathbf{175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175} \bmod 257 = (175^{128} \bmod 257) \times (\mathbf{175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175} \bmod 257) \bmod 257 = t \times d \bmod 257 = 256 \times 254 \bmod 257 = 3$

- $175^{128} \bmod 257 = (175^{64} \bmod 257)^2 \bmod 257$
- $= t \times t \bmod 257$
- $= 16 \times 16 \bmod 257 = 256$
- **d ← $175^{128} \times 175^{64} \times 175^{32} \times 175^{8} \times 175^{2} \times 175 \bmod 257 = 3$**
- **return d.**

# Analysis on d and t (1)

- d = $175 \bmod 257$
- d = $175^2 \times 175 \bmod 257$
- d = $175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{64} \times 175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$
- d = $175^{128} \times 175^{64} \times 175^{32} \times 175^8 \times 175^2 \times 175 \bmod 257$

$d = t \times d \bmod 257$ when $t = \mathbf{175^k}$ **and** $\mathbf{k = 2^{j-1}}$

# Analysis on d and t (2)

- $t = 175^2 \bmod 257 = 42$
- $t = 175^4 \bmod 257 = (175^2 \bmod 257)^2 \bmod 257 = 222$
- $t = 175^8 \bmod 257 = (175^4 \bmod 257)^2 \bmod 257 = 197$
- $t = 175^{16} \bmod 257 = (175^8 \bmod 257)^2 \bmod 257 = 2$
- $t = 175^{32} \bmod 257 = (175^{16} \bmod 257)^2 \bmod 257 = 4$
- $t = 175^{64} \bmod 257 = (175^{32} \bmod 257)^2 \bmod 257 = 16$
- $t = 175^{128} \bmod 257 = (175^{64} \bmod 257)^2 \bmod 257 = 256$

$$t = t^2 \bmod 257$$

# Practice: $175^{235} \bmod 257$

- $235_{10} = 11101011_2$.
- *1*. d := 1 × 175 mod 257 = 175, t := $175^2$ mod 257 = 42;
- *2*. d := 175 × 42 mod 257 = 154, t := $42^2$ mod 257 = 222;
- *3*. t := $222^2$ mod 257 = 197;
- *4*. d := 154 × 197 mod 257 = 12, t := $197^2$ mod 257 = 2;
- *5*. t := $2^2$ mod 257 = 4;
- *6*. d := 12 × 4 mod 257 = 48, t := $4^2$ mod 257 = 16;
- *7*. d := 48 × 16 mod 257 = 254, t := $16^2$ mod 257 = 256;
- *8*. d := 254 × 256 mod 257 = 3
- ***Return* d = 3**

# Next class

- Topic: Probability
- Pre-class reading: Chap 7.1