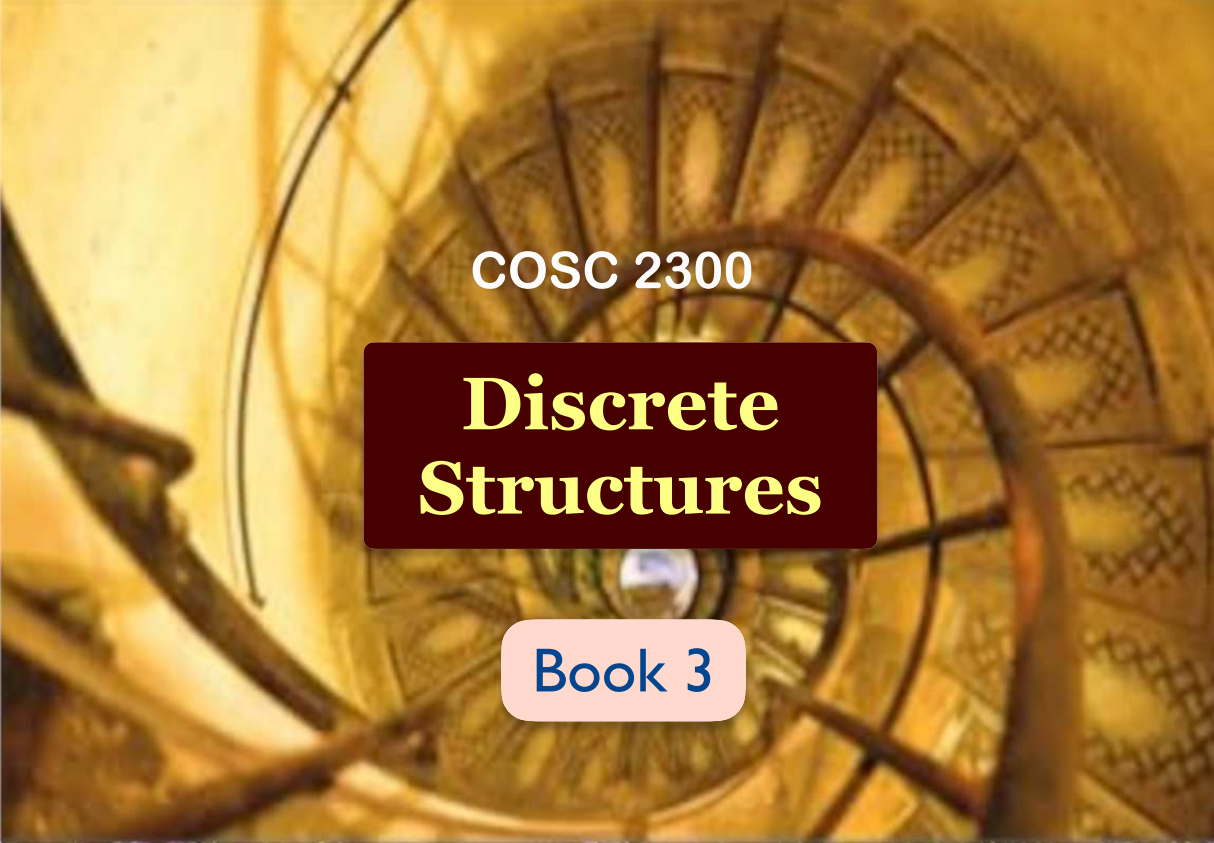

COSC 2300
Discrete Structures
Book 3

I want to give 19 identical silver dollars to five people.

Represent silver dollars by 19 *'s and separate them using 4 |'s eg. ***|*****|**||*********

Answer: $\binom{23}{19} = \binom{23}{4} = 8855$.

What if instead we require each of the five people to get at least one of the silver dollars?
First give out five silver dollars, one apiece, then $\binom{14+4}{4} = 3060$.

$\sum_{k=0}^{n} \binom{n}{k} = 2^n$ First proof: $(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k}$

Second proof: Count subsets of an n-set.

$1 - 6 + 15 - 20 + 15 - 6 + 1 = 0$

$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = \begin{cases} 0 & \text{for } n \geq 1 \\ 1 & \text{for } n = 0. \end{cases}$ Proof: Use $x=1$, $y=-1$ in the Binomial Theorem.

$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$

Eg. $n=3$. $1^2 + 3^2 + 3^2 + 1^2 = 20 = \binom{6}{3} = \frac{6\times5\times4}{3\times2\times1}$

If a, b are integers, we say c divides b if b is a multiple of c

(All variables here are integers)

$\Leftrightarrow$ $b = kc$ for some k

$\Leftrightarrow$ c is a divisor of b

$\Leftrightarrow$ $c \mid b$

The divisors of 12 are $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$. (There are 12 divisors of 12.)
The divisors of 30 are $\pm1, \pm2, \pm3, \pm5, \pm6, \pm10, \pm15, \pm30$. (There are 16 divisors of 30.)
The divisors of 7 are $\pm1, \pm7$. A number $p > 1$ is prime if its only positive divisors are 1 and p.
eg. 7 is prime; 1 is not.

The divisors of 12 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$.

The divisors of 30 are $\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$.

The common divisors of 12 and 30 are $\pm 1, \pm 2, \pm 3, \pm 6$. (There are 8 common divisors of 12 and 30.)

The greatest common divisor of 12 and 30 is 6: $\gcd(12, 30) = 6$.

Computing the gcd of two integers a, b is very practical and is much easier than factoring (if a, b are large).

$\gcd(12, 30) = \gcd(2^2 \cdot 3, 2 \cdot 3 \cdot 5) = 2 \cdot 3 = 6$.

This method is not practical for numbers that are hundreds of digits long.

Eg. $\gcd(124, 46) = \gcd(46, 32) = \gcd(32, 14) = \gcd(14, 4) = \gcd(4, 2) = \gcd(2, 0)$

$124 = 2 \times 46 + 32$
$46 = 1 \times 32 + 14$
$32 = 2 \times 14 + 4$
$14 = 3 \times 4 + 2$
$4 = 2 \times 2 + 0$

The last nonzero remainder here is $\gcd(124, 46) = 2$.

Divisors of 2: $\pm 1, \pm 2$

Divisors of 0: $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \cdots$ $\quad 0 = 0 \cdot 5$

Common divisors of 0 and 2: $\pm 1, \pm 2$

$\gcd(0, 2) = 2$.

This is Euclid's Algorithm for computing $\gcd(a, b)$.

It relies on repeated application of the Division Algorithm:

Given any integers n, d with $d \geq 1$, there exist unique q, r such that

$$n = qd + r, \quad r \in \{0, 1, 2, \cdots, d-1\}$$

(q is the quotient; r is the remainder.)

($r = n \bmod d$)

The extended form of Euclid's Algorithm does another thing that we need:

An integer linear combination of $a, b \in \mathbb{Z}$ is a number of the form $ra + sb$ where $r, s \in \mathbb{Z}$.

eg. an integer linear combination of 124 and 46 is any integer of the form $124r + 46s$ $(r, s \in \mathbb{Z})$.

These are precisely the multiples of $\gcd(124, 46) = 2$. To see this, we want to express $\gcd(a, b)$ as an integer linear combination of a and b.

Eg. $\gcd(124, 46) = \gcd(46, 32) = \gcd(32, 14) = \gcd(14, 4) = \gcd(4, 2) = \gcd(2, 0)$

$124 = 2 \times 46 + 32$
$46 = 1 \times 32 + 14$
$32 = 2 \times 14 + 4$
$14 = 3 \times 4 + 2$
$4 = 2 \times 2 + 0$

The last nonzero remainder here is $\gcd(124, 46) = 2$.

$2 = 14 - 3 \times 4$
$= 14 - 3 \times (32 - 2 \times 14)$
$= 7 \times 14 - 3 \times 32$
$= 7 \times (46 - 32) - 3 \times 32$
$= 7 \times 46 - 10 \times 32$
$= 7 \times 46 - 10 \times (124 - 2 \times 46)$
$= 27 \times 46 - 10 \times 124$. Check! (I did.)

Two integers a, b are relatively prime (coprime) if $\gcd(a, b) = 1$.
Two large integers are relatively prime about 61% of the time.
If $\gcd(b, n) = 1$ then we can find an inverse for b mod n is a number c such that $bc \bmod n = 1$.
There is a unique inverse for b mod n in this case.
If $\gcd(b, n) \neq 1$ then b doesn't have an inverse mod n.

eg. $n = 15$. Find the inverse of 11 mod 15. $11c \bmod 15 = 1$.

$4 \cdot 4 = 16$
$4 \cdot 4 \bmod 15 = 16 \bmod 15 = 1$.
$(-4)(-4) = 16$
$11 \cdot 11 \bmod 15 = 1$.
$121 \bmod 15 = 1$

$120 = 2^3 \cdot 3 \cdot 5$

Eg. Find the inverse of 7 mod 23
i.e. Solve for c: $7c \bmod 23 = 1$
$\gcd(7, 23) = 1 = 7r + 23s$ for some $r, s \in \mathbb{Z}$.

23	7	
1	0	23
0	1	7
1	-3	2
-3	10	1
7	-23	0

$\gcd(23, 7) = 1 = -3 \cdot 23 + 10 \cdot 7$.

Take this mod 23:
The inverse of 7 mod 23 is 10.

In integers mod p (p prime) everything except 0 mod p has an inverse.

a	a^{-1} mod 7
0	does not exist
1	1
2	4
3	5
4	2
5	3
6	6

$\phi(7) = 6$.

If p is prime, then $\phi(p) = p-1$.

In the integers mod 15, eight of them are relatively prime to 15 and so these have inverses:

a	a^{-1} mod 15
0	Does not exist
1	1
2	8
3	Does not exist
4	4
5	Does not exist
6	DNE
7	13
8	2
9	DNE
10	DNE
11	11
12	DNE
13	7
14	14

$\phi(15) = 8$

If $n = pq$ where p and q are distinct primes, then

$\gcd(0, n) = n$ (only one integer x mod n has $\gcd(x, n) = n$)

the integers x mod n satisfying $\gcd(x, n) = p$ are exactly

$x \in \{p, 2p, 3p, \cdots, (q-1)p\}$ ($q-1$ of them)

the integers x mod n satisfying $\gcd(x, n) = q$ are

$x \in \{q, 2q, 3q, \cdots, (p-1)q\}$ ($p-1$ of them).

How many integers x mod n have $\gcd(x, n) = 1$? $n - (p-1) - (q-1) - 1 = pq - p - q + 1 = (p-1)(q-1)$

If n is any positive integer, $\phi(n)$ is the number of elements of $\{1, 2, \cdots, n\}$ that are relatively prime to n (equivalently, it's the number of integers mod n that have inverses mod n).

$\phi(p)\ \phi(q)$

$\phi(ab) = \phi(a)\phi(b)$ whenever $\gcd(a, b) = 1$.

eg. $\phi(15) = \phi(3)\phi(5) = 2 \cdot 4 = 8$.

$\phi(9) \neq \phi(3)\phi(3)$

6 $\quad$ $2 \cdot 2 = 4$

For every integer x, $x^p \bmod p = x \bmod p$. (p prime)

for every integer $x \bmod p \neq 0$ (x not divisible by p),

$$x^{p-1} \bmod p = 1.$$

eg. $p=7$:

x	x^2	x^3	x^4	x^5	x^6	x^7	x^8	mod 7
0	0	0	0	0	0	0	0	...
1	1	1	1	1	1	1	1	...
2	4	1	2	4	1	2	4	...
3	2	6	4	5	1	3	2	...
4	2	1	4	2	1	4	2	...
5	4	6	2	3	1	5	4	...
6	1	6	1	6	1	6	1	...