

Given two integers  $a$  and  $b$ , the  
greatest common divisor of  $a$  and  $b$

$$\gcd(a, b)$$

is a divisor of  $a$  and a divisor of  $b$  and  
it's the largest such integer.

Well defined concept :

- 1 is a common divisor, so there is one
- Common divisor  $\leq \min(a, b)$ , so there must be a largest.

Example  $a = 300$   $b = 18$  what is  $\gcd(300, 18)$

List divisors of 300 and 18 and check them

$$D_{300} = \{1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 25, 30, 50, 60, 75, 100, 150, 300\}$$

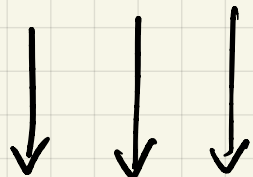
$$D_{18} = \{1, 2, 3, 6, 9, 18\}$$

Bad: Requires going through all numbers  $1, 2, 3, \dots, n = 300$

Example: Factor into primes

$$300 = 2^2 \cdot 3^1 \cdot 5^2$$

$$18 = 2^1 \cdot 3^2 \cdot 5^0$$



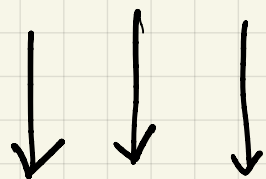
$$2^1 \cdot 3^1 \cdot 5^0 = 6$$

Pick the  
smallest  
power for  
each prime

Pick as many prime factors  
as possible to make the  
largest divisor of both

Bad: Not easy to factor into primes in general.

Side Remark: What if we pick the largest power for each prime?



$$2^2 \cdot 3^2 \cdot 5^2 = 900 = \text{lcm}(300, 18)$$

least common multiple.

Observation :  $\gcd(a, b) \times \text{lcm}(a, b) = a \times b$

Fact 1 :  $d \mid a \wedge d \mid b \iff d \mid \gcd(a, b)$

Fact 2 :  $a \mid m \wedge b \mid m \iff \text{lcm}(a, b) \mid m$

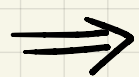
Here's what we will prove:

$$a = b \cdot q + r \quad 0 \leq r < b$$

└───┬───  
quotient      remainder of  $a/b$

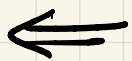
$$d \mid a \wedge d \mid b \iff d \mid b \wedge d \mid r$$

direction



$$\begin{array}{l} a = md \\ b = nd \end{array} \implies \begin{array}{l} md = nd \cdot q + r \\ r = d(m - nq) \implies d \mid r \end{array}$$

direction



: similar

Conclusion:  $\gcd(a, b) = \gcd(b, r)$

Euclid's Algorithm for finding  $\gcd(a, b)$  ( $a \geq b$ )

Construct sequence (decreasing)

$$\begin{array}{ccccccc} a_0 & a_1 & a_2 & \dots & a_k & & a_{k+1} \\ \hline & & & & & & \underbrace{\hspace{1cm}} \\ & & & & & & 0 \end{array}$$

$$a_{i-2} = a_{i-1} q_{i-1} + \underbrace{a_i}_{\text{remainder of } \frac{a_{i-2}}{a_{i-1}}}$$

then  $a_k = \gcd(a_0, a_1)$

Example:

300	18	12	6	0
			$\uparrow$	$\uparrow$
			$\gcd(300, 18)$	stop

Example: Find  $\gcd(100, 39)$

100

39

22

17

5

2

1

0

$\nearrow$   
 $\gcd(100, 39)$

$\uparrow$   
stop

In general:  $\gcd(a_0, a_1) = \gcd(a_1, a_2) = \dots = \gcd(a_{k-1}, a_k)$

but  $a_k \mid a_{k-1}$

So  $a_k = \gcd(a_{k-1}, a_k)$

Why is this good? It's fast.

Why is it fast?

$a_0 \quad a_1 \quad a_2 \quad \dots \quad a_{i-2} \quad a_{i-1} \quad a_i \quad \dots \quad a_k \quad \underbrace{a_{k+1}}_0$

$$a_{i-2} = a_{i-1} \cdot q_{i-1} + a_i \quad (q_{i-1} \geq 1)$$

$$\geq a_{i-1} + a_i \quad (a_i < a_{i-1})$$

$$> a_i + a_i = 2a_i$$

$$a_i < \frac{a_{i-2}}{2}$$

We can half  $a_0$   $\lfloor \log_2 a_0 \rfloor$  times before getting to 1

so  $k$  is logarithmic in  $a_0$ .



# The extended Euclidean Alg

$$a_0 \quad a_1 \quad a_2 \quad \dots \quad a_{i-2} \quad a_{i-1} \quad a_i \quad \dots \quad a_k \quad \overbrace{a_{k+1}}^0$$

Claim:  $\forall i, a_i = a_0 x_i + a_1 y_i \quad x_i, y_i \in \mathbb{Z}$  (not uniquely)

"Every number in the sequence is a linear combination of the first two"

Example:       $\underbrace{300}_{a_0}$        $\underbrace{18}_{a_1}$       12      6      0

$$300 = a_0 \boxed{1} + a_1 \boxed{0}$$

$$18 = a_0 \boxed{0} + a_1 \boxed{1}$$

$$12 = a_0 \boxed{1} + a_1 \boxed{-16}$$

$$6 = a_0 \boxed{-1} + a_1 \boxed{17}$$

$$0 = a_0 \boxed{3} + a_1 \boxed{-50}$$

## Proof by induction:

Base case:  $a_0 = a_0 \times 1 + a_1 \times 0$   
 $a_1 = a_0 \times 0 + a_1 \times 1$

Inductive step:  $P(0), P(1), \dots, P(i)$  are true

Prove  $P(i+1)$  is true

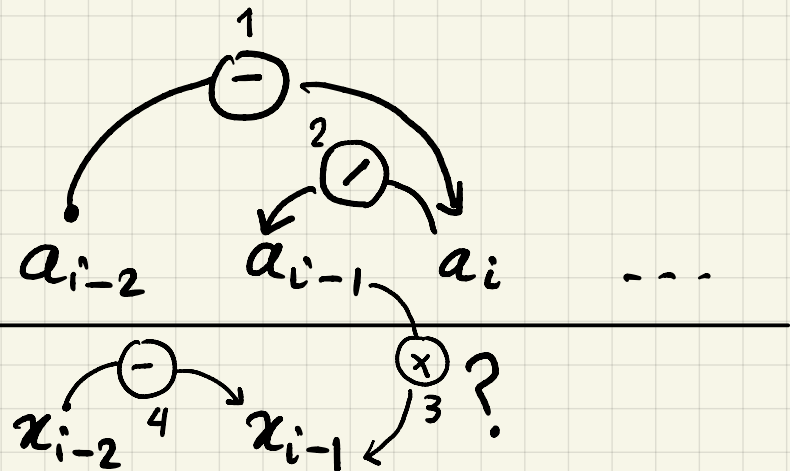
$$\begin{aligned} a_{i+1} &= \text{remainder of division } \frac{a_{i-1}}{a_i} \\ &= a_{i-1} - q_i a_i \\ &= (a_0 x_{i-1} + a_1 y_{i-1}) - q_i (a_0 x_i + a_1 y_i) \\ &= a_0 \left[ \underbrace{x_{i-1} - q_i x_i}_{x_{i+1}} \right] + a_1 \left[ \underbrace{y_{i-1} - q_i y_i}_{y_{i+1}} \right]. \end{aligned}$$

$$x_i = x_{i-2} - q_{i-1} x_{i-1}$$

$$= x_{i-2} - \frac{a_{i-2} - a_i}{a_{i-1}} x_{i-1}$$

Same formula for y

	$a_0$	$a_1$	...
$x$	1	0	
$y$	0	1	



Example:

	300	18	12	6	0
x	1	0	1	-1	3
y	0	1	-16	17	-50

$$\gcd(300, 18) = 6 = 300(-1) + 18(17)$$

Remember: Not unique!

Idea:  $ar + bs = a(r+b) + b(s-a)$

That's why we can always find

$$\gcd(a, b) = ar - bs \text{ where } r, s \geq 0$$