

# Number Theory

## Divisibility:

### Definition & Notation

1.  $a$  divides  $b$

2.  $a$  is a divisor of  $b$

3.  $b$  is a multiple of  $a$

$$\exists m \in \mathbb{Z}, b = ma \quad (\text{definition})$$

4.  $a \mid b$  (notation)

If  $a$  does not divide  $b$  ( $a \nmid b$ )

In general,

[unique representation]  $b = a \cdot q + r$  where  $0 \leq r < a$   
( $r=0 \Rightarrow a \mid b$ )

$q$ : quotient

$r$ : remainder,  $r \in \{0, 1, 2, \dots, a-1\}$

Prove uniqueness: (By contradiction)

Suppose  $b = aq_1 + r_1 = aq_2 + r_2$  ( $r_2 > r_1$ )

what can we say about  $r_2 - r_1$ ?

$$0 < r_2 - r_1 < a$$

$$r_2 = b - aq_2$$

$$r_1 = b - aq_1$$

$$\begin{aligned} r_2 - r_1 &= (b - aq_2) - (b - aq_1) \\ &= a(q_1 - q_2) \end{aligned}$$

Now,  $0 < a(q_1 - q_2) < a$

$0 < q_1 - q_2 < 1$ , a contradiction.

because there is no integer strictly between 0 and 1.

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

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

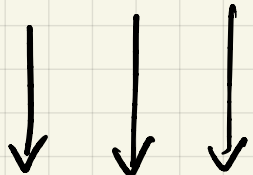
$$D_{18} = \{1, 2, 3, 6, 9, 18\}$$

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

Example: Factor into primes

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

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



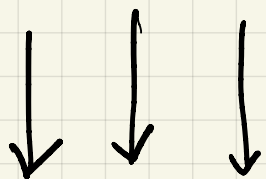
$$2^1 \cdot 3^1 \cdot 5^0 = 6$$

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.

Fact 1:  $\text{gcd}(a, b) \times \text{lcm}(a, b) = a \times b$

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

Fact 3:  $a \mid m \wedge b \mid m \iff \text{lcm}(a, b) \mid m$

The  $\Leftarrow$  direction is easy to prove in both cases.

- $d \mid \text{gcd}(a, b)$  and  $\text{gcd}(a, b) \mid a \Rightarrow d \mid a$   
(same for  $b$ )
- $m$  is mult. of  $\text{lcm}(a, b)$  and  $\text{lcm}(a, b)$  is mult. of  $a$   
 $\Rightarrow m$  is mult. of  $a$   
(same for  $b$ )

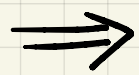
Here's what we will prove:

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

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

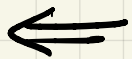
$$d \mid a \wedge d \mid b \iff d \mid b \wedge d \mid r$$

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





