Number Theory

Divisibility: Definition & Notation

1. a divides b
2. a is a divisor of b
3. b is a multiple of a

   $\exists\, m \in \mathbb{Z},\quad b = ma$ (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 $0 \leqslant r < a$

$(r=0 \Rightarrow a \mid b)$

q: quotient

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

Prove uniqueness: (By contradiction)

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

what can we say about $r_2 - r_1$?

$$0 < r_2 - r_1 < a$$

$$r_2 = b - aq_2$$

$$r_1 = b - aq_1$$

$$r_2 - r_1 = (b - aq_2) - (b - aq_1)$$

$$= a(q_1 - q_2)$$

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 <u>greatest common divisor</u> 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 $1, 2, 3, \ldots, n = 300$

Example: Factor into primes

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

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

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

Pick the smallest power for each prime

$$\downarrow \quad \downarrow \quad \downarrow$$

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

Bad: Not easy to factor into primes in general.

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

$$\downarrow \quad \downarrow \quad \downarrow$$

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

least Common Multiple.

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

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

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

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

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

Here's what we will prove :

$$a = \underbrace{b \cdot q}_{\text{quotient}} + r \qquad 0 \leqslant r < b$$

$r \rightarrow$ remainder of a/b

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

direction $\Longrightarrow$: $a = md$, $b = nd$ $\Longrightarrow$ $md = nd \cdot q + r$

$$r = d(m - nq) \Rightarrow d \mid r$$

direction $\Longleftarrow$: similar

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

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

Construct sequence (decreasing)

$$\underbrace{a_0 \quad a_1}_{a \quad b} \quad a_2 \quad \cdots\cdots \quad a_k \quad \underbrace{a_{k+1}}_{0}$$

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

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

Example: 300 18 12 6 0

$6 \uparrow$ gcd(300, 18)

$0 \uparrow$ stop

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

$$100 \quad 39 \quad 22 \quad 17 \quad 5 \quad 2 \quad 1 \quad 0$$

$\uparrow$ $\gcd(100,39)$ $\quad$ $\uparrow$ stop

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

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

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

Euclidean Algorithm

Why is this good? It's fast.