Notation

$\mathbb{N}$: natural numbers $\{1, 2, 3, \dots\}$

$\mathbb{N}_0$: $\mathbb{N} \cup \{0\}$

$\mathbb{Z}$: integers $\{\dots, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{Q}$: rational numbers $\left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$

$\mathbb{R}$: real numbers

$\mathbb{C}$: complex numbers

$\mathbb{P}$: prime numbers

2 basic principles (used in number theory proofs)

1. Well-ordering

Any non-empty set of positive integers contains a least element.

2. Induction

$S \subseteq \mathbb{Z}^+$. If $1 \in S$ and $n+1 \in S$ whenever $n \in S$ then $\mathbb{Z}^+ \subseteq S$ i.e., $S = \mathbb{Z}^+$.

(Def.) **Divisibility**: $a, b \in \mathbb{Z}$, $a \neq 0$.

b is divisible by a if $\exists\, x \in \mathbb{Z}$ s.t. $b = ax$

x: cofactor of a in b.

$a \mid b$

$a \nmid b$: a does not divide b

Properties

1. $a \mid 0 \quad \forall\, a \in \mathbb{Z}$
2. $a \mid b \Rightarrow |a| \leq |b|$
3. $a \mid b$ and $b \mid c \Rightarrow a \mid c$
4. $a \mid b$ and $a \mid c \Rightarrow a \mid (bx + cy) \quad \forall\, x, y \in \mathbb{Z}$

$b = ka \quad c = la \quad k, l \in \mathbb{Z} \quad bx + cy = (bk + cl)a \Rightarrow a \mid bx + cy$

5. $a|b$ & $b|a \Rightarrow a = \pm b$

6. $a|b$, $a>0, b>0 \Rightarrow a \leq b$

7. If $m \neq 0$ & $a|b \Rightarrow am|bm$

(Defn) Greatest Common Divisor (GCD)

Let $a, b \in \mathbb{Z}$, both not zero. The greatest common divisor of a & b, denoted $\gcd(a,b)$, is the largest positive common divisor of both a & b.

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

$\gcd(a,0) = a$

$\gcd(0,0)$: undefined

-24: 1, 2, 3, 4, 6, 8, 12, 24

15: 1, 3, 5, 15

$\gcd(-24, 15) = 3$

a, b $O(|a|) = O(2^{\log|a|})$.

(Defn) $a, b \in \mathbb{Z}$ are co-prime or relatively prime if

$$\gcd(a,b) = 1$$

25: 1, 5, 25

36: 1, 2, 3, 4, 6, 9, 18, 36

25, 36 are coprime

(Defn) Euclidean Division

For $a, b \in \mathbb{Z}$ with $b \neq 0$, $\exists$ unique $q, r \in \mathbb{Z}$

s.t. $a = qb + r$ and $0 \leq r < |b| - 1$

q: quotient, a quot b

r: remainder, a rem b

Euclid's Theorem

$a, b \in \mathbb{Z}, \quad b \neq 0$

$$\gcd(a,b) = \gcd(b, a \text{ rem } b)$$

Proof: $a = bq + r$

Let $d = \gcd(a,b)$ & $d' = \gcd(b,r)$

$d \mid a$, $d \mid b \Rightarrow d \mid a - bq \Rightarrow d \mid r$

$\Rightarrow d \leq d'$ ①

$d' \mid b$, $d' \mid r \Rightarrow d' \mid bq + r \Rightarrow d' \mid a$

$\Rightarrow d'' \leq d$ ②

① & ② $\Rightarrow d' = d$

Algorithm GCD(a, b)

i/p: integers a, b

o/p: $\gcd(a, b)$

```
if a = 0 and b = 0
    return 0;

if a < 0, a ← -a;
if b < 0, b ← -b;
while b ≠ 0 do
    r ← a rem b;
    a ← b;
    b ← r;
end while
return a;
```

Compute a sequence of remainders

$r_0, r_1, r_2, \ldots, r_k$

$r_0 = a, \quad r_1 = b$

$r_0 = q_2 r_1 + r_2$

$r_1 = q_3 r_2 + r_3$

$r_2 = q_4 r_3 + r_4$

$\vdots$

$r_{i-2} = q_i r_{i-1} + r_i$

$\vdots$

$r_{k-1} = q_{k+1} r_k \quad (r_{k+1} = 0)$

From Euclid's thm

$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2)$

$= \gcd(r_2, r_3) = \cdots = \gcd(r_{k-1}, r_k)$

$= \gcd(r_k, r_{k+1}) = \gcd(r_k, 0) = r_k$

Running time of GCD $= O(\log_2 \min(a,b))$

$$r_1 > r_2 > r_3 > \cdots > r_{k-1} > r_k$$

Assume $a > b$. Then $r_1 = b$.

No. of iterations $\leq b$

$r_{i-1} > r_i$ for all $i \geq 1$

$q_i \geq 1$ for all $i \geq 2$

$$r_{i-2} = q_i r_{i-1} + r_i \geq r_{i-1} + r_i > 2 r_i$$

$$\Rightarrow r_i < \frac{r_{i-2}}{2}$$

i.e., in 2 iterations, remainder reduces by at least a factor of 2

No. of iterations $= O(\log_2 b)$

(Thm) **Bézout's relation**: For $a, b \in \mathbb{Z}$, not both 0, $\exists u, v \in \mathbb{Z}$ satisfying $\gcd(a,b) = ua + vb$. Also, $\gcd(a,b)$ is the smallest positive linear combination of a, b.

Proof: $S = \{ xa + yb : x, y \in \mathbb{Z} \}$

$S \cap \mathbb{Z}^+$: non-empty $\Rightarrow$ hence has a least element

$c = ua + vb$. $(c \le z \quad \forall z \in S \cap \mathbb{Z}^+)$

Let $d = \gcd(a,b)$

$d|a, d|b \Rightarrow d|ua+vb \Rightarrow d|c \Rightarrow d \le c$

$c|a$: suppose $c \nmid a$. $a = qc + r$, $0 < r < c$

$r = a - qc = a - q(ua+vb) = a(\underbrace{1-qu}_{\in\mathbb{Z}}) + b(\underbrace{-qv}_{\in\mathbb{Z}}) \Rightarrow r \in S$

contradicts the choice of c as the least element!

III^{ly} $c|b \Rightarrow c \le d$

$d \le c, c \le d \Rightarrow c = d$

Extended GCD

Computes u, v along with $\gcd(a, b)$

Remainder sequence: $r_0, r_1, r_2, \ldots$

2 additional sequences: $u_0, u_1, u_2, \ldots$

$v_0, v_1, v_2, \ldots$

so that $\boxed{r_i = u_i a + v_i b}$ for all $i \geq 0$

$$r_{i-2} = q_i r_{i-1} + r_i$$

$$r_i = r_{i-2} - q_i r_{i-1} \qquad u_i = u_{i-2} - q_i u_{i-1} \qquad v_i = v_{i-2} - q_i v_{i-1}$$

$$r_0 = a, \; r_1 = b \qquad u_0 = 1, \; u_1 = 0 \qquad v_0 = 0, \; v_1 = 1$$

$$r_i = r_{i-2} - q_i(r_{i-1}) = (u_{i-2} - q_i u_{i-1})a + (v_{i-2} - q_i v_{i-1})b$$

$$= u_i a + v_i b$$

Algorithm Extended GCD

Running time: $O(\log_2 \min(a,b))$

i/p : a, b

o/p : u, v, d s.t. $d = \gcd(a,b) = ua + vb$

if $a = 0$ and $b = 0$, return $(0,0,0)$;

if $a < 0$, $a \leftarrow -a$; if $b < 0$, $b \leftarrow -b$;

$u_0 \leftarrow 1$; $u_1 \leftarrow 0$; $r_0 \leftarrow a$; $r_1 \leftarrow b$;

while $r_1 \neq 0$ do

$q \leftarrow r_0 / r_1$;

$r_2 \leftarrow r_0 - q r_1$; $r_0 \leftarrow r_1$; $r_1 \leftarrow r_2$;

$u_2 \leftarrow u_0 - q u_1$; $u_0 \leftarrow u_1$; $u_1 \leftarrow u_2$;

end while;

$u \leftarrow u_2$; if $a < 0$ $u \leftarrow -u$

if $b = 0$, $v \leftarrow 0$; else $v \leftarrow (r_0 - ua)/b$; return (u, v, r_0)