Jan 28, 2025 101

n-bit string (x) ⟶ x y

100111010001

$|x|$ → number corresponding to x.

Las Vegas
Monte Carlo

$p_1 - p_k$ → primes $\leq n^2$

$h_i = |x| \bmod p_i$

$(h_1 - h_k)$ ⟶ $h_1 - h_k$
$p_1 \quad p_k$ $\quad p_1 \quad p_k$

$h_i' = |y| \bmod p_i$

claim that $x \equiv y$ if $h_i' = h_i \ \forall i = 1, \ldots k$.

$a \bmod m = b \bmod m \qquad a \neq b$

$m \mid (a-b)$

$|y| \bmod p_i = |x| \bmod p_i \ \forall i$

$\Rightarrow (|x| - |y|) \bmod p_i = 0 \quad \forall i$

$p_i \mid (|x| - |y|)$.

① # of prime divisors of a number m.

$m = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$

$\geq 2^{\alpha_1} \cdots 2^{\alpha_t}$

$\geq 2 \cdot \cdots 2 \ (t\text{-times}) = 2^t$

$t \leq \log_2 m$

$p \quad \Pr(p_i \mid (|x|-|y|)) \leq \left(\frac{\#\text{ primes divisors of } |x|-|y|}{\#\text{ primes} \leq n^2}\right)$

p^K

Prime Number Theorem $\quad \#\text{primes} \leq m \approx \frac{m}{\log m}$

$$\#\text{primes} \leq n^2 \approx \frac{n^2}{2\log n}$$

$$p \leq \frac{2 \cdot 2\log n}{n^2} = \frac{2\log n}{n} \qquad 10^{-5}$$

$n \approx 10^6$

$\frac{5}{11111}$

$\frac{101}{1}$

$f(n) \rightarrow$ size of the input

All Number theoretic algorithms must work in $O(\text{poly-}\log n)$

$(b_{k+1} \ldots b_0)$ is base B log.

$\sum_{i=0}^{k+1} b_i B^i \neq$

$b_{k+1} \ldots b_0$

$\sum_{i=0}^{k+1} b_i \cdot 2^i$

3464-bit

$$\begin{array}{r} 534 \\ \times\ 236 \\ \hline 3204 \\ 02 \end{array}$$

GCD

Euclid's Algorithm

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

$a \geq b$.

$a = r_0$

$b = r_1$

$r_0 = q_0 r_1 + r_2$ — $r_2 < r_1$ — $r_0 \bmod r_1$

$r_1 = q_1 r_2 + r_3$ — $r_3 < r_2$ — $r_1 \bmod r_2$

$r_2 = q_2 r_3 + r_4$ — $r_4 < r_3$ — $r_2 \bmod r_3$

$\vdots$

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

$q_1 = q_2 = \cdots = q_{k+1} = 1$

$k-1 \leq \frac{\log r_1}{\log \phi}$ $\quad \phi = \frac{1+\sqrt{5}}{2}$

Jan 30, 2025

$a, b \geq 1$.

$1 \geq \frac{1+\sqrt{5}}{2}$

$f_k b \geq \phi^{k+1}$

$a = f_{k+1}$

$b = f_k$

$f_{k+1} = q_k f_k + f_{k-1}$

$f_k = q_{k-1} f_{k-1} + f_{k-2}$

$\vdots$

$f_1 = q_0 f_0 \geq 1$

$f_1 \geq 1$

$f_k \geq f_{k-1} + f_{k-2}$

$\geq \phi^{k-2} + \phi^{k-3}$

$= \phi^{k-3}(\phi + 1)$

$= \phi^{k-3} \cdot \phi^2$

$= \phi^{k-1}$

$a = \phi \cdot b$

$1 \geq \left(\frac{1+\sqrt{5}}{2}\right)^{-1}$

$\phi^{-1} = \frac{1}{\frac{1+\sqrt{5}}{2}}$

$\phi = \frac{1+\sqrt{5}}{2}$

$\phi^2 = \frac{1+5+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1+\phi$

$b \geq \phi^{k+1}$

$\Rightarrow (k+1)\log\phi \leq \log b$

$k \leq \frac{\log b}{\log \phi} + 1$

$\frac{1+\sqrt{5}}{2}$

$\lfloor x \rfloor$ unique integer m : $m \le x < m+1$ $\quad \|a\| = \lfloor \log_B a \rfloor + 1$

$\lceil x \rceil$ unique int. m : $m-1 < x \le m$

$a \le B^{\|a\|} - 1$

a — $\text{len}(a)$ $\quad \|a\| = \lfloor \log_B a \rfloor + 1$ $\quad \log_B(a+1) \le \|a\|$

a, b	len( )	time to compute
$a+b$	$\max(\|a\|, \|b\|) \le \ell \le \max(\|a\|, \|b\|)+1$	

$\underbrace{1111111111}_{t}$ $\to 2^t - 1$

$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$

$\|a\| = \lfloor \log_B a \rfloor + 1$

$a \geq B^{\|a\|-1}$

$\|a\| \leq \log_B a + 1$

$\|a\| - 1 \leq \log_B a < \|a\|$

$a = \sum_{i=0}^{\|a\|-1} a_i B^i$

$a_{\|a\|-1} \neq 0$

$a_0 = 1$

$a_{i,i>0} = 0$

$a = B^{\|a\|-1} \cdot a_{\|a\|-1} + B^{\|a\|-2} \cdot a_{\|a\|-2} + \cdots + B^0 \cdot a_0$

$a \geq B^{\|a\|-1}$

$\Rightarrow \log_B a \geq \|a\| - 1$

$\Rightarrow \|a\| - 1 \leq \log_B a < \|a\|$

$\|a\| = \lfloor \log_B a \rfloor + 1$

$B^{\|a\|-1}(B-1) + \cdots + B^0(B-1)$

$= (B-1)(\underbrace{1 + 1 + 1 + \cdots + 1}_{\|a\|})$

$= (B-1)\left(\underbrace{1 + B + B^2 + \cdots + B^{\|a\|-1}}_{\frac{B^{\|a\|}-1}{B-1}}\right)$

$a < B^{\|a\|}$

$\log_B a < \|a\|$

$\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$ (unique)

$\text{len}(a) = \lfloor \log_B a \rfloor + 1$

l

$a = \sum_{i=0}^{l-1} a_i B^i$ $\quad a_{l-1} \neq 0$

$\Rightarrow a \geq B^{l-1} \Rightarrow \log_B a \geq l-1$

$l = \|a\|$

$l - 1 \le \log_B a$

$a = \sum_{i=0}^{l-1} a_i B^i$

$\le (B-1) \sum_{i=0}^{l-1} B^i = (B-1)\frac{B^l - 1}{B-1}$

$a < B^l - 1 \Rightarrow a < B^l$

$\Rightarrow \log_B a < l$

$l - 1 \le \log_B a < l$

$\Rightarrow l - 1 = \lfloor \log_B a \rfloor$

$\|a\| = \lfloor \log_B a \rfloor + 1$

$\| a + b \|$ $\quad \max(\|a\|, \|b\|) \le \|a+b\| \le \max(\|a\|, \|b\|) + 1$

$\| a * b \|$ $\quad \ldots$

$\|a*b\|$

$\|a\| = \lfloor \log_B a \rfloor + 1$

$\|b\| = \lfloor \log_B b \rfloor + 1$

$\|a*b\| = \lfloor \log_B (a*b) \rfloor + 1$

$\lfloor \log_B (a*b) \rfloor \le \log_B a + \log_B B < \lfloor \log_B (a*b) \rfloor + 1$

$\log a + \log b$

$\le \lfloor \log_B (a*b) \rfloor \le \lfloor \log_B a \rfloor + \lfloor \log_B b \rfloor + 1$

$\|a\| + \|b\| - 2$

$\|a\| - 1 + \|b\|$

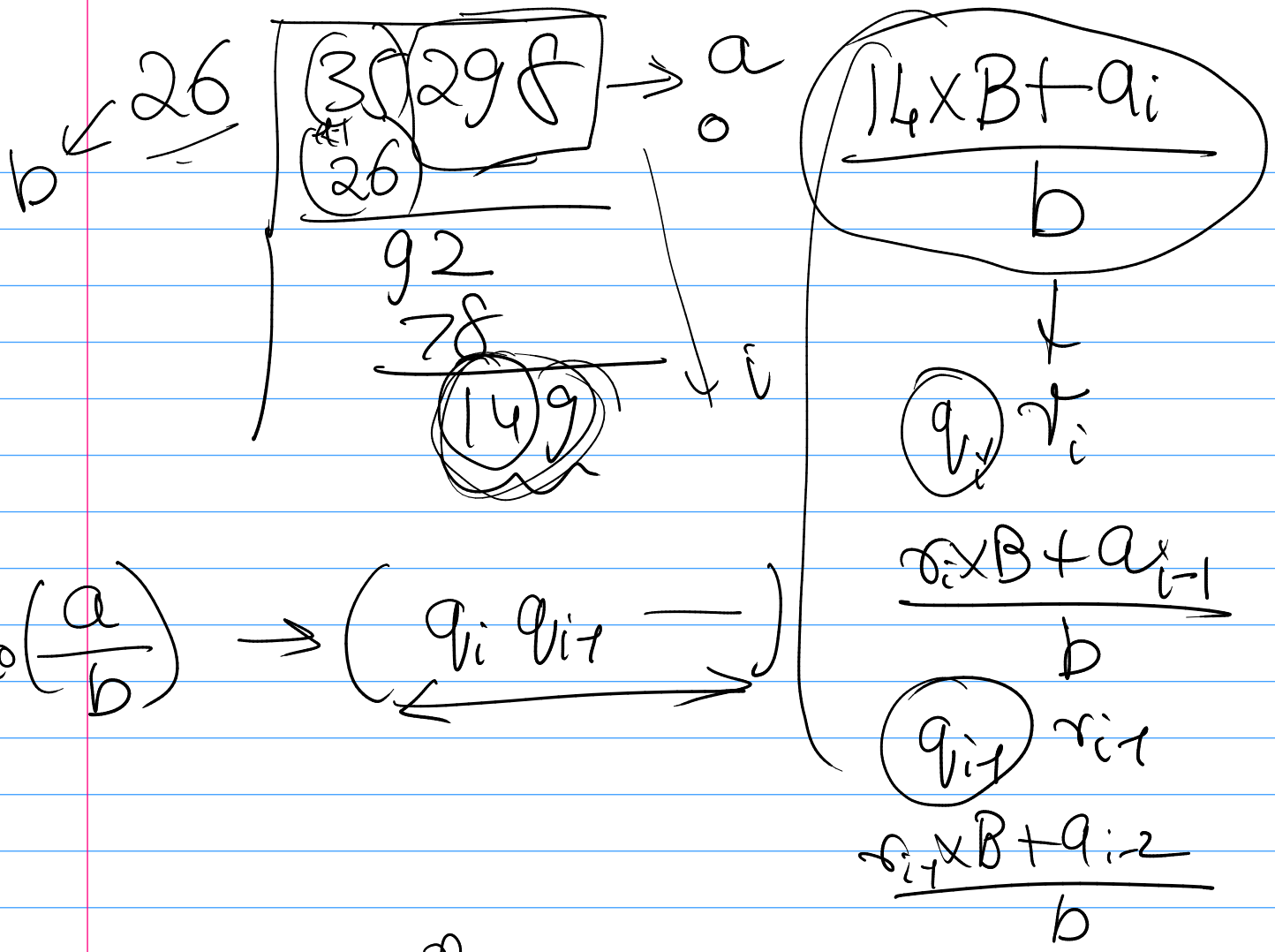
$\|a\| + \|b\| - 1 \le \|a*b\| \le \|a\| + \|b\|$

① $\max(\|a\|, \|b\|) \le \|a+b\| \le \max(\|a\|, \|b\|) + 1$

② $\|a\| + \|b\| - 1 \le \|a*b\| \le \|a\| + \|b\|$?

$\|a\| \quad \|b\| \quad (a/b)$

$\|a/b\| = \Theta(\|a\| - \|b\|)\,\|b\|$



$$x = x' 2^n + s$$

$$y = y' 2^n + t$$

$$\left\lfloor \frac{x}{y} \right\rfloor + 2 \geq \left\lfloor \frac{x'}{y'} \right\rfloor \geq \left\lfloor \frac{x}{y} \right\rfloor$$

Feb 4, 2025 $\|a\|$, l_a

$a_i \le B-1$

$$a = \sum_{i=0}^{l_a-1} B^i a_i \quad , \quad a_{l_a-1} \neq 0$$

$$a \ge B^{l_a-1} \qquad a_{l_a-1}=1 \qquad a_i = 0 \ \forall i \neq l_a-1$$

$$a \le \sum_{i=0}^{l_a-1} (B-1) B^i = (B-1) \sum_{i=0}^{l_a-1} B^i = (B-1)\frac{B^{l_a}-1}{B-1}$$

$$a \le B^{l_a} - 1$$

$$\boxed{B^{l_a-1} \le a \le B^{l_a} - 1}$$

$\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$

$\lceil x \rceil - 1 < x \le \lceil x \rceil$

(1) $\|a\|$ in terms of a, B

$$a \le B^{l_a} - 1 < B^{l_a}$$

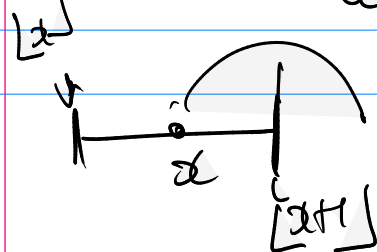
$$\log_B a < l_a$$

$$a \ge B^{l_a-1} \Rightarrow \log_B a \ge l_a - 1$$

$$l_a - 1 \le \log_B a < l_a$$

$$l_a \le \log_B a + 1 < l_a + 1$$

$$l_a = \lfloor \log_B a + 1 \rfloor = \lfloor \log_B a \rfloor + 1$$



$$\|a\| = l_a = \lfloor \log_B a \rfloor + 1$$

② $\|a+b\| = l$ $\quad l = f(l_a, l_b)$

$l_a \geq l_b$

$B^{l_a-1} + B^{l_b-1} \leq a+b \leq B^l - 1$

$B^{l_b-1}\left(B^{l_a-l_b}+1\right) \leq B^l - 1 < B^l$

$B^{l_a-l_b} < B^{l-l_b+1}$

$l_a - l_b < l - l_b + 1 \rightarrow l > l_a - 1 \Rightarrow \boxed{l \geq l_a}$

$B^{l_a-1} + B^{l_b-1} \geq a+b \geq B^{l-1}$

$B^{l_a} + B^{l_b} > B^{l-1} \Rightarrow B^{l_b}\left(B^{l_a-l_b}+1\right) > B^{l-1}$

$B^{l_a-l_b} + 1 > B^{l-l_b-1}$

$\Rightarrow B^{l_a-l_b} \geq B^{l-l_b-1}$

$\Rightarrow l_a - l_b \geq l - l_b - 1 \Rightarrow \boxed{l \leq l_a + 1}$

$\boxed{l_a \leq l \leq l_a+1}$ l_a is the length of $\max(a, b)$.

③ $\|a*b\| = l$

$\left(B^{l_a-1}\right)\left(B^{l_b-1}\right) \leq a*b \leq B^l - 1 < B^l$

$B^{l_a+l_b-2} < B^l \Rightarrow \boxed{l \geq l_a + l_b - 1}$

$(B^{l_a}-1)(B^{l_b}-1) \geq a*b \geq B^{l-1}$

$B^{l_a+l_b} > B^{l_a+l_b} - B^{l_a} - B^{l_b} + 1 \geq B^{l-1}$ $\quad B^{l_a}, B^{l_b} > 1$

$l_a + l_b > l-1 \qquad l < l_a + l_b + 1$

$\boxed{l \leq l_a + l_b}$

$\boxed{l_a + l_b - 1 \leq l \leq l_a + l_b} \rightarrow$

④ $\lfloor a // b \rfloor$ $\qquad a // b = x$

$\boxed{l_a - l_b \pm 1}$ $\qquad \left\lfloor \frac{a}{b} \right\rfloor = x$

$x \leq \frac{a}{b} < x+1$

$\boxed{b \cdot x \leq a < b(x+1)}$

$\|b \cdot x\| \leq \|a\| \leq \|b(x+1)\|$

$a - b$

$a - 2b$

$a - 3b$

$\boxed{\left\lfloor \frac{a}{b} \right\rfloor \|a\|}$ X

polylog $(\|a\|, \|b\|)$

$\frac{50}{3}$

$\|00\|0$ ⑥

Thm: $x = x'2^n + l$, $y = y2^n + t$

$$\left\lfloor \frac{x}{y} \right\rfloor - 2 \le \left\lfloor \frac{x'}{y'} \right\rfloor \le \left\lfloor \frac{x}{y} \right\rfloor$$

$$\frac{35926780 19}{8 \times 10^4 + 3250} \quad \frac{359267819}{83250} = q_{k-1} q_{k-2} \cdots q_0$$

$$\frac{a}{b} = q \cdots -$$

$$\left\lfloor \frac{a}{b} \right\rfloor = q_{k-1} q_{k-2} - q_0$$

$$a = b \times (q \cdots -)$$

$$b\left(\sum_{i=0}^{k-1} B^i q_i\right) \le a \Rightarrow b \times q$$

$$\left\lfloor \frac{a}{b} \right\rfloor$$

$$\left(\sum_{j=0}^{l_b - 1} B^j b_j\right)\left(\sum_{i=0}^{k-1} B^i q_i\right) \le \sum_{l=0}^{la-1} B^l a_l$$

$$\frac{a}{b} = q \cdots - \Rightarrow \left\lfloor \frac{a}{b} \right\rfloor = q \cdots$$

$$\frac{35926780 \times 10^3 + 019}{83 \times 10^3 + 250}$$

Proof:

$$x \equiv x' B^n + l \quad | \quad y = y' B^n$$

$$\frac{x}{y} = \frac{x'}{y'} + \frac{l}{y' B^n}$$

$$\frac{x}{y} \ge \frac{x'}{y'} \Rightarrow \left\lfloor \frac{x}{y} \right\rfloor \ge \left\lfloor \frac{x'}{y'} \right\rfloor$$

$$\frac{x}{y} = \frac{x'}{y'} + \frac{l}{y' B^n} \le \frac{x'}{y'} + \frac{B^n - 1}{y' B^n} = \frac{x'}{y'} + \frac{1}{y'} - \frac{1}{y' B^n}$$

? $\left\lfloor \frac{x}{y} \right\rfloor \le \left\lfloor \frac{x'}{y'} \right\rfloor \Rightarrow \left\lfloor \frac{x}{y} \right\rfloor = \left\lfloor \frac{x'}{y'} \right\rfloor$

? $2y' \ge \frac{x}{y}$ assume.

$x = x'B^n + s$

$y = y'B^n + t$

$\frac{x}{y} = \frac{x'B^n + s}{y'B^n + t} \le \frac{x''B^n + s}{y'B^n}$

$\left\lfloor \frac{x}{y} \right\rfloor \le \left\lfloor \frac{x''B^n + s}{y'B^n} \right\rfloor = \left\lfloor \frac{x'}{y'} \right\rfloor$

$\frac{x}{y} \ge \frac{x'}{y'+1}$

$\frac{x}{y} = \frac{x'B^n + s}{yB^n + t} \ge \frac{x'B^n + s}{y'B^n + B^n}$

$= \frac{x'}{y'+1} + \left(\frac{s}{B^n(y'+1)} \right)$

$\ge \frac{x'}{y'+1}$

$x'y - xy' - x \le 0$

$2y' \ge \frac{x}{y} \Rightarrow 2y''y - x \ge 0$

$x'y - xy' - x \le 0 \le 2y'y - x$

$$\frac{x'}{y'} - \frac{x}{y} \leq 2$$

$$\frac{x'}{y'} \leq \frac{x}{y} + 2 \Rightarrow \boxed{\left\lfloor \frac{x'}{y'} \right\rfloor \leq \left\lfloor \frac{x}{y} \right\rfloor + 2}$$

Feb 6, 2025

$$\boxed{\begin{aligned} x &= x' B^n + s \\ y &= y' B^n + t \end{aligned}} \quad t = 0$$

$$\Rightarrow \left\lfloor \frac{x}{y} \right\rfloor = \left\lfloor \frac{x'}{y'} \right\rfloor$$

$$\frac{x}{y} = \frac{x' B^n + s}{y' B^n} = \frac{x'}{y'} + \frac{s}{y' B^n} \Rightarrow \frac{x}{y} \geq \frac{x'}{y'}$$

$$\Rightarrow \left\lfloor \frac{x}{y} \right\rfloor \geq \left\lfloor \frac{x'}{y'} \right\rfloor$$

$$\frac{x}{y} = \frac{x'}{y'} + \frac{s}{y' B^n} < \frac{x'}{y'} + \frac{1}{y'} \leq \left\lfloor \frac{x'}{y'} \right\rfloor + \frac{y'-1}{y'} + \frac{1}{y'}$$

$$= \left\lfloor \frac{x'}{y'} \right\rfloor + 1$$

$$x' = q y' + r$$

$$\leq q y' + (y' - 1)$$

$$\frac{x'}{y'} \leq q + \frac{(y'-1)}{y'}$$

$$\frac{x}{y} < \left\lfloor \frac{x'}{y'} \right\rfloor + 1 \Rightarrow \boxed{\left\lfloor \frac{x}{y} \right\rfloor \leq \left\lfloor \frac{x'}{y'} \right\rfloor}$$

$$\left\lfloor \frac{x'}{y'} \right\rfloor$$

$$\boxed{\left\lfloor \frac{x}{y} \right\rfloor = \left\lfloor \frac{x'}{y'} \right\rfloor}$$

$$\frac{4328}{679}$$

$\left\lfloor \frac{4372}{679} \right\rfloor$ ± 2 $\left\lfloor \frac{4372}{67} \right\rfloor$ $\left\lfloor \frac{437}{6} \right\rfloor$

437

$$2y' \geq \frac{x}{y}$$

$$2y'y \geq x$$

x'' $(x = x'B^n + s)B^k$ $\quad x'' = (x'B^k)\cdot B^n + s\cdot B^k$

y'' $(y = y'B^n + t)B^k$ $\quad y'' = (y'B^k)B^n + t\cdot B^k$

$$2(y'B^k)\cdot y'' \geq x''$$

$$2(yB^k)\cdot yB^k \geq x\cdot B^k$$

$$2y'y \geq \frac{x}{B^k}$$

$$(2y'y)B^k \geq x$$

$$x'' = q''\cdot y'' + r'' \qquad q'' = \left\lfloor \frac{x''}{y''} \right\rfloor$$

$$q_1 = \left\lfloor \frac{x}{y} \right\rfloor \qquad x = qy + r$$

$$q = q''$$

$$r * B^k = r''$$

$$B^k x = q''\cdot B^k y + r''$$

$$x = \underbrace{q''}_{q}\cdot y + \left(\frac{r''}{B^k}\right) r$$

$$47329 - x$$
$$682 - y$$

$$\frac{473 \times 10^2 + 29}{6 \times 10^2 + 82} \qquad x' = 473 \quad y' = 6$$

$$2 \cdot y' y \geq x / 10^k$$

$$2 \cdot 6 \cdot 682 \geq \frac{473|2|9}{10^k}$$

$$8184 \qquad k = 1$$

$$T(a * b) = O(l_a \times l_b)$$

$$T(a/b) = O(l_a \times l_b)$$

GCD(a, b)

$a = r_0$

$b = r_1$

$r_0 = q_1 r_1 + r_2$

$r_1 = q_2 r_2 + r_3$

$r_{k-1} = q_k r_k + (r_{k+1} = 0)$.

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

r_{k-1}

r_k

$$r_i = q_{i+1} r_{i+1} + r_{i+2} = 0$$

$$\Rightarrow \gcd(r_i, r_{i+1}) = \gcd(r_{i+1}, r_{i+2}).$$

EGCD

$$\underbrace{g = \alpha \cdot a + \beta b}_{k \longleftarrow k}$$

$$r_i = q_{i+1} r_{i+1} + r_{i+2}$$

$$\begin{bmatrix} q_{i+1} & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} r_{i+1} \\ r_{i+2} \end{bmatrix} = \begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix}$$

$i = k-1$

$$\begin{pmatrix} r_{i+1} \\ r_{i+2} \end{pmatrix} = \begin{bmatrix} q_{i+1} & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} r_i \\ r_{i+1} \end{bmatrix}$$

$$\begin{bmatrix} r_k \\ 0 \end{bmatrix} = \begin{bmatrix} q_k & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} r_{k-1} \\ r_k \end{bmatrix} \Rightarrow \begin{bmatrix} q_{k-1} & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} r_{k-2} \\ r_{k-1} \end{bmatrix}$$

$$= \begin{bmatrix} q_k & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} q_{k-1} & 1 \\ 1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} r_{k-2} \\ r_{k-1} \end{bmatrix}$$

$$= \underbrace{\prod_{i=k}^{1} \begin{bmatrix} q_i & 1 \\ 1 & 0 \end{bmatrix}^{-1}}_{i=k} \begin{bmatrix} r_0 \\ r_1 \end{bmatrix}$$

$$\begin{bmatrix} g \\ 0 \end{bmatrix} = \begin{bmatrix} x & y \\ z & \alpha \end{bmatrix} \begin{bmatrix} r_0 \\ r_1 \end{bmatrix} \Rightarrow g = x r_0 + y r_1 = x \cdot a + y b.$$

Binary GCD

$a \cdot 2^m \qquad b \cdot 2^n$

$$\gcd(a \cdot 2^m, b \cdot 2^n) = 2^{\min(m,n)} \cdot \gcd(a \cdot 2^{m-n}, b)$$

$m \geq n$

```
k = 0
while 2|a and 2|b:
    a ← a/2 ; b ← b/2 ; k ← k+1
return 2^k · gcd(a,b)
```

```
gcd(a,b):
    k = 0
    while 2|a and 2|b:
        a ← a/2 ; b ← b/2 ; k ← k+1
    return 2^k · gcd(a,b)
```

$a = a' \cdot 2^t$, b is odd.

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

V2

```
g = gcd(a,b):
    k = 0
    while 2|a & 2|b:
        a ← a/2 ; b ← b/2 ; k ← k+1
    g = 2^k · gcd(a,b)
    while 2|a: a ← a/2
    while 2|b: b ← b/2
    g = 2^k · gcd(a,b)
```

(at least one of a & b is odd)

a ← a − b

if a < b: swap(a, b)

$g = 2^k \gcd(a, b)$

assert ( )

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

$g = 2^k \gcd(a, b)$

termination when $a = 0$

$r_i = q_{i+1} r_{i+1} + r_{i+2}$

$\gcd(r_i, r_{i+1}) = \gcd(r_{i+1}, r_{i+2})$

$\{d \mid d | r_i \text{ and } d | r_{i+1}\} = \{d \mid d | r_{i+1} \text{ and } d | r_{i+2}\}$

$a = r_0$

$b = r_1$

$r_0 = q_1 r_1 + r_2$ $\quad \gcd(a, b) = \gcd(r_1, r_2)$

$r_1 = q_2 r_2 + r_3 \Rightarrow \gcd(a, b) = \gcd(r_2, r_3)$

$r_{k-1} = q_k r_k + 0 \Rightarrow \gcd(a, b) = \gcd(r_{k-1}, r_k) = r_k$

EGCD

$s_0 = 1$

$s_1 = 0$

$s_{i+1} = s_{i-1} - q_i s_i$

$t_0 = 0$

$t_1 = 1$

$t_{i+1} = t_{i-1} - q_i t_i$

$a = r_0$

$b = r_1$

$r_0 = q_1 r_1 + r_2$

$\vdots$

$r_i = q_{i+1} r_{i+1} + r_{i+2}$

$\forall i: r_i = s_i a + t_i b.$

$\gcd(s_i, t_i) = 1$