Class 08

Wednesday, May 26, 2021 7:37 PM

settere → s
se
set
sett
sette
setter

} Proper prefix

20 → 19

$19 \times N$

$20 \times 25 \times 10^3$

$2.5 \times 2 \times 10^5$

5×10^5

— o —

set → s, se

lol → l, lo

setter → s, se, set, sett, sette

setting

unordered_map<ll, vector<int>>

h[setting] ← {4

h[settin] ← {3, 4

h[s] ← {0, 2, 3, 4

h[se] ← {0, 2, 3, 4

h[l] ← {1

h[lo] ← {1

h[set] ← {2, 3, 4

h[sett] ← {2, 3, 4

h[sette] ← {2,

h[setti] ← {3, 4

— o —

s → ATLANTA → $|s| = 7$

p → WLANK → $|p| = 5$

lo = 0

hi = 5

AT LANTA

WLANK

n = |s|

m = |p|

$O((n+m) \cdot \log(\min(n,m)))$

0	1	2	3	4	5
✓	✓	✓	✓	✗	✗

ATLANTA → O(n)

WLANK → O(m)

3

ATL

TLA

LAN

ANT

WLA

LAN

NJA

for(i=0 .... n-1)

for(i=0 .... m-1)

3 — 2 — 1

$f(k) \to \underbrace{abacaba}$ | $f(k) \to aba$ | $f(k) = a$

$f(k-1) \to \underbrace{a}b\,a$

$f(k-2) \to a$

—o—

$d(\underbrace{abaaba}) \to 3$

$f(k) = abaaba$

$f(k-1) = aba$

$f(k-2) = a$

$d(aaaaa)$

$f(k) = aaaaa \to 3$

$f(k-1) = aa \to 2$

$f(k-2) = a \to 1$

$d(aaaa)$

$f(k) = aaaa$

—·—

<u>Primality Testing</u>

$i = [2, N-1]$ $\quad i = [2, \sqrt{N}]$

$N \% i == 0$

$N = 12$

a	b
1	12
2	6

$N = 12$

$a \times b = N$

$\Rightarrow a^2 = N$

$\therefore a = \sqrt{N}$

2	6
3	4
⋮	⋮
x	N/x

```
isPrm(n):
    if(n<2) → false
    for(i=2...√n)
        if(n % i==0)
            → false
→ true
```

$1 \rightarrow 6$

$2 \rightarrow 3$

$v \leftarrow \{i\}$

if($i \times i$!= N)

$v \leftarrow \{N/i\}$

a	b
1	6
2	3

1, 6, 2, 3

1, 2, 3, 6

— o —

$N = (P)^2$

$N = (P_1^{k_1} \times P_2^{k_2} \times P_3^{k_3})^2 \longleftarrow N = n^2$

$\Rightarrow N = P_1^{2k_1} \times P_2^{2k_2} \times P_3^{2k_3}$

$\underbrace{(2k_1+1)}\,\underbrace{(2k_2+1)}\,\underbrace{(2k_3+1)}\cdots\underbrace{(2k_n+1)} = 3$

$(2k_1+1) = 3 \Longrightarrow k_1 = 1$

$12 = 2^2 \times 3^1$

$(2+1)(1+1)$

$= 3 \times 2 = 6$

$N = (P\ \ )^2$

Pollard-rho

Miller-Rabin

divCount[K]

— o —

Miller-Rabin

Q

K L R

[1]
[3]

— o —

— L R

K is odd

$1 \le L \le R \le 10^{10}$

$1 \le K \le 10^{3}$

$1 \le Q \le 10^{5}$

10^5

vector<~~int~~ ll> divCount[1400];

$n_1 \; n_2 \; n_3 \longrightarrow 3$

divCount[3] → {$n_1 n_2 n_3$}

$N = P_1^{k} \; P_2^{k_2} \; P_3^{k_3} \cdots$

$N \to [1, N]$

$N \to [1, 100]$

$2^4 \times 3^2 \times 5 \times 7$

7×11

$2^4 \times 3^2 \times$

2, 3, 5, 7, 11,

$x_1 \geq x_2 \geq x_3 \geq x_4 \geq x_5 \geq x_6 \geq x_7$

$2 \quad 3 \quad 5 \quad 7 \quad 11 \quad 13 \quad 17 \; - \; - \le N \ldots$