

**F: Uinny**

原案: ogiekako

解答: ogiekako, inazz

解説: ogiekako

# 問題

- 同じハッシュの異なる文字列を100個 答えよ  
長さは50まで.
- 長さ  $n$  の文字列  $s$  のハッシュは,

$$h(s) = \sum_{i=0}^{n-1} s[i] a^{n-1-i} \pmod{b}$$

ただし,  $1 \leq s[i] \leq 26$

- $a < b \leq 10^9$

(例えば, Javaの String#hashCode はこういう実装)

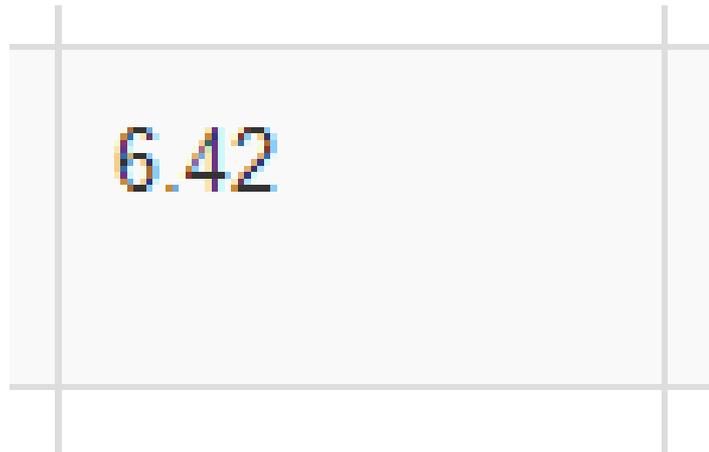
$\times a^3 \quad \times a^2 \quad \times a^1 \quad \times a^0$

u   t   p   c

# 部分点

- $n \leq 100$  個しか出力しなかったら  $n\%$  の点が入る
- TLE までランダム生成して、最も多く衝突したものを答える

→



# 解答の鍵

$s_1, s_2$  が同じ長さで同じハッシュをもつ  
 $t_1, t_2$  も同じ長さで同じハッシュをもつ  
とき

$$s_1 + t_1, s_1 + t_2, s_2 + t_1, s_2 + t_2$$

のハッシュは全て等しい。

$$\begin{array}{cccc} \times a^3 & \times a^2 & \times a^1 & \times a^0 \\ \color{lightgreen}\square & \color{lightgreen}\square & \color{lightcoral}\square & \color{lightcoral}\square \end{array}$$

3つ以上でも同様。

# 解法

同じハッシュをもつペア 7個

$$(s_{11}, s_{12}), (s_{21}, s_{22}), \dots, (s_{71}, s_{72})$$

が見つかれば, 同様にして,  $2^7 = 128 \geq 100$   
個の同じハッシュを持つ文字列が生成できる.

$|s_{ij}| \leq 7$  なら, 文字列長は 50 以下.

# 解法

- 文字列長 7 の, 同じハッシュとなるペアを見つけたい
- 乱択!
- ランダムに生成すれば,  $O(\sqrt{b})$  回の試行で過去のどれかと重複する.

<http://ja.wikipedia.org/wiki/誕生日攻撃>

(全く同じ文字列である確率  $< \frac{10^9}{26^7} \approx \frac{1}{8}$ )

# 結果

- First AC (200) : Komaki
- AC / try : 7/59