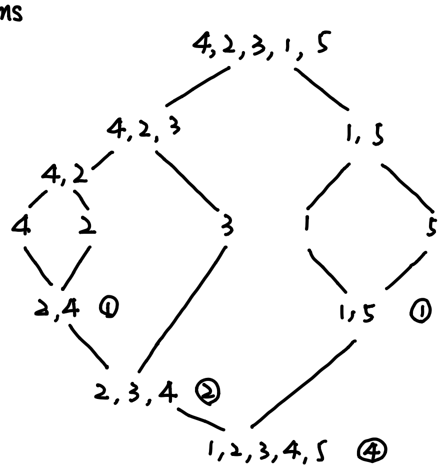
VE 203 Mid 2 周维凯 518021911039

Algorithms

Ex1. i)



We need $1+1+2+4=8$ comparisons.

ii).
4 2 3 1 5) 1
2 4 3 1 5) 2
2 3 4 1 5) 1
1 2 3 4 5) 5
1 2 3 4 5

We need $1+2+1+5=9$ comparisons.

Ex2. i) $\frac{6}{7}=\frac{1}{2}+\frac{5}{14}=\frac{1}{2}+\frac{1}{3}+\frac{1}{42}$

ii) Since $0<x=\frac{p}{q}<1$, we have $0<p<q$ for $p,q\in\mathbb{N}$

So $p\geq 1$ and $p\in\mathbb{N}$, $q\geq 2$ and $q\in\mathbb{N}$, also $p<q$.

1 When $p=1$, $\frac{1}{q}$ is egyptian fraction

2 Then we will prove that $\frac{p}{q}$ can be expressed as Egyptian fraction if all the rational numbers between $(0,\frac{1}{m}]$ have the Egyptian fraction representation, where m is the number such that $\frac{1}{m}\leq\frac{p}{q}<\frac{1}{m-1}$

If $\frac{p}{q}=\frac{1}{m}$, then it of course has Egyptian fraction.

If $\frac{1}{m}<\frac{p}{q}<\frac{1}{m-1}\Rightarrow p(m-1)<q\Rightarrow pm-q<p$

$$\frac{p}{q}-\frac{1}{m}=\frac{pm-q}{mq}<\frac{p}{mq}<\frac{q}{mq}<\frac{1}{m}$$

Therefore, $\frac{p}{q}-\frac{1}{m}$ has Egyptian fraction representation.

Therefore, $\frac{p}{q}=\left(\frac{p}{q}-\frac{1}{m}\right)+\frac{1}{m}$ has Egyptian fraction representation.

Also, $\frac{p}{q}-\frac{1}{m}<\frac{1}{m}$, so there is no repeated n_i.

Therefore, it is proved.

iii) Input: $p, q \in N$ and $0<p<q$

Output: $n_1, n_2, \cdots, n_k$, where n_i for $1 \le i \le k$ are distinct and $\sum_k \frac{1}{n_i} = \frac{p}{q}$

$\alpha \leftarrow p/q$;

$i \leftarrow 1$;

$n_1 \leftarrow 0$;

while $\alpha \neq 0$ do

  $m \leftarrow \lceil 1/\alpha \rceil$;

  $n_i \leftarrow m$;

  $i \leftarrow i+1$;

  $\alpha \leftarrow \alpha - 1/m$;

end while

return $(a_1, a_2, \cdots, a_k)$

iv) We can first minus 1 to get the new α, then we judge whether the new α is within $(0,1)$, if not, we minus $\frac{1}{2}$; other wise, it is within $(0,1)$ and can be solved by iii). For those minus $\frac{1}{2}$, we further judge whether the new α is within $(0,1)$, if not, we minus $\frac{1}{3}$; other wise, it is within $(0,1)$ and can be solved by iii) $\cdots$ We can continue to do this process untill the new α is with $(0,1)$ and can be solved by iii). In other words, we can find the smallest m such that $a = \alpha - \sum_{k=1}^{m} \frac{1}{k} < 1$. Then the Egyptian fraction of a can be find in iii). After that, the Egyptian of α equals the Egyptian of a plus $\sum_{k=1}^{m} \frac{1}{k}$. However, some fraction, e.g. $\frac{1}{n}$, may appear for more than once.

Recall that $\frac{1}{n(n+1)} = \frac{1}{n} - \frac{1}{n+1}$, therefore $\frac{1}{n} = \frac{1}{n(n+1)} + \frac{1}{n+1}$. Then we can replace all the repeated $\frac{1}{n}$ except the first one. Continue doing this, we can find the final Egyptian fraction.

$\frac{12}{5} = 1 + \frac{7}{5} = 1 + \frac{1}{2} + \frac{9}{10} = 1 + \frac{1}{2} + \frac{1}{2} + \frac{2}{5} = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{3} + \frac{1}{15} = 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{3} + \frac{1}{3} + \frac{1}{15} = 1 + \frac{1}{2} + \frac{1}{6} + \frac{1}{3} + \frac{1}{12} + \frac{1}{4} + \frac{1}{15} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{6} + \frac{1}{12} + \frac{1}{15}$

Combinatorics

Exl. $20000 = 2^5 \cdot 5^4$

Therefore, $20000 = n_1 \cdot n_2 \cdot n_3 = 2^{p_1+p_2+p_3} \cdot 5^{q_1+q_2+q_3}$, where $n_i = 2^{p_i} \cdot 5^{q_i}$, $i = 1,2,3$.

Then we have $p_1+p_2+p_3 = 5$ and $q_1+q_2+q_3 = 4$, where all p_i and $q_i \in N$, $i=1,2,3$.

Therefore $\binom{5+3-1}{5} \cdot \binom{4+3-1}{4} = \binom{7}{5}\binom{6}{4} = 315$ solution triples by Example 2.4.45.

Pigeonhole Principle

Ex4. For each guest, the number of guests he/she has met before is from 0 to $n-1$.

① If no guest has met zero guest before, then the number of guests he/she has met before is from 1 to $n-1$. There are n people and there are $n-1$ possible number of guests that one has met before.
Then we can get $f: M \to N$, card $M = n$, card $N = n-1$. By pigeonhole principle, we know at least two guests have met the same number of other guests before.

② If there is one guest has met zero guest before, then for the rest guests, the number of guests he/she is from 1 to $n-2$. For these $n-1$ people, there are $n-2$ possible number of guests that one has met before.
Then we can get $f: M \to N$, card $M = n-1$, card $N = n-2$. By pigeonhole principle, we know at least two guests have met the same number of other guests before.

③ If there are more than one people have met zero guest before, then we can always find at least 2 people have met no guests before.

Therefore, at least two people have previously met the same number of other guests.

Inclusion - Exclusion

Ex1. For 10 digit phone number, there are 10^{10} possibilities.

Let's denote A_i as the set that the phone number contain i; S denote the set of all possible phone number.

Then we want to get $|A_1 \cap A_3 \cap A_5 \cap A_7 \cap A_9|$

$$|A_1 \cap A_3 \cap A_5 \cap A_7 \cap A_9| = |S| - \sum_{1\le i\le 5} |A_i^c| + \sum_{1\le i<j\le n} |A_i^c \cap A_j^c| - + \cdots + - |A_1^c \cap A_3^c \cap A_5^c \cap A_7^c \cap A_9^c|$$

$$= 10^{10} - 5\times 9^{10} + \binom{5}{2}\times 8^{10} - \binom{5}{3}\times 7^{10} + \binom{5}{4}\times 6^{10} - 5^{10}$$

Probability

Ex2. We want to prove $\sum_{k=1}^{6} P_k^2 \ge \frac{1}{6}$ with $\sum_{k=1}^{6} P_k = 1$

From Cauchy Inequality, we know that $\sum_{i=1}^{n} a_i^2 \sum_{i=1}^{n} b_i^2 \ge \left(\sum_{i=1}^{n} a_i b_i\right)^2$ ("=" is taken when $\frac{a_1}{b_1} = \cdots = \frac{a_n}{b_n}$, or at least a_i or b_i is all zeros).

Then we have $\sum_{k=1}^{6} P_k^2 \sum_{k=1}^{6} 1^2 \geqslant \left(\sum_{k=1}^{6} P_k\right)^2$

$$\sum_{k=1}^{6} P_k^2 \cdot 6 \ge 1^2$$

$$\sum_{k=1}^{6} P_k^2 \ge \frac{1}{6}$$

Cryptography

Ex1. $91 = 13\times 7$

$(13-1)(7-1) = 72$

Then we want to find d, the inverse to $5 \bmod 72$

$72 = 5\times 14 + 2$

$5 = 2\times 2 + 1$

$2 = 2\times 1 + 0$

so $\gcd(5, 72) = 1$.

Then we have

$1 = 5 - 2\times 2$

$= 5 - 2\times(72 - 5\times 14)$

$= 29\times 5 - 2\times 72$

Therefore, $d = 29$

Also $m \equiv c^d \bmod n$

$30^4 \equiv 900\times 900 \equiv (-10)\cdot(-10) \equiv 100 \equiv 9 \bmod 91$

$30^{29} \equiv (30^4)^7 \cdot 30 \equiv 9^7 \cdot 30 \equiv (9^2)^3 \cdot 9 \cdot 30 \equiv (-10)^3 \cdot 9 \cdot 30 \equiv -10\cdot 9\cdot 9\cdot 30 \equiv 3000 \equiv 88 \bmod 91$

Therefore, $m = 88$.

Recurrence Relations

Ex1. The characteristic equation is

$r^2 = r + 2 \Rightarrow r_1 = -1,\ r_2 = 2$

Then $J_n = \alpha_1 (-1)^n + \alpha_2 \cdot 2^n$

$$\left.\begin{aligned} J_0 &= \alpha_1 + \alpha_2 = 0 \\ J_1 &= -\alpha_1 + 2\alpha_2 = 1 \end{aligned}\right\} \Rightarrow \begin{cases} \alpha_1 = -\frac{1}{3} \\ \alpha_2 = \frac{1}{3} \end{cases}$$

Then $J_n = -\frac{1}{3}(-1)^n + \frac{1}{3}\cdot 2^n$