理论

置换的定义

设X是有限集。不失一般性，取X为有前n个正整数组成的集合$\{1,2,\ldots,n\}$□X的**置换**$i_1,i_2,\ldots,i_n$可以看成是X到自身的一一映射，其定义为□ $$f:X\to X$$ 其中$$f(1)=i_1,f(2)=i_2,\ldots,f(n)=i_n$$ 为了强调其可视性，常用$2\times n$的阵列来表示这个置换，如□ $$\left(\begin{array}{c} 1 &2 &\ldots &n\\i_1 &i_2 &\ldots &i_n\end{array} \right)$$

置换群的定义

把有n个元素的集合$\X={1,2,\ldots,n\}$的所有$n!$个置换构成的集合记为S_n□则如果S_n中的非空子集G满足如下三条性质，则定义它为X的**置换群**： (1)合成运算的封闭性□$\forall f,g\in G,f\circ g\in G$ (2)单位元□S_n中的恒等置换$\iota \in G$ (3)逆元的封闭性□$\forall f\in G,f^{-1}\in G$

特别的S_n是一个置换群，称它为n阶对称群，仅有一个恒等置换的集合$G=\{\iota \}$也是一个置换群。

置换群都满足消去律□ $$f\circ g=f\circ h \; \leftrightarrow \; g=h$$ 因为用f^{-1}左乘等式两端，并通过结合律，则得证

置换的幂运算

参考文献: *《2005信息学国家集训队论文：置换群快速幂运算 研究与探讨》——潘震皓*

对任意置换T□可对其进行循环分解，如 $$f=\left (\begin{array}{c} 1&2&3&4&5&6&7&8\\6&8&5&4&1&3&2&7\end{array}\right)=[1\;6\;3\;5]\circ[2\;8\;7]\circ[4]$$ 显然有如下性质：对置换T□$T^k=\iota$的最小正整数解为T中所有循环长度的最小公倍数

特别地，当T为单循环时，则$T^k=\iota$的最小正整数解为T的循环长度l

对置换的整幂运算T^n□感觉用快速幂$O(nlogk)$就行（~~其实是因为论文中的算法没看懂~~

对置换的分数幂运算（开方） 分两种情况：

单循环：如果循环长度和指数互质则能开方，否则不能

多循环：取$m=gcd(l,k)$个长度相同的循环合并，如果某个长度的循环数不能被m整除则不能开方

题目

1、置换群中的循环

poj1026 Cipher

每次给出一个置换，再给出多个字符串，如果字符串长度为k则对字符串的下标置换k次（空出来的地方填空格），然后输出新的字符串

不用置换群的知识就硬模拟都行，找出置换群里的每个循环，然后模拟即可

poj3270 Cow Sorting

一个两两不同的序列$a[i]$□可以交换$a[i],a[j]$的值，花费为$a[i]+a[j]$□问如何花费最少的代价使得序列边为升序

记排序后的序列的下标序列为p□则可以构造原下标对应p一个置换 $$\left (\begin{array}{c} 1&2&\ldots&n\\p_1&p_2&\ldots&p_n\end{array}\right)$$ 求出置换中所有的循环，考虑每个循环中交换的花费。记某个循环中所有下标对应最小的值为mi□循环长度为len□该循环中所有下标对应值的和为sum□所有序列中的最小值为low□则每个循环的最小花费为$min\{sum+mi\times (len-2),\; sum+mi+low\times (len+1)\}$