求一个 N 阶有限群 G 的全部子群

张子豪　　1120203325

1　循环群

1.1　循环群的判断

若 N 为素数，由 Lagrange 定理的推论，其必为循环群。

若 N 不为素数，由算术基本定理，必有

$$N = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}.$$

其中，p_i 为素数, $r_i \in N, i = 1, 2, 3, \ldots, n$ 且 $p_1 < p_2 < \ldots < p_n, N > 1$.

由第一 Sylow 定理，G 中必存在 p_i^r 阶子群，其中，$1 \le i \le n$ 且 $1 \le r \le r_i$.

以下考虑 $p_1 = 2$ 且 $r_1 \ge 2$ 的情况：

显然，群 G 必存在 4 阶子群，又 Klein 四元群是 4 阶非循环群，故由定理 10.14 可知，若群 G 存在与 Klein 四元群同构的子群，则群 G 必为非循环群。

令 $G = \{e, a_1, a_2, \ldots, a_{N-1}\}$. 可通过如下算法判断群 G 是否存在子群 H 与 Klein 四元群同构：

Algorithm 1 ClienJudge(G, N)

找到群 G 的所有二阶元 $b_1, b_2, \ldots, b_s$
if $s \le 2$ **then**
　return false
end if
for $i = 1$ to $s - 2$ **do**
　for $j = i + 1$ to $s - 1$ **do**
　　for $k = j + 1$ to s **do**
　　　if $b_i * b_j = b_k$ 且 $b_i * b_k = b_j$ 且 $b_j * b_k = b_i$ **then**
　　　　return true
　　　end if
　　end for
　end for
end for
return false

若 G 存在与 Klein 四元群同构的子群，则 G 不是循环群。

1.2 循环群子群的求解

若 G 为循环群，根据定理 10.14，求解群 G 的所有子群的思路如下：

首先找到群 G 的一个生成元 a 满足 $G=<a>$, 然后对于 N 的每个正因子 d, 计算 $<a^{\frac{n}{d}}>$ 得到其唯一的 d 阶子群。即求出 G 的所有子群。

算法伪代码如下：

Algorithm 2 CircleRes(G, N)

```
for i = 1 to N do
    if G = {a_i^1, a_i^2, ..., a_i^N} then
        a = a_i
    end if
end for
for d = 1 to N do
    if d|N then
        H = {a^{n/d}, a^{2n/d}, ..., a^{Nn/d}}
        print  H
    end if
end for
```

2 非循环群

若 $G=\{e,a_1,a_2,\ldots,a_{N-1}\}$ 为非循环群，不妨设 $|a_1|\leq|a_2|\leq\ldots\leq|a_{N-1}|$ 且二阶元的数目为 m，即 $a_1,a_2,\ldots,a_m$ 均为二阶元，其中 $m\geq 0$. 易证 G 中阶大于 2 的元素个数是偶数，故可将 $a_{m+1},a_{m+2},\ldots,a_{N-1}$ 表示为 $b_1,b_2,\ldots,b_s,c_1,c_2,\ldots,c_s$. 其中,$c_i=b_i^{-1},2s=N-m-1,i=1,2,\ldots,s$. 即

$$G=\{e,a_1,a_2,\ldots,a_m,b_1,b_2,\ldots,b_s,c_1,c_2,\ldots,c_s\}$$

所以，对于 G 的某子集 Ω，若 Ω 满足以下条件之一，则 Ω 一定不是 G 的子群：

(1)$\exists b_i\in\Omega,c_i\notin\Omega$ 或 $\exists c_i\in\Omega,b_i\notin\Omega$，$i=1,2,\ldots,s$.

(2)Ω 中 2 阶元个数的奇偶性与 $|\Omega|$ 的奇偶性相同

(3)$|\Omega|$ 不是 N 的因子

基于上述分析，可以快速判断某子集 Ω 不是 G 的子群，由此得到的改进穷举法求解 G 的所有子群的算法如下：

3 测试结果

以 Klein 四元群为例，结果如图 1 所示：

Algorithm 3 TraverseRes(G, N)

for $\Omega \in G$ **do**
  $flag = 1, numtwo = 0$
  for $a \in \Omega$ **do**
    if $a * a = e$ **then**
      $num_t wo + +$
    end if
  end for
  if $numtwo = |\Omega| \bmod 2 \vee N \neq |\Omega| \bmod |\Omega|$ **then**
    continue;
  end if
  for $i \in \{1, 2, \ldots, s\}$ **do**
    if $b_i \in \Omega \wedge c_i \notin \Omega \vee c_i \in \Omega \wedge b_i \notin \Omega$ **then**
      $flag = 0, break$;
    end if
  end for
  if $flag = 0$ **then**
    continue;
  end if
  for $\forall a, b \in \Omega$ **do**
    if $a * b \notin \Omega$ **then**
      $flag = 0, break$;
    end if
  end for
  if $flag = 0$ **then**
    continue;
  end if
  print Ω
end for

```
请输入群G中元素个数：4
请输入第1个元素依次左乘所有元素的结果，以逗号分隔：0,1,2,3
请输入第2个元素依次左乘所有元素的结果，以逗号分隔：1,0,3,2
请输入第3个元素依次左乘所有元素的结果，以逗号分隔：2,3,0,1
请输入第4个元素依次左乘所有元素的结果，以逗号分隔：3,2,1,0
群G： [0, 1, 2, 3]
群G的运算表：
 0   1   2   3
 1   0   3   2
 2   3   0   1
 3   2   1   0
G是非循环群
G的全部子群如下：
[0]

[0, 1]

[0, 2]

[0, 3]

[0, 1, 2, 3]
```

图 1: