作业5

1. 请心算列举出群 $\mathbb{Z}_{10}$ 的所有生成元。
2. 群 $\mathbb{Z}_{17}^*$ 有多少个生成元？已知 3 是其中一个生成元，请问 9 和 10 是否生成元？
3. p 和 q 是素数，请问 $\mathbb{Z}_{pq}$ 都多少个生成元？r 是任意正整数，请问 $\mathbb{Z}_{p^r}$ 都多少个生成元？
4. 证明：如果 p 是素数，则 $\mathbb{Z}_p$ 没有非平凡子群。
5. 证明：设 n 为任意正整数，群 $\mathbb{Z}_n$ 的生成元 r 满足以下条件：$1 \leq r \leq n$，且 $gcd(r,n) = 1$。
6. 证明：如果群 $\mathbb{G}$ 没有非平凡子群，则群 $\mathbb{G}$ 是循环群。
7. 证明：群 $\mathbb{G}$ 中任意元素的阶都整除群 $\mathbb{G}$ 的阶。
8. 编程完成以下工作：构造一个素数 p，找出 $\mathbb{Z}_p^*$ 的一个生成元。
9. 设 q 是素数且 $p = 2 * q + 1$ 也是素数。选取 $g = h^2$ 且 $g \neq 1$，其中 h 是 $\mathbb{Z}_p$ 中的元素。显然，$\langle g \rangle$ 是循环群。
   (a). 群 $\langle g \rangle$ 的阶是多少，为什么？
   (b). 群 $\langle g \rangle$ 中有多少个生成元，为什么？
   (c). 写一个 Python（或者 Sage）程序生成群 $\langle g \rangle$。

1.Z_{10} 的所有生成元：1,3,7,9。

2.Z_{17}^* 有8个生成元，9不是生成元，10是生成元。 生成元为：3、5、6、7、10、11、12、14

3 Z_p 有 $\Phi(p) \cdot \Phi(q)$ 个生成元，Z_{p^r} 有 $\varphi(p^r) = p^r - p^{r-1}$ 个生成元

4.证明：如果p是素数，那么Z_p没有非平凡子群

假设p是素数，那么$Z_p = \{[0],[1],[2],\cdots,[p-1]\}$

Z_p的平凡子群为：Z_p本身，和仅含一个单位元0的$\{0\}$

假设Z_p有非平凡子群，那么设H是Z_p的非平凡子群，$|Z_p| = p$，

那么H必有Z_p的非单位元，设为h, h∈H 且 h∈Z_p 。

由拉格朗日定理可知，子群的阶必定能够整除群的阶，又因为Z_p的阶p为素数，所以h的阶只能等于1或者p。

因为h≠1，所以h=p,即h生成的循环子群H的阶也是p，$|H| \geq p = |Z_p|$

有 H=Z_p ，与我们的假设H是Z_p的非平凡子群相矛盾，所以Z_p没有非平凡子群

5.证明：设n为任意正整数，群Zn的生成元r满足1≤r <n，且 $gcd(r,n) = 1$

欲证明该命题，我们须先证明定理1：n阶循环群G，a是G的一个生成元，当n|k时，有$a^k = e$。和定理2：n阶循环群G，a是G的一个生成元，如果$b = a^k$，那么b的阶就是n/d,其中 $d = gcd(k,n)$

（1）先证明定理1

我们知道Zn是循环群，阶为n,设生成元a∈Zn,假设$a^k=e$，由除法定理知，$k=qn+r$，其中$0\le r<n$，因此有

$e=a^k=a^{nq+r}=a^{nq}a^r=ea^r=a^r$，因为最小的正整数必须为n使得$a^n=e$成立，所以有r=0，n|k

反过来也是一样，如果n|k，对于任意整数q,有$k=qn$，有

$a^k=a^{qn}=(a^n)^q=e^q=e$成立，所以定理1成立。

（2）证明定理2

Zn是循环群，有$a^n=e$成立。任取生成元a∈Zn，设$b=a^k$，且设m为满足$b^m=e$的最小正整数,

有 $b^m=a^{km}=e$，根据定理1可知，m必须满足 $n|km$，即$n/d|m(k/d)$，其中$d=gcd(k,n)$。

因为d是k,n的最大公约数，所以n/d 与 k/d是互素的。

因此 n/d 必须整除 m。所以，满足这个条件最小的m=n/d，定理2得证。

设r为Zn的一个生成元，设 $gcd(r,n)=1$ ，$r^k=e$，有 $rk\equiv 0 \quad mod \quad n$

即$n|rk$，又 $gcd(r,n)=1$ ， 有n | k成立，这与定理2 符合，所以$gcd(r,n)=1$是成立的

又因为r∈Zn，所以$r\in[1,n)$

6.证明：如果群G没有非平凡子群，那么群G是循环群

设群G无非平凡子群，任取一个元素a∈G，且a是非单位元，则$\langle a\rangle$是G的子群

又因为子群$\langle a\rangle$≠{e}，所以G=$\langle a\rangle$，即G是循环群（G可由非单位元a生成）。

7.证明：群G中任意元素的阶都能整除G的阶

欲证明该命题，先证明群论中的拉格朗日定理

设G是一个有限群，H为G的子群，群G被划分为[G:H]个不同的左陪集（相当于[G:H]个等价类），每个左陪集有$|H|$ 个元素，因此有

$|G|=[G:H]|H|$，即G的阶能被子群的阶整除

再证明对于任意元素$g\in G$，有 g的阶能整除G的阶

对于$\forall g\in G$，对元素g不断地做自乘，会形成循环子群，满足$g^e mod|G|=1$ 的最小正整数e就是元素g的阶，也是这个循环子群的阶。

因为循环子群也是G的一个子群，子群的阶能够整除群G的阶，所以，元素的阶也能够整除群G的阶，证毕！

8.编程

```
/**
    找到zp*的一个生成元,p为素数
    @author:陈海龙
*/
//穷举，速度很慢
#include<iostream>
```

```
#include<set>
#include<math.h>
using namespace std;
set<long long> ans;
int change(int p)
{
    if (p == 2)
        return 1;
    int count = 0;
    for (int i = 2; i < p; i++)
    {
        for (int j = 0; j < p-1; j++)
        {
            long long c = pow(i, j);
            c = (c + p) % p;
            cout << c << " ";
            if (ans.find(c) == ans.end())
                ans.insert(c);
            else
                break;
        }
        //cout << ans.size() << endl;
        if (ans.size() == (p - 1))
        {
            count++;
            cout << i << endl;
        }
        cout << endl;
        ans.clear();
    }
    return count;
}
int main() {
    int p;
    cin >> p;
    cout << change(p) << endl;
    return 0;
}
```

9.设q是素数且p=2*q+1也是素数，选取g=h^2 且 g≠1，其中h是Z_p^*中的元素。显然,$< g >$是循环群

(a)群$< g >$的阶是多少，为什么？

答：是q，因为设$< g >$的阶为n，那么由费马小定理知

$g^q \quad mod \quad p \equiv h^{2q} \quad mod \quad p \equiv h^{p-1} \quad mod \quad p \equiv 1$ ，

故n 整除 q，而q为素数，且q≠1，则n=q成立，故的阶为q。

(b)群$< g >$中有多少个生成元，为什么？

q-1个，因为$< g >$是循环群，根据定理应该有Φ(q)个生成元

(c)写一个python(或sage)程序生成群$< g >$

```
#@author:陈海龙
```

```python
#生成群<g>
#ans列表装的是每个g的阶
#s列表代表每个g的生成群<g>
q=3
p=2*q+1 #p必须是素数
i=2
ans=[]
while(i!=p):
    g=i**2
    j=1
    k=g
    s=[]
    #print(g)
    #i=p-1时，h=-1 ，不满足条件，必须舍去
    while(j!=p+1):
        g%=p
        if(g==1):
            ans.append(j)
            s.append(g)
            break
        s.append(g)
        g*=k
        #print(g)
        g%=p
        j=j+1
    print(s)  #每一个g=h^2的生成群<g>,这个代码输出时会有多一个含1的列表，这个不是生成群
    i+=1
ans.pop()
print(ans)
```