阶

定义

对于一个正整数 a ，求满足 $ax \equiv 1(mopd)$的最小正整数 x 。保证 a, p 互质。这个最小正整数 x称作 a 在对 p 取模意义下的阶，记做 $ord_p(a)$ ，在 p的值十分明确的时候，可以记做 $ord(a)$ 。

性质

1. $a^n \equiv 1(mopp)$充要条件是 $ord_p(a)|n$ 。推论： $ord_p(a)|\varphi(p)$ 。
2. 若 $a \equiv b(modp)$ ，则 $ord_p(a) = ordp(b)$ 。
3. 若 $a_n \equiv a_i(mopd)$，则 $n \equiv i(modord_p(a))$
4. 令 $n = ord_p(a)$ ，则 $a_0, a_1, \cdots, a_{n-1}$对 p取模两两不同。

原根

定义

若 g是模 p意义下的原根，则 g 满足 $ord_p(g) = \varphi(p)$。

性质

1. 模 p意义下存在原根，当且仅当 p 是如下形式的数： $2, 4, x^a, 2x^a$ 。（x 为奇素数,a 为正整数
2. 当 p为奇素数时，模 p 意义下的原根个数为 $\varphi(\varphi(p))$
3. 若p是一个奇素数，g是模p的一个原根，则g和$g + p$是模p^2的原根；若g是模p的一个原根，则g是模p^a的原根
4. 对于质数 p ， $\varphi(p) = p - 1$ ，将 $p - 1$分解质因数，得到 $p - 1 = \prod p_i^{q_i}$ ，则正整数 g 是模 p 意义下的原根的充分必要条件是：对于所有 i ， $g^{\frac{p-1}{p_i}} \not\equiv 1(modp)$ 。证明：充分性很显然。必要性：首先考虑阶的第 1 点性质，可以得知 $ord_p(g)|p - 1$ ，那么，如果这个值比$p - 1$ 小，必然可以找到一个 i ，使得 $ordp(g)|\frac{p-1}{p_i}$，那么 $g^{\frac{p-1}{pi}} \equiv 1(modp)$，故 g 不是原根，否则，说明 $ordp(m) = p - 1 = \varphi(p)$，$g$是原根。

```
const int N = 1000005;
int cnt, tot, p;
int vis[N], prime[N], fac[N];
//质数筛
void Factor(int x) {
    tot = 0;
    int t = (int) sqrt(x + 0.5);
    for(int i = 1; prime[i] <= t; i++) {
        if(x % prime[i] == 0) {
            fac[tot++] = prime[i];
            while(x % prime[i] == 0) x /= prime[i];
        }
    }
    if(x > 1) fac[tot++] = x;
}
int mypow(int a, int b, int mod) {
    int ans = 1;
    while(b) {
        if(b & 1) ans = 1ll*ans*a% mod;
        a = 1ll*a * a % mod;
        b>>= 1;
    }
    return ans;
}
init();
int solve(int _p) {
    p=_p;
    Factor(p - 1);
    for(int g = 2; g < p; g++) {
        bool flag = true;
        for(int i = 0; i < tot; i++) {
            int t = (p - 1) / fac[i];
            if(quick_pow(g, t, p) == 1) {
                flag = false;
                break;
            }
        }
        if(flag) {return g;break;}
    }
}
```