1. 欧拉判别法

判断数a是否为p的平方剩余

方法：如果a^((p-1)/2)=1(mod p)，那么a是p的平方剩余；如果a^((p-1)/2)=-1(mod p)，那么a是模p的平方非剩余

作用

①：判断大整数是否为完全平方数：判断大整数是否为完全平方数

理论依据：

如果x^2=a(mod p)存在解使得(a,p)=1,那么a为p的平方剩余。

由简化剩余系，可以得到p的平方剩余只为(1^2,2^2,···(p-1)^2)集合的去重结果。

令n是大数，p为一个大素数，那么如果n是一个平方数，将其表示为k\*k=n,则n%p=(k%p)\*(k%p)是p的平方剩余，即n是p的平方剩余。

那么，如果n不是p的平方剩余，我们可以知道n不是一个平方数。

由于这是一个概率算法，我们需要取多个大素数p来进行重复计算来增大计算正确的概率。一般取p为素数，且p>1e9,重复20次。

可以计算出位数为1e6位的大整数n是否为平方数。

计算一次就能确定出n不是平方数的概率：50%（至于原理，我也不知道，暴力测试出来的结果）

此处对于判断大整数是否为完全平方数补充一个稍low的概率性算法

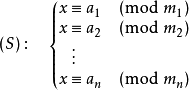
http://blog.163.com/shikang999@126/blog/static/17262489620123710322546/

1. 欧拉降幂求解超大数取模



这个式子当且仅当x>φ(m)时满足

1. =(n\*(n+1)\*(2n+1))/2
2. 在利用for循环的变量i做递推时候，注意使用long long类型的循环变量i，否则可能溢出
3. 容斥原理：一般地，对于任意多个集合，我们都可以列出这样一个等式，等式左边是所有集合的并的元素个数，右边是这些集合的“各种搭配”。每个“搭配”都是若干个集合的交集，且每一项前面的正负号取决于集合的个数——奇数个集合为正，偶数个集合为负。例如：AUBUC|=|A|+|B|+|C|-|A∩B|-|A∩C|-|B∩C|+|A∩B∩C|
4. 组合数的递推公式C[i][j] = (C[i - 1][j] + C[i - 1][j - 1])//支持模运算
5. 中国剩余定理计算公式



其中，m1,m2,m3……两两互质，则对于任意的整数a1,a2,a3,an方程组有解。

https://gss0.bdstatic.com/94o3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D223/sign=afd164d67a310a55c024d9f684444387/7af40ad162d9f2d30fcbdacaaaec8a136327cc39.jpg

https://gss3.bdstatic.com/7Po3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D203/sign=56bcfe3fc55c1038207ec9c28110931c/91ef76c6a7efce1b22fa36efac51f3deb58f65c6.jpg

设https://gss3.bdstatic.com/-Po3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D59/sign=98cf0fe8ff039245a5b5e10687947d4e/562c11dfa9ec8a133826aec5f403918fa0ecc0d3.jpg是https://gss2.bdstatic.com/-fo3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D20/sign=3421af3261d0f703e2b292dc08fa9d75/91ef76c6a7efce1b232431efac51f3deb48f658c.jpg 模 https://gss2.bdstatic.com/9fo3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D17/sign=9757be9e4410b912bbc1f2f9c3fd6213/f3d3572c11dfa9ecd055af3261d0f703918fc198.jpg 的数论倒数( https://gss0.bdstatic.com/-4o3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D14/sign=600e2894abcc7cd9fe2d30dd3801d19f/dcc451da81cb39db7a5c542fd8160924ab18302e.jpg 为 https://gss2.bdstatic.com/-fo3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D20/sign=987bd370be003af349badb60342ace9c/d0c8a786c9177f3ec9a1cf7478cf3bc79f3d5635.jpg模 https://gss2.bdstatic.com/-fo3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D17/sign=41ce7c820246f21fcd345a54f624e601/dc54564e9258d10925da9bcbd958ccbf6c814d89.jpg 意义下的逆元)

https://gss1.bdstatic.com/9vo3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D270/sign=1e2b1996a1ec8a13101a50e7c7039157/5ab5c9ea15ce36d39c3ebe4932f33a87e950b194.jpg

方程组 的通解形式为

https://gss3.bdstatic.com/-Po3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D486/sign=cb3ee938d72a283447a637036db5c92e/2fdda3cc7cd98d10aa8ef514223fb80e7bec90b9.jpg

在模 https://gss1.bdstatic.com/-vo3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D16/sign=e44c04e9c0cec3fd8f3ea373d6887f24/a8ec8a13632762d0aa5d5d9aa3ec08fa513dc6b0.jpg 的意义下，方程组只有一个解：

https://gss0.bdstatic.com/94o3dSag_xI4khGkpoWK1HF6hhy/baike/s%3D162/sign=6e46f98494510fb37c197391eb32c893/8ad4b31c8701a18b0f5da572942f07082838fe5d.jpg

1. 对于多项式P(X),其最高项次数为k，对于整数D,如果对于所有1-k+1，均有P(X)/D为整数，那么对于所有的整数X,P(X)/D都为整数。

证明：

当k=0时，若P(1)能被D整除，那么对于所有的X，P(X)/D都为整数；

当k=1时，P(X)为等差数列，首项为b,公差为P(n+1)-P(n)=a，只要首项和公差都是D的倍数，那么对于所有的X，P(X)/D都为整数。

假设当k=n时候该结论成立。对于k=n+1,P(x+1)-P(x)的结果为最高次为n的多项式。由所有的Pn+1(X)/D都为整数可知，Pn+1(1)/D为整数，并且Pn+1(x+1)-Pn+1(x)为整数。要证明一个最高次为n的多项式Pn(X)/D均为整数，只要对于x等于1到n+1，Pn(X)/D均为整数即可，即要求对于x=1到n+2，P(X)/D均为整数。得证。

1. Burnside定理：对于一个置换f，若一个着色方案s经过置换后不变，称s为f的不动点。将f的不动点数目记为C(f)，则可以证明等价类数目为所有C(f)的平均值。
2. Polya定理：等价类的个数等于所有置换f的的平均数 （用于解决等价类问题，如手镯珠子旋转后等价）
3. 两个循环矩阵的乘积仍然是循环矩阵。（利用该定理可以将循环矩阵快速幂的时间优化到n^2，其中矩阵大小为nxn）
4. 错排公式(n封信装到n个信封，每个都装错的方案数)：D(N)=(N-1)\*(D(N-1)+D(N-2));
5. 卡特兰数(Catalan Number),表示一个进栈序列的出栈序列方案数。设F(n)为n个元素序列的进栈后出栈方案数，那么F(n)= F(0)F(n-1)+F(1)F(n-2)+……+f(n-1)f(0)。其中，F(0)=1,F(1)=1。等价于F(n)=F(n-1)\*(4\*n-2)/(n+1)。以及F(n)=C(2n,n)/(n+1)或者F(n)=C(2n,n)-C(2n,n-1)可以联系到凸多边形三角形划分数，以及n对括号的正确方案匹配
6. 多项式之间可以求gcd，利用辗转相除法,可以找出在模n意义下的最大GCD。理论最坏复杂度n^2logn(远达不到上界)
7. 高斯整数：x=a+b 高斯素数:a\*a+2\*b\*b为素数的高斯整数
8. 约瑟夫环的数论问题：求sum=

解决方案：分层枚举。令tmp=k/I,可以求得k/i=tmp的最大i。maxi=k/tmp

根据k/i的值进行分层枚举即可。

1. 在[初等数论](https://baike.baidu.com/item/%E5%88%9D%E7%AD%89%E6%95%B0%E8%AE%BA/2375326)中，威尔逊定理给出了判定一个自然数是否为[素数](https://baike.baidu.com/item/%E7%B4%A0%E6%95%B0/115069)的[充分必要条件](https://baike.baidu.com/item/%E5%85%85%E5%88%86%E5%BF%85%E8%A6%81%E6%9D%A1%E4%BB%B6/10943559)。即：[当且仅当](https://baike.baidu.com/item/%E5%BD%93%E4%B8%94%E4%BB%85%E5%BD%93/7689242)p为素数时：( p -1 )! ≡ -1 ( mod p )
2. 对于求解形如g(r)=r的方程，可以采用不动点迭代的方法进行求解。

算法分析：x0 = 初始设定值

x1 = g(x0)

x2 = g(x1)

x3 = g(x2)

... ...

x(k+1) = g(x(k))

直到收敛至g(r) = g(lim x(i)) = lim x(i+1) = r