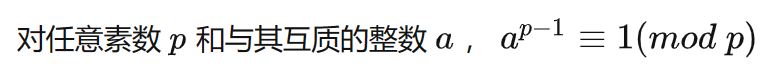
Wj心心念念：整理的不好多多见谅😭，尤其是菲某人不要骂我

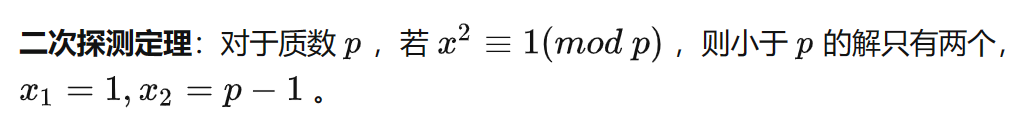
**一、原理（强拟素性检验：****Miller-Rabin素性检验）**

1、预备定理

费马小定理：



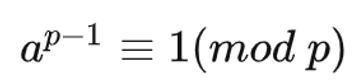
二次探测定理：



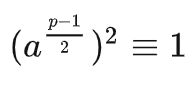
2、思路

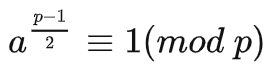
由于费马小定理的产生，尝试将费马小定理反过来用，即“随机选取一小于p的整数a，若满足上式，则是否可以证明p是一素数？”但是这个说法行不通，因为存在一些合数满足这个等式（称为费马伪素数）

于是考虑多选取几个a，提高判别的正确率，即使仍然存在一些合数满足上述等式（称为卡迈克尔数），但是正确率已经大大提高。

**于是整体思路为：对给定p值，取多个a值，如果都满足，则p为素数。**

现在问题变成了：如何选取a值，以及取多少个a值比较合适。

考虑二次检测定理，将其拆分为，如果在mod p 情况下的解不是1或者p-1，那p就不是素数。（不满足二次探测定理）

如果，那可以模仿之前的操作，再进行一轮检验，变成判断，直到最后变成奇数。

也就是说，我们可以将p -1 =u \* 2t(u为奇数)，au，au\*2，au\*4...这一系列数进行检验，他们的解要么全是1，要么出现p-1后全是1 (之前不能有1)，否则就不是素数。当然要注意 p-1不能出现在最后一个数，否则就连费马小定理都不满足了（还要注意这过程中不能产生 p 的倍数）

**再次总结思路：**

**（1）先特判筛掉3以下的数与偶数。**

**（2）将待检验数p，p-1化为 u\*2t（这里求出u和t）**

**（3）选取多个底数，分别对au，au\*2，au\*4进行检验，判断其解是否全为1，或在非最后数的情况下出现 p -1。**

**（底数的选择：在int范围内，选取{2,7,61}三个数作为底数可以保证100%正确；在long long范围内，选取{2,325,9375,28178,450775,9780504,1795265022}七个数作为底数可保证100%正确）**

**（↑这个我不知道他为什么保证100%正确，可能是排除掉了那些合数之后的出来的数吧，关于底数的选择还有一个做法是：**

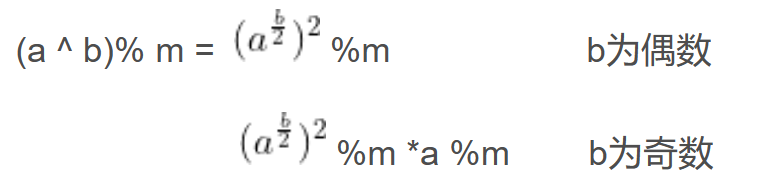
**从2..(n-2)中随机出一个a，若满足第三点，则判n为素数，否则判为合数。此时的出错概率为1/4，且若选取了x个数都满足该点，则出错概率为pow(1/4,x)，若给定出错概率（或者说精度，可以先通过计算算出要选取几个a，再进行随机数的选取））**

**（4）如果都满足，我们就认为这个数是素数**

**二、考虑乘方或者取模过程中的溢出问题**

提供做法：二分思想和快速幂取模

1、二分思想



代码部分：

|  |
| --- |
| long long binarypow(long long a,long long b,long long m){  if(b==1) return a%m;  else if(b%2==0){  long long k=fun(a,b/2,m);  return (k\*k)%m;  }  else{  long long k=fun(a,b/2,m);  return (((k\*k)%m)\*(a%m))%m;  }  } |

2、快速幂取模

“积的取余等于取余的积的取余。即(a \* b) % m = (a%m)\*(b%m) %m”

代码部分：

|  |
| --- |
| long long quickpow(long long a,long long b ,long long m){  long long k=1;  while(b>0){  if(b&1){  k=(k\*a)%m;  }  b=b>>1;  a=(a\*a)%m;  }  return k;  } |

**三、其他素性检验的方法**

1、确定性的素性检验

2、Fermat素性检验

3、Euler拟素性检验

（这些感觉不是重点好像现在用的也不多我就不整理了，现在主流应该就是Miller-Rabin素性检验）

**【参考】**

[【朝夕的ACM笔记】数论-Miller Rabin素数判定 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/349360074)

[(30条消息) 【算法编程】乘方取模\_我从崖边跌落的博客-CSDN博客](https://blog.csdn.net/qq_20135597/article/details/86254261)

[概率算法实现素性检验 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/95424449)

[计算数论1：素性检验 - 知乎 (zhihu.com)](https://zhuanlan.zhihu.com/p/105902706)