强素数生成实现

1.强素数应满足下列条件：

1 什么是强素数

1984年Gordon J.提出了强素数的概念，强素数p应当满足以下4个条件：

(1) p是一个很大的随机素数；

(2) p-1必须有一个很大的素数因子r；

(3) p+1必须有一个很大的素数因子；

(4) r-1也必须有一个大的素数因子。

该定义于1986年写入ISO-DP-9307[3]。

2.算法步骤如下：

4.1 算法步骤

(1) 随机生成 128 位的二进制数 q1，计算 r=p1*q1+1；

(2) 采用 Miller-Rabin 检测 r，若通过转(3)，否则转(1)；

(3) 随机生成 256 位二进制数 q2，计算 p=r*q2+1；

(4) 采用 Miller-Rabin 检测 p，若通过转(5)，否则转(3)；

(5) 对 p+1 采用 $(256)_{10}$ 以内的素数进行分解，最终最到 m，如果 m 少于 64 位转(3)；

(6) 输出 512 位的素数 p，该素数满足强素数特性(1)(2)(4)，并以较大概率满足特性(3)。

关于其中的第5步，也就是验证强素数概念(3)：p+1有一个很大的素数因子：

快速将 p+1 按小素数因子分解，也即用(256)10 之内的素数试除，直到剩下的数不能被(256)10 内素数整除为止，并判断剩余部分的位数。如果高于某个阀值(如 64 位)，则大致认为 p+1 存在大素数因子，否则认为其不存在。

参考文献：一种快速的强素数生成方法 - 豆丁网 (docin.com)