素性测试

杨礼珍

同济大学计算机科学与技术系, 2017

Outline

1. reading
2. 5.5 primetest

作业

阅读《密码学原理与实践》5.4节（P139-146），《数论讲义》上册第六章第2节（161－164）。其中费马素性测试见《数论讲义》，其它算法见《密码学原理与实践》。
课件中注明的章节均来自《密码学原理与实践》。

素性测试

生成随机素数的方法：

1. 生成随机整数n
2. 辨别n是否为素数，有两种辨别方法：

确定性算法 概率1确定x是否为素数，2002年三位印度计算机科学家发现了第一个多项式时间的算法，称为AKS素性测试，计算复杂度为$O(\log^{12}(n))$

随机算法 如果x通过某些素数判定准则，则x可能为素数，如果不通过则x肯定为合数。

如：Solovay-Strassen素性测试、Miller-Rabin素性测试、Fermat素性测试、Lucas素性测试。

素性测试

成功概率分析

- 在$1 \sim N$之间随机选取一个数，其为素数的概率$\approx 1/\ln N$。
- 512比特的随机整数为素数的概率大约为$1/\ln 2^{512} \approx 1/355$。
- 在RSA中，大素数p, q选取为512比特的素数，是可以在随机选取的355 个数中以高概率找到一个素数的。

素性测试
Fermat素性测试

- 回顾Fermat小定理：如果p为素数，则对$a \neq 0 \bmod p$有$a^{p-1} \equiv 1 \bmod p$。
- 反之，如果对整数n，整数$0 < a < n$有$a^{n-1} \neq 1 \bmod n$，则n为合数。

根据以上性质构造素性测试算法：

Fermat素性测试

输入：　整数n，测试次数k

反复运行k次：　随机选取整数$a \in \{1, \dots, n-1\}$

如果$a^{n-1} \neq 1 \bmod n$则n为合数，否则n可能为素数。

素性测试
Fermat素性测试

- 通过增加测试次数k来提高测试准确性。
- 计算复杂度：$O(\log(n)^3)$
- 缺陷：存在合数n，

$$\text{对所有}0 < a < n, \gcd(a, n) = 1\text{有}a^{n-1} \equiv 1 \bmod n$$

这样的合数称为Carmichael数，如561是一个Carmichael数。

  - Carmichael 数非常稀少，而且距离很远。对小于10^{16}的整数，存在246,683个Carmichael数，279,238,341,033,925个素数。

- 应用：PGP加密软件使用Fermat素性测试，在PGP中，通过测试的数为Carmichael数的概率小于$\frac{1}{10^{50}}$。

素性测试
基本概念

- 判定问题：只回答“是(yes)”或者“否(No)”的问题。
- 随机算法：使用了随机数的算法。
- 判定问题的一个偏是(yes-biased)Monte-Carlo算法：算法给出“是”的回答总是正确的，给出“否”的回答也许不正确。如果对应该为“是”的输入至多以ε的概率给出“否”的答案则说该算法具有错误概率ε。
- 判定问题的一个偏否(no-biased)Monte-Carlo算法：算法给出“否”的回答总是正确的，给出“是”的回答也许不正确。如果对应该为“否”的输入至多以ε的概率给出“是”的答案则说该算法具有错误概率ε。

- Miller-Rabin测试，也称为强伪素数测试，是对Fermat测试的改进。
- 原理：$a^{p-1} \equiv 1 \bmod p$等价于$a^{(p-1)/2} \equiv \pm 1 \bmod p$，因为对素数$p$，$x^2 \equiv 1 \bmod p$有2个解$\pm 1$（对合数解的数量多于2或无解）
- 分析：如果$p-1=2^k m$，其中m是一个奇数。

$$
\begin{array}{llcl}
 & a^{2^k m} \equiv 1 \bmod p & \Leftrightarrow & a^{2^{k-1} m} \equiv \pm 1 \bmod p \\
\text{如果} & a^{2^{k-1} m} \equiv 1 \bmod p & \Leftrightarrow & a^{2^{k-2} m} \equiv \pm 1 \bmod p \\
\text{如果} & a^{2^{k-2} m} \equiv 1 \bmod p & \Leftrightarrow & a^{2^{k-3} m} \equiv \pm 1 \bmod p \\
 & \vdots & & \\
\text{如果} & a^{2m} \equiv 1 \bmod p & \Leftrightarrow & a^{m} \equiv \pm 1 \bmod p
\end{array}
$$

- 结论：如果$p-1=2^k m$是素数，序列$a^m, a^{2m}, \ldots, a^{2^{k-1}m}, a^{2^k m} \bmod p$形如

$$(1, 1, \ldots, 1)\text{或者}(*, \ldots, *, -1, 1, \ldots, 1)$$

素性测试

根据上面的素数性质，推导出Miller-Rabin素性测试，前面的讨论知道，对于合数问题是一个偏是的Monte Carlo算法。

算法5.7 Miller-Rabin(n)

把$n-1$写成$n-1=2^k m$，其中m是一个奇数
随机选取整数a，使得$1 \le a \le n-1$
$b \leftarrow a^m \bmod n$ (从a^m开始检查)
If $b \equiv 1 \pmod n$ (这时形为$(1,1,\ldots,1)$)
    then return ("n is prime")
for $i \leftarrow 0$ **to** $k-1$

do {
  if $b \equiv -1 \pmod n$ (这时形为$(***-1,1,\ldots,1)$)
    then return ("n is prime")
  else $b \leftarrow b^2 \bmod n$
}

return ("n is composite")

错误概率分析

- 如果n是奇合数，则至多有$(n-1)/4$个$a \in \{1, \ldots, n-1\}$让n通过Miller-Rabin测试。
- 这说明奇合数只有至多1/4的概率通过一次Miller-Rabin测试。
- 奇合数通过k次Miller-Rabin测试的概率至多为$1/4^k$。

定义两个随机变量：

a： 一个特定长度的随机奇整数n是合数

b： 算法连续回答了m次“n是一个素数”

分析：

- 错误概率为$Pr[a|b]$，待求
- $Pr[b|a] \leq \frac{1}{4^m}$ (即奇合数通过m次素性测试的概率)
- $Pr[\bar{a}] \approx \frac{2}{\ln n}$，即奇整数$n$为素数的概率 (根据素数性质得到)
- $Pr[a] \approx 1 - \frac{2}{\ln n}$
- $Pr[b|\bar{a}] = 1$

演算

$$
\begin{aligned}
Pr[a|b] &= \frac{Pr[b|a]Pr[a]}{Pr[b]} \quad \text{(贝叶斯公式)} \\
&= \frac{Pr[b|a]Pr[a]}{Pr[b|a]Pr[a] + Pr[b|\bar{a}]Pr[\bar{a}]} \quad \text{(全概率公式)} \\
&\approx \frac{Pr[b|a](\ln n - 2)}{Pr[b|a](\ln n - 2) + 2} \quad \text{(代入前面的估计式并约简)} \\
&\le \frac{4^{-m}(\ln n - 2)}{4^{-m}(\ln n - 2) + 2} \quad \text{(代入}Pr[b|a] \le 4^{-m}\text{)} \\
&= \frac{\ln n - 2}{\ln n - 2 + 2^{2m+1}}
\end{aligned}
$$

m	4^{-m}	错误概率的界
1	0.250	0.978
5	0.977×10^{-3}	0.147
10	0.954×10^{-6}	0.168×10^{-3}
50	0.789×10^{-30}	0.139×10^{-27}

素性测试
Solovay-Strassen测试

- Solovay-Strassen测试没有Miller-Rabin测试效率高（运行一次算法，奇合数通过Miller-Rabin测试的概率至多为1/4，通过Solovay-Strassen测试至多为1/2）。
- Solovay-Strassen测试有关的定义：

二次剩余

假设p是奇素数，那么：

a定义为模p的二次剩余 ： $a \not\equiv 0 \pmod{p}$且剩余方程$y^2 \equiv a \pmod{p}$有解。

a定义为模p的二次非剩余 ： $a \not\equiv 0 \pmod{p}$且剩余方程$y^2 \equiv a \pmod{p}$无解。

素性测试
Solovay-Strassen测试

Solovay-Strassen测试有关的定义：

定义5.3(Legendre符号)

假设p是奇素数，对任一整数a，定义legendre符号$\left(\frac{a}{p}\right)$如下：

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod{p} \\ 1 & a\text{是一个模}p\text{二次剩余} \\ -1 & a\text{是一个模}p\text{二次非剩余} \end{cases}$$

由欧拉判定准则有

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

素性测试

Solovay-Strassen测试

Solovay-Strassen测试有关的定义：
把奇素数的Legendre符号推广到奇数上：

定义5.4(Jacobi符号)

假设n是正奇数，且n的素因子分解如下：

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

对整数a，定义Jacobi符号$\left(\frac{a}{n}\right)$如下：

$$\left(\frac{a}{n}\right) \equiv \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}$$

素性测试
Solovay-Strassen测试

Solovay-Strassen测试的原理

- 如果n是奇素数，那么$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$成立。
- 如果n是奇合数，那么$\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}$成立的概率至多为$1/2$，同余方程成立的$a$称为对于基底$n$的Euler伪素数。

算法5.6 Solovay-Strassen算法(n)

随机选取整数a，使得$1 \leq a \leq n-1$
计算$x \leftarrow \left(\frac{a}{n}\right)$
如果$x = 0$ 那么返回(“n是合数”)
否则计算$y \leftarrow a^{(n-1)/2} \pmod{n}$，如果$x \equiv y \pmod{n}$，那么返回(“$n$是素数”)，否则返回(“$n$是合数”)

素性测试

Solovay-Strassen算法的有效性需回答以下2个问题：

- 如何用欧拉判定准则外的方法有效的计算$\left(\frac{a}{n}\right)$：二次剩余一章中已解决。
- 测试多少次才能以高概率确定一个奇数为素数？错误概率是多少？类似于Miller-Rabin素性测试的讨论。

运行m次Solovay-Strassen算法，错误概率分析：
定义随机变量：

- a：一个特定长度的随机奇整数n是一个合数
- b：算法连续回答了m次“n是一个素数”

分析如下：

- 输入为合数时运行1次算法回答是素数的概率$\leq \frac{1}{2}$(见习题5.22)
- 输入为合数时运行m次算法都回答是素数的概率$= Pr[b|a] \leq 2^{-m}$
- 算法运行m次都回答n是素数时，n是合数的概率$= Pr[a|b]$。套用Miller-Rabin素性测试的错误概率讨论，有

$$Pr[a|b] \leq \frac{\ln n - 2}{\ln n - 2 + 2^{m+1}}$$

m	2^{-m}	错误概率的界
10	$.977 \times 10^{-3}$	.147
50	$.888 \times 10^{-15}$	$.157 \times 10^{-12}$
100	$.789 \times 10^{-30}$	$.139 \times 10^{-27}$