第六章 素性检验
2015年06月02日

信息安全数学基础

陈恭亮 教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

素性检验

问题:

如何有效生成大素数?

如何利用素数所具有的性质来生成大素数?

在本章, 我们研究如何产生以及如何快速产生大素数.

伪素数

Fermat 素性检验

6.1.1 伪素数 Fermat 素性检验

根据Fermat 小定理, 我们知道: 如果n 是一个素数, 则对任意整数$b,\ (b,n)=1$, 有

$$b^{n-1}\equiv 1\ (\mathrm{mod}\ n).$$

由此, 我们得到: 如果有一个整数$b,\ (b,n)=1$ 使得

$$b^{n-1}\not\equiv 1\ (\mathrm{mod}\ n),$$

则n 是一个合数.

将指数的语言用于上述的讨论, 并结合定理5.1.1 我们有: 如果n 是一个素数, 则对任意整数$b,\ (b,n)=1$, 有

$$\mathrm{ord}_n(b)\mid n-1.$$

由此, 我们得到: 如果有一个整数$b,\ (b,n)=1$ 使得

$$\mathrm{ord}_n(b)\not\mid n-1.$$

则n 是一个合数.

例6.1.1 因为 $2^{62} \equiv 2^{60} \cdot 2^2 \equiv (2^6)^{10} \cdot 2^2 \equiv 64^{10} \cdot 2^2 \equiv 4 \not\equiv 1 \pmod{63}$,
所以63 一个是合数. 事实上, 我们也有

$$\begin{cases} 2^3 \equiv 1 \pmod 7 \\ 2^6 \equiv 1 \pmod 9, \end{cases}$$

以及$\mathrm{ord}_{63}(2) = 6 \nmid 63 - 1$.
上述说法的否定说法不能成立.
事实上, 我们有

$$\begin{cases} 8^1 \equiv 1 \pmod 7 \\ 8^2 \equiv 1 \pmod 9, \end{cases}$$

以及$\mathrm{ord}_{63}(8) = 2 \mid 63 - 1$.

例6.1.2

$$8^{62} \equiv (2^6)^{31} \equiv 1 \pmod{63}.$$

定义6.1.1 设n 是一个奇合数. 如果整数$b,\ (b,n)=1$ 使得同余式

$$b^{n-1}\equiv 1\ (\mathrm{mod}\ n) \tag{1}$$

成立, 则n 叫做对于基b 的**伪素数**.

注 伪素数的表述也可以用周期序列来解释. 设n 是一个奇合数. 如果整数$b,\ (b,n)=1$ 使得$n-1$ 为序列$u=\{u_k=b^k\ \mathrm{mod}\ n\mid k\geq 1\}$ 的周期, 则n 叫做对于基b 的**伪素数**.

因为n 为素数时, 对任意整数$b,\ (b,n)=1$, 有$n-1$ 为序列$u=\{u_k=b^k\ \mathrm{mod}\ n\mid k\geq 1\}$ 的周期.

由此, 若存在整数$b,\ (b,n)=1$, 使得$n-1$ 不是序列$u=\{u_k=b^k\ \mathrm{mod}\ n\mid k\geq 1\}$ 的周期, 则n 一定是合数.

例6.1.3 整数63 都是对于基$b=8$ 的伪素数,

例6.1.4 整数$341 = 11 \cdot 31,\ 561 = 3 \cdot 11 \cdot 17,\ 645 = 3 \cdot 5 \cdot 43$ 都是对于基$b = 2$ 的伪素数, 因为

$$2^{340} \equiv 1 \pmod{341}, \quad 2^{560} \equiv 1 \pmod{561}, \quad 2^{644} \equiv 1 \pmod{645}.$$

事实上, 我们有

$$\begin{cases} 2^{10} \equiv 1 \pmod{11} \\ 2^{5} \equiv 1 \pmod{31}, \end{cases} \quad \begin{cases} 2^{2} \equiv 1 \pmod{3} \\ 2^{10} \equiv 1 \pmod{11} \\ 2^{8} \equiv 1 \pmod{17}, \end{cases} \quad \begin{cases} 2^{2} \equiv 1 \pmod{3} \\ 2^{4} \equiv 1 \pmod{5} \\ 2^{14} \equiv 1 \pmod{43}, \end{cases}$$

下面讨论伪素数的性质.

定理6.1.1 设是一个奇合数. 则

(i) n 是对于基b 的伪素数当且仅当b 模n 的阶整除$n-1$.

(ii) 若n 是对于基b_1 和基b_2 的伪素数, 则n 是对于基$b_1 \cdot b_2$ 的伪素数.

(iii) 如果n 是对于基b 的伪素数, 则n 是对于基b^{-1} 的伪素数.

(iv) 如果有一个整数b 使得同余式(1) 不成立, 则模n 的简化剩余系中至少有一半的数使得同余式(1) 不成立.

证 (i) 如果n 是对于基b 的伪素数, 则我们有 $b^{n-1} \equiv 1 \pmod{n}$.

根据定理5.1.1, 我们有 $\mathrm{ord}_n(b) \mid n-1$.

反过来, 如果$\mathrm{ord}_n(b) \mid n-1$, 则存在整数$q$ 使得$n-1 = q \cdot \mathrm{ord}_n(b)$.

因此, 我们有 $b^{n-1} \equiv (b^{\mathrm{ord}_n(b)})^q \equiv 1 \pmod{n}$.

(ii) 因为n 是对于基b_1 和基b_2 的伪素数, 所以我们有

$$b_1^{n-1} \equiv 1, \quad b_2^{n-1} \equiv 1 \pmod{n}.$$

从而, $(b_1 \cdot b_2)^{n-1} \equiv b_1^{n-1} \cdot b_2^{n-1} \equiv 1 \pmod{n}$.

故n 是对于基$b_1 \cdot b_2$ 的伪素数.

(iii) 因为n 是对于基b 的伪素数, 所以我们有

$$b^{n-1} \equiv 1 \pmod{n}.$$

从而,

$$(b^{-1})^{n-1} \equiv (b^{n-1})^{-1} \equiv 1 \pmod{n}.$$

故n 是对于基b^{-1} 的伪素数.

(iv) 设$b_1, \ldots, b_s, b_{s+1}, \ldots, b_{\varphi(n)}$ 是模的简化剩余系, 其中前s 个数使得同余式(1) 成立, 后$\varphi(n) - s$ 个数使得同余式(1) 不成立. 根据假设条件, 存在一个整数b, $(b, n) = 1$, 使得同余式(1) 不成立, 再根据结论(ii) 和(iii), 我们有s 个模n 不同简化剩余

$$b \cdot b_1, \ldots, b \cdot b_s$$

使得同余式(1) 不成立. 因此,

$s \leq \varphi(n) - s$, 或者$\varphi(n) - s \geq \dfrac{\varphi(n)}{2}$.

这就是说, 模n 的简化剩余系中至少有一半的数使得同余式(1) 不成立. 证毕

例6.1.5 设$n = 63$. 求出所有整数b, $1 \leq b \leq n-1$ 使得n 是对于基b的伪素数.

a	a^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}	a	a^{n-1}
1	1	12	18	23	25	34	22	45	9	56	49
2	4	13	43	24	9	35	28	46	37	57	36
3	9	14	7	25	58	36	36	47	4	58	25
4	16	15	36	26	46	37	46	48	36	59	16
5	25	16	4	27	36	38	58	49	7	60	9
6	36	17	37	28	28	39	9	50	43	61	4
7	49	18	9	29	22	40	25	51	18	62	1
8	1	19	46	30	18	41	43	52	58		
9	18	20	22	31	16	42	0	53	37		
10	37	21	0	32	16	43	22	54	18		
11	58	22	43	33	18	44	46	55	1		

定理6.1.1 (iv) 告知我们: 对于大奇数, 如果有一个整数$b,\ (b,n)=1$, 使得同余式(1) 不成立, 则模n 的简化剩余系中至少有一半的数使得同余式(1)不成立. 这就是说, 对于随机选取的整数$b,\ (b,n)=1$, 我们有50% 以上的机会来判断出n 是合数, 或者说n 是合数的可能性小于50% .

假设一个盒子内有N 个大小相同的球(如$N=2^{1024}$), 球的颜色为绿色和红色两种. 如果蓝球个数小于或等于红球个数, 则从盒子中随机取到蓝球的概率小于或等于$\frac{1}{2}$, 连续k 次取到蓝球的概率小于或等于$\frac{1}{2^k}$.

现在, 我们给出判断一个大奇整数n 为素数的方法:

1. 随机选取整数$b_1,\ 0 < b_1 < n$, 计算b_1 和n 的最大公因数$d_1 = (b_1, n)$.
2. 如果$d_1 > 1$, 则n 不是素数.
3. 如果$d_1 = 1$, 则计算$b_1^{n-1} \pmod n$, 看看同余式(1) 是否成立.
   - 如果不成立, 则n 不是素数.
   - 如果成立, 则n 是合数的可能性小于$\frac{1}{2}$ 或者说n是素数可能性大于$1 - \frac{1}{2}$.

重复上述步骤.

1. 再随机选取整数$b_2,\ 0 < b_2 < n$, 计算b_2 和n 的最大公因数$d_2 = (b_2, n)$.
2. 如果$d_2 > 1$, 则n 不是素数.
3. 如果$d_2 = 1$, 则计算$b_2^{n-1} \pmod n$, 看看同余式(1) 是否成立.
   - 如果不成立, 则n 不是素数.
   - 如果成立, 则n 是合数的可能性小于$\frac{1}{2^2}$ 或者说n是素数可能性大于$1 - \frac{1}{2^2}$.

继续重复上述步骤, . . . , 直至第t 步.

1. 随机选取整数$b_t,\ 0 < b_t < n$, 计算b_t 和n 的最大公因数$d_t = (b_t, n)$.
2. 如果$d_t > 1$, 则n 不是素数.
3. 如果$d_t = 1$, 则计算$b_t^{n-1} \pmod n$, 看看同余式(1) 是否成立.
   - 如果不成立, 则n 不是素数.
   - 如果成立, 则n 是合数的可能性小于$\frac{1}{2^t}$ 或者说n是素数可能性大于$1 - \frac{1}{2^t}$.

上述过程也可简单归纳为:

Fermat 素性检验

给定奇整数$n \geq 3$ 和安全参数t.

1. 随即选取整数$b,\ (b, n) = 1,\ 2 \leq b \leq n - 2$;
2. 计算$r = b^{n-1} \pmod n$;
3. 如果$r \neq 1$, 则n 是合数.
4. 上述过程重复t 次.

6.1.2 无穷多伪素数

本节讨论伪素数的存在性.

引理6.1.1 设d, n 都是正整数. 如果d 能整除n, 则2^d-1 能整除2^n-1.

证 因为$d \mid n$, 所以存在一个整数q 使得$n = q \cdot d$. 因此, 我们有

$$2^n - 1 = (2^d)^q - 1 = ((2^d)^{q-1} + (2^d)^{q-2} + \cdots + 2^d + 1)(2^d - 1).$$

故$2^d - 1 \mid 2^n - 1$. 证毕

定理6.1.2 存在无穷多个对于基2 的伪素数.

证 (I) 我们证明: 如果n 是对于基2 的伪素数, 则$m = 2^n - 1$ 也是对于基2 的伪素数. 事实上, 因为n 是对于基2 的伪素数, 所以n 是奇合数, 并且$2^{n-1} \equiv 1 \pmod{n}$. 由于$n$ 是奇合数, 所以我们有因数分解式$n = q \cdot d$, $1 < d < n, 1 < q < n$. 根据引理, 我们得到$2^d - 1 \mid 2^n - 1$. 因此$m = 2^n - 1$ 是合数.

现在验证:

$$2^{m-1} \equiv 1 \pmod{m}.$$

因为$2^{n-1} \equiv 1 \pmod{n}$, 所以我们可以将$m-1 = 2(2^{n-1}-1)$ 写成$m-1 = kn$. 根据引理, 我们得到$2^n - 1 \mid 2^{m-1} - 1$. 因此, 同余式

$$2^{m-1} \equiv 1 \pmod{m}$$

成立. 故$m = 2^n - 1$ 是对于基2 的伪素数.

(II) 取n_0 为对于基2 的一个伪素数, 例如$n_0 = 341$ 是一个对于基2 的伪素数. 再令

$$n_1 = 2^{n_0} - 1,\ n_2 = 2^{n_1} - 1,\ n_3 = 2^{n_2} - 1,\ \ldots.$$

根据结论(I), 这些整数都是对于基2 的伪素数. 证毕

5.1.3 平方因子的判别

因为判断n 是否有平方因子是产生大素数或作因数分解的重要步骤之一, 所以我们给出相关的结论:

定理6.1.3 设n 是一个有平方因子的整数. 则存在整数$b,\ (b,n)=1$ 使得同余式(1) 不成立, 即 $b^{n-1}\not\equiv 1\ (\mathrm{mod}\ n)$

证 (i) 反证法. 设对所有的正整数$b,\ (b,n)=1$, 都有同余式

$$b^{n-1}\equiv 1\ (\mathrm{mod}\ n)$$

成立. 根据定理假设, 存在一个素数幂$p^\alpha,\ \alpha\geq 2$, 使得$n=p^\alpha\cdot n',\ (n',p)=1$. 根据定理5.2.4, 存在$g$ 使得g 是模p^α 原根, 即 $\mathrm{ord}_{p^\alpha}(g)=p^{\alpha-1}(p-1)$.

现在中国剩余定理, 可求得$x\equiv b\ (\mathrm{mod}\ n)$ 满足: $\begin{cases} x\equiv g\ (\mathrm{mod}\ p^\alpha),\\ x\equiv 1\ (\mathrm{mod}\ n'). \end{cases}$

这时, 我们有$(b,n)=1$ 以及

$$\mathrm{ord}_{p^\alpha}(b)=\mathrm{ord}_{p^\alpha}(g)=p^{\alpha-1}(p-1).$$

因为 $b^{n-1}\equiv 1\ (\mathrm{mod}\ n)$, 所以 $b^{n-1}\equiv 1\ (\mathrm{mod}\ p^\alpha)$. 根据定理5.1.1, 得到

$$\mathrm{ord}_{p^\alpha}(b)\mid n-1 \quad 或 \quad p^{\alpha-1}(p-1)\mid n-1.$$

因此, $p\mid n-1$. 这不可能. 证毕

5.1.4 Carmicheal 数

本节讨论使得Fermat 素性检验算法无效的整数.

定义6.1.2 合数n 称为**Carmichael** 数, 如果对所有的正整数$b,\ (b,n)=1,$ 都有同余式

$$b^{n-1}\equiv 1\ (\mathrm{mod}\ n)$$

成立.

注 Carmichael 数n 也可解释为这样一个正合数n, 它使得: 对所有的正整数$b,\ (b,n)=1, n-1$ 都是序列$u=\{u_k=b^k\ \mod\ n \mid k\geq 1\}$ 的周期.

例6.1.6 整数$561=3\cdot 11\cdot 17$ 是一个Carmichael 数.

证 如果$(b,561)=1$, 则$(b,3)=(b,11)=(b,17)=1$. 根据Fermat 小定理, 有

$$b^2\equiv 1\ (\mathrm{mod}\ 3),\quad b^{10}\equiv 1\ (\mathrm{mod}\ 11),\quad b^{16}\equiv 1\ (\mathrm{mod}\ 17).$$

从而,
$$\begin{cases} b^{560}\equiv (b^2)^{280}\equiv 1 \pmod 3,\\ b^{560}\equiv (b^{10})^{56}\equiv 1 \pmod{11},\\ b^{560}\equiv (b^{16})^{35}\equiv 1 \pmod{17}. \end{cases}$$

因此, 我们有 $b^{560}\equiv 1\ (\mathrm{mod}\ 561).$

定理6.1.4 n 是一个奇合数.

(i) 如果n 被一个大于1 平方数整除, 则n 不是Carmichael 数.

(ii) 如果$n = p_1 \cdots p_k$ 是一个无平方数, 则n 是Carmichael 数的充要条件是

$$p_i - 1 \mid n - 1, \quad 1 \le i \le k.$$

证 (i) 由定理6.1.3 得到. (ii) 设$n = p_1 \cdots p_k$ 是一个无平方数.

充分性. 设有正整数$b,\ (b, n) = 1$, 则$(b, p_i) = 1,\ 1 \le i \le k$. 我们有

$$b^{p_i - 1} \equiv 1 \pmod{p_i}, \quad 1 \le i \le k.$$

进而 $b^{n-1} \equiv \left(b^{p_i-1}\right)^{\frac{n-1}{p_i-1}} \equiv 1 \pmod{p_i},\ 1 \le i \le k$. 这说明$n$ 是Carmichael 数.

必要性. 设n 是Carmichael 数. 则对所有的正整数$b,\ (b, n) = 1$, 都有同余式

$$b^{n-1} \equiv 1 \pmod{n}.$$

固定$i,\ 1 \le i \le k$, 并设g_i 是模p_i 原根, 则存在b_i满足 $\begin{cases} x \equiv g_i \pmod{p_i}, \\ x \equiv 1 \pmod{\dfrac{n}{p_i}}. \end{cases}$

这时, $(b_i, n) = 1$, 且 $b_i^{n-1} \equiv 1 \pmod{n}$. 进而, $b_i^{n-1} \equiv 1 \pmod{p_i}$.

这意味着 $\mathrm{ord}_{p_i}(b_i) \mid n - 1$ 或 $p_i - 1 \mid n - 1$. 证毕

定理6.1.5 每个Carmichael 数是至少三个不同素数的乘积.

证 (i) 反证法. 假设有一个Carmichael 数n, 其可以表示为两个素数的乘积. 不妨设$n = p \cdot q,\ p < q$. 根据定理6.1.4 (ii), 我们有$n - 1 \equiv 0 \pmod{q-1}$. 从而,

$$p - 1 = n - 1 - p(q-1) \equiv 0 \pmod{q-1}.$$

这不可能. 因此, 每个Carmichael 数是至少三个不同素数的乘积. 证毕

注: 1. 存在无穷多个Carmichael 数.

2. 当n 充分大时, 区间$[2, n]$ 内的Carmichael 数的个数$\geq n^{2/7}$.

6.2 Euler 伪素数

6.2.1 Euler 伪素数 Solovay-Stassen 素性检验

设n 是奇素数. 根据定理4.3.1, 对任意整数b 成立, 有同余式

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$$

因此, 如果存在整数b, $(b,n)=1$, 使得

$$b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) \pmod{n},$$

则n 不是一个素数.

例6.2.1 设$n=341$, $b=2$. 我们分别计算得到:

$$2^{\frac{341-1}{2}} \equiv 1 \pmod{341} \quad \text{以及} \quad \left(\frac{2}{341}\right) = (-1)^{\frac{341^2-1}{8}} = -1,$$

因为 $2^{\frac{341-1}{2}} \not\equiv \left(\frac{2}{341}\right) \pmod{341}$. 所以341 不是一个素数.

定义6.2.1 设n 是一个正奇合数. 设整数b 与n 互素. 如果整数n 和b 满足条件:

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}, \tag{2}$$

则n 叫做对于基b 的**Euler 伪素数**.

例6.2.2 设$n = 1105,\ b = 2$. 我们分别计算得到:

$$2^{\frac{1105-1}{2}} \equiv 1 \pmod{1105} \quad \text{以及} \quad \left(\frac{2}{1105}\right) = (-1)^{\frac{1105^2-1}{8}} = 1.$$

因为

$$2^{\frac{1105-1}{2}} \equiv \left(\frac{2}{1105}\right) \pmod{1105},$$

所以1105 是一个对于基2 的Euler 伪素数.

例6.2.3 设$n = 11 \cdot 31 = 341$. 求出所有整数b, $1 \le b \le n-1$ 使得n 是对于基b 的Euler-伪素数.

解 $\varphi(n) = 300$. 使得n 是对于基b 的伪素数的b 有97 个. 概率为$\frac{97}{300}$. 这些b 为

$$
\begin{array}{rcccccccccc}
b = & 1, & 2*, & 4, & 8*, & 15*, & 16, & 23*, & 27*, & 29, & 30, \\
& 32*, & 35*, & 39*, & 46, & 47, & 54, & 58*, & 60*, & 61, & 63*, \\
& 64, & 70, & 78, & 85, & 89*, & 91*, & 92*, & 94*, & 95*, & 97, \\
& 101*, & 108*, & 109*, & 116, & 120, & 122*, & 123, & 125, & 126, & 128*, \\
& 139, & 140*, & 147*, & 151, & 153, & 156*, & 157, & 159, & 163, & 170*, \\
& 171*, & 178, & 182, & 184, & 185*, & 188, & 190, & 194*, & 201*, & 202, \\
& 213*, & 215, & 216, & 218, & 219*, & 221, & 225, & 232*, & 233*, & 240*, \\
& 244, & 246*, & 247*, & 249*, & 250*, & 252*, & 256, & 263, & 271, & 277, \\
& 278*, & 280, & 281*, & 283*, & 287, & 294, & 295, & 302*, & 306*, & 309*, \\
& 311, & 312, & 314*, & 318*, & 325, & 326*, & 333*, & 337, & 339*, & 340
\end{array}
$$

其中未标注$*$ 号的数b 使得n 是对于基b 的Euler 伪素数. 共有50 个. 概率为$\frac{50}{300}$.

b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$
1	1	1	11	242	0	21	56	1	31	155	0	41	56	-1
$2*$	1	-1	12	67	-1	22	242	0	$32*$	1	-1	42	56	-1
3	67	-1	13	56	1	$23*$	1	-1	33	187	0	43	67	1
4	1	1	14	67	1	24	67	1	34	67	-1	44	242	0
5	56	1	$15*$	1	-1	25	67	1	$35*$	1	-1	45	67	1
6	67	1	16	1	1	26	56	-1	36	56	1	46	1	1
7	67	-1	17	67	1	$27*$	1	-1	37	67	-1	47	1	1
$8*$	1	-1	18	56	-1	28	67	-1	38	67	1	48	67	-1
9	56	1	19	67	-1	29	1	1	$39*$	1	-1	49	56	1
10	56	-1	20	56	1	30	1	1	40	56	-1	50	67	-1

b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$
51	56	-1	61	1	1	71	56	1	81	67	1	91∗	1	-1
52	56	1	62	155	0	72	56	-1	82	56	1	92∗	1	-1
53	56	-1	63∗	1	-1	73	56	1	83	56	1	93	155	0
54	1	1	64	1	1	74	67	1	84	56	1	94∗	1	-1
55	253	0	65	67	1	75	56	-1	85	1	1	95∗	1	-1
56	67	1	66	187	0	76	67	-1	86	67	-1	96	67	1
57	56	1	67	56	1	77	187	0	87	67	-1	97	1	1
58∗	1	-1	68	67	1	78	1	1	88	242	0	98	56	-1
59	67	1	69	67	1	79	67	1	89∗	1	-1	99	253	0
60∗	1	-1	70	1	1	80	56	1	90	67	-1	100	67	1

b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$
101∗	1	−1	111	56	1	121	253	0	131	67	−1	141	67	−1
102	56	1	112	67	−1	122∗	1	−1	132	187	0	142	56	−1
103	56	1	113	56	1	123	1	1	133	56	1	143	253	0
104	56	−1	114	56	−1	124	155	0	134	56	−1	144	56	1
105	67	1	115	56	−1	125	1	1	135	56	−1	145	56	1
106	56	1	116	1	1	126	1	1	136	67	−1	146	56	−1
107	67	−1	117	67	1	127	67	1	137	56	−1	147∗	1	−1
108∗	1	−1	118	67	−1	128∗	1	−1	138	67	−1	148	67	−1
109∗	1	−1	119	56	−1	129	56	−1	139	1	1	149	67	−1
110	253	0	120	1	1	130	67	−1	140∗	1	−1	150	56	1

b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$
151	1	1	161	67	1	171∗	1	−1	181	56	−1	191	56	1
152	67	1	162	67	−1	172	67	1	182	1	1	192	67	−1
153	1	1	163	1	1	173	56	−1	183	67	−1	193	67	−1
154	187	0	164	56	−1	174	67	1	184	1	1	194∗	1	−1
155	155	0	165	242	0	175	56	−1	185∗	1	−1	195	56	−1
156∗	1	−1	166	56	−1	176	242	0	186	155	0	196	56	1
157	1	1	167	67	1	177	56	−1	187	187	0	197	56	1
158	67	−1	168	56	−1	178	1	1	188	1	1	198	253	0
159	1	1	169	67	1	179	67	−1	189	67	1	199	56	−1
160	56	−1	170∗	1	−1	180	67	1	190	1	1	200	67	−1

b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$
201∗	1	−1	211	67	−1	221	1	1	231	253	0	241	67	1
202	1	1	212	56	−1	222	56	−1	232∗	1	−1	242	253	0
203	67	−1	213∗	1	−1	223	67	−1	233∗	1	−1	243	56	−1
204	56	−1	214	67	1	224	67	1	234	67	−1	244	1	1
205	67	−1	215	1	1	225	1	1	235	56	1	245	67	1
206	56	−1	216	1	1	226	56	−1	236	67	1	246∗	1	−1
207	56	−1	217	155	0	227	56	−1	237	56	−1	247∗	1	−1
208	56	1	218	1	1	228	56	1	238	56	1	248	155	0
209	187	0	219∗	1	−1	229	67	−1	239	56	1	249∗	1	−1
210	67	−1	220	253	0	230	56	1	240∗	1	−1	250∗	1	−1

b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$
251	67	-1	261	56	1	271	1	1	281*	1	-1	291	67	-1
252*	1	-1	262	67	1	272	67	1	282	67	1	292	56	1
253	242	0	263	1	1	273	67	1	283*	1	-1	293	67	-1
254	67	-1	264	187	0	274	56	1	284	56	1	294	1	1
255	67	-1	265	67	-1	275	187	0	285	67	1	295	1	1
256	1	1	266	56	-1	276	67	1	286	253	0	296	67	1
257	56	1	267	67	1	277	1	1	287	1	1	297	242	0
258	56	1	268	56	1	278*	1	-1	288	56	-1	298	67	1
259	56	1	269	56	-1	279	155	0	289	56	1	299	56	-1
260	67	1	270	56	1	280	1	1	290	56	-1	300	56	-1

b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$	b	$b^{\frac{n-1}{2}}$	$(\frac{b}{n})$
301	56	-1	311	1	1	321	56	1	331	56	-1
302$*$	1	-1	312	1	1	322	67	-1	332	56	1
303	67	1	313	67	-1	323	56	-1	333$*$	1	-1
304	67	-1	314$*$	1	-1	324	67	1	334	67	-1
305	56	1	315	56	-1	325	1	1	335	67	1
306$*$	1	-1	316	67	1	326$*$	1	-1	336	56	1
307	67	-1	317	67	1	327	67	1	337	1	1
308	187	0	318$*$	1	-1	328	56	1	338	67	-1
309$*$	1	-1	319	242	0	329	67	-1	339$*$	1	-1
310	155	0	320	56	1	330	242	0	340	1	1

Solovay-Stassen 素性检验

给定奇整数$n \geq 3$和安全参数t.

1. 随即选取整数b, $2 \leq b \leq n-2$;
2. 计算$r = b^{\frac{n-1}{2}} \pmod{n}$;
3. 如果$r \neq 1$以及$r \neq n-1$, 则n是合数.
4. 计算Jacobi 符号$s = \left(\frac{b}{n}\right)$;
5. 如果$r \neq s$, 则n是合数.
6. 上述过程重复t次.

6.2.2 无穷多Euler 伪素数

定理6.2.1 如果n 是对于基b 的Euler 伪素数, 则n 是对于基b 的伪素数.

证 设n 是对于基2 的Euler 伪素数, 则我们有

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}.$$

上式两端平方, 并注意到$\left(\frac{b}{n}\right) = \pm 1 \pmod{n}$, 我们有

$$b^{n-1} \equiv (b^{\frac{n-1}{2}})^2 \equiv \left(\frac{b}{n}\right)^2 \equiv 1 \pmod{n},$$

因此, n 是对于基b 的伪素数. 证毕

定理6.2.1 的逆不成立, 即不是每个伪素数都是Euler 伪素数. 例如: 341 是对于基2 的伪素数, 但不是对于基2 的Euler 伪素数.

6.3 强伪素数

6.3.1 强伪素数 Miller-Rabin 素性检验

设n 是奇素数, 并且有$n-1=2^s t$, 则我们有如下因数分解式:

$$b^{n-1}-1=(b^{2^{s-1}t}+1)(b^{2^{s-2}t}+1)\cdots(b^t+1)(b^t-1).$$

因此, 如果有同余式

$$b^{n-1}\equiv 1 \pmod{n},$$

则如下同余式至少有一个成立:

$$\begin{aligned} b^t &\equiv 1 \pmod{n},\\ b^t &\equiv -1 \pmod{n},\\ b^{2t} &\equiv -1 \pmod{n},\\ &\vdots\\ b^{2^{s-1}t} &\equiv -1 \pmod{n}. \end{aligned}$$

由此得到: 如果有整数b 使得

$$\begin{cases} b^t \not\equiv 1 \pmod{n}, \\ b^t \not\equiv -1 \pmod{n}, \\ b^{2t} \not\equiv -1 \pmod{n}, \\ \vdots \\ b^{2^{s-1}t} \not\equiv -1 \pmod{n}, \end{cases}$$

则n 是合数.

在计算$b^{n-1} \pmod{n}$ 时, 通常要运用模重复平方法, 这时, 计算次序为:

$$b^t \pmod{n} \to b^t \pmod{n} \to (b^t)^2 \pmod{n} \to \ldots \to (b^t)^{2^{s-1}} \pmod{n}.$$

这意味着如下的素性检验方法比费马素性检验的效果要好些.

定义6.3.1 设n 是一个奇合数, 且有表示式$n-1=2^s t$, 其中t为奇数. 设整数b 与n 互素. 如果整数n 和b 满足条件:

$$b^t \equiv 1 \pmod{n},$$

或者存在一个整数$r,\ 0 \le r < s$ 使得

$$b^{2^r t} \equiv -1 \pmod{n},$$

则n 叫做对于基b 的**强伪素数**.

例6.3.1 整数$n = 2047 = 23 \cdot 89$ 是对于基$b = 2$ 的强伪素数.

解 因为

$$2^{2046/2} \equiv (2^{11})^{93} \equiv (2048)^{93} \equiv 1 \pmod{2047},$$

所以整数2047 是对于基$b = 2$ 的强伪素数.

Miller-Rabin 素性检验

给定奇整数$n \geq 3$和安全参数k.

写$n-1=2^s t$, 其中t为奇整数.

1. 随机选取整数b, $2 \leq b \leq n-2$;

2. 计算$r_0 \equiv b^t \pmod{n}$;

3. a) 如果$r_0 = 1$或$r_0 = n-1$, 则通过检验, 可能为素数. 回到1. 继续选取另一个随机整数b, $2 \leq b \leq n-2$;

b) 否则, 有$r_0 \neq 1$以及$r_0 \neq n-1$, 我们计算$r_1 \equiv r_0^2 \pmod{n}$;

4. a) 如果$r_1 = n-1$, 则通过检验, 可能为素数. 回到1. 继续选取另一个随机整数b, $2 \leq b \leq n-2$;

b) 否则, 有$r_1 \neq n-1$, 我们计算$r_2 \equiv r_1^2 \pmod{n}$;

如此继续下去,

s+2. a) 如果$r_{s-1} = n-1$, 则通过检验, 可能为素数. 回到1. 继续选取另一个随机整数b, $2 \leq b \leq n-2$;

b) 否则, 有$r_{s-1} \neq n-1$, n为合数.

6.3.2 无穷多强伪素数

定理6.3.2 存在无穷多个对于基2 的强伪素数.

证 i) 我们证明: 如果n 是对于基2 的伪素数, 则$m = 2^n - 1$ 是对于基2 的强伪素数. 事实上, 因为n 是对于基2 的伪素数, 所以n 是奇合数, 并且$2^{n-1} \equiv 1 \pmod{n}$. 由此得到$2^{n-1} - 1 = nk$ 对某整数k, 进一步, k 是奇数. 我们有

$$m - 1 = 2^n - 2 = 2(2^{n-1} - 1) = 2^1 nk,$$

这是$m - 1$分解为2 的幂和奇数乘积的表达式.

注意到$2^n = (2^n - 1) + 1 = m + 1 \equiv 1 \pmod{m}$, 我们有

$$2^{(m-1)/2} \equiv 2^{nk} \equiv (2^n)^k \equiv 1 \pmod{m}.$$

此外, 在定理6.3.1 的证明中, 我们知道: n 是合数时, m 也是合数. 故m 是对于2 的强伪素数.

ii) 因为对于基2 的伪素数n 产生一个对于基的强伪素数$2^n - 1$, 而且存在无穷多个对于基2 的伪素数, 所以存在无穷多个对于基2 的伪素数. 证毕

定理6.3.2 如果n 是对于基b 的强伪素数, n 是对于基b 的Euler 伪素数.

定理6.3.3 设是一个奇合数. 则n 是对于基b, $1 \leq b \leq n-1$, 的强伪素数的可能性至多为25%.

例6.3.2 设$n = 63$. 求出所有整数b, $1 \leq b \leq n-1$ 使得n 是对于基b 的强伪素数.