# 超强伪素数及素性检验加速算法*

王 泽 辉
（中山大学 科学计算与计算机应用系，广东 广州 510275）

摘 要：提出超强伪素数的概念，并构造超强伪素数检测算法 HSP（$n$, $h$），可将目前应用最广泛的素性检测算法 Miller-Rabin 算法的出错率 1/4 大为改善，可证明对一个子类 HSP（$n$, $h$）出错率降为 1/30；且只需对后者增加 $O(\log_2 n)$ 次乘法，便可重复作 $m$ 次检测，从而达到素性加速检验，可用来生成大素数。

关键词：超强伪素数；素性检测；平方时间复杂性；大素数生成
中图分类号：O157.4 文献标识码：A 文章编号：0529-6579（2004）02-0025-05

现代密码体制如 RSA 体制的建立，需要生成若干满足要求的大素数作为密匙[1]，其基础工作是对随机整数进行素性检验，素性检测不存在多项式时间的确定型判断算法，目前应用最广泛的 Miller-Rabin 算法（简称 M-R 算法）是概率型算法，M-R 算法把合数误认为素数的出错率为 1/4，本文将其出错率降低，甚至大大降低。

## 1 素数模的高阶同余方程若干特性

本文中设 **N**、**Z** 分别为正整数集、整数集，$\wedge$ 为幂运算，$a \wedge b = a^b$；$QR_n$ 与 $NQR_n$ 分别为模 $n$ 的二次剩余集和二次非剩余集，$(p, q)$ 是 $p$、$q$ 的最大公约数，将 $\log_2 n$ 简记为 $\log n$；$A \equiv B$ 均为 $A \equiv B \pmod n$ 的简记；对 $\forall s$ 定义

$$\Delta_s(x) = \sum_{i=0}^{2s} x^i, \quad \Gamma_s(x) = \sum_{i=0}^{2s} (-1)^i x^i$$

定义 1 设 $n, b, r, L \in \mathbf{N}$，$n-1 = 2^r \times L$，$2 \nmid L$，$r > 0$，$b$ 与 $n$ 互素，如

$$b^L \equiv 1 \pmod n \tag{1}$$

或 $\exists t, 0 \leqslant t < r$，使

$$b \wedge (2^t \times L) \equiv -1 \pmod n \tag{2}$$

则称 $n$ 是以 $b$ 为基、宽度 $h = 2$ 的超强伪素数，在（1）、（2）式成立时分别记为 $n \in \mathrm{HSP}(2, b^+, 0)$ 与 $n \in \mathrm{HSP}(2, b^-, t)$。

易知 $h = 2$ 的超强伪素数即是原来意义上的强伪素数。

定理 1 设 $n$ 为奇素数，$n-1 = 2^r \times L$，$2 \nmid L$，$r > 0$，$L = (p_1 \wedge u_1)(p_2 \wedge u_2)\cdots(p_m \wedge u_m)L_0$，其中 $p_1 < p_2 < \cdots < p_m$ 为前 $m$ 个奇素数，$p_i \nmid L_0$，$i = 1, 2, \cdots, m$；至少有一个 $u_j \geqslant 1$，$1 \leqslant j \leqslant m$，$si = (p_i - 1)/2$。

（1）当 $n \in \mathrm{HSP}(2, b^+, 0)$ 时，如 $u_i \geqslant 1$，记 $L = (p_i \wedge u_i)L_i$，$B_i = b \wedge L_i$。那么，或者 $B_i \equiv 1 \pmod n$，或者 $\exists J_i, 0 \leqslant J_i < u_i$，使 $\Delta_{si}[B_i \wedge (p_i \wedge J_i)] \equiv 0 \pmod n$；

（2）当 $n \in \mathrm{HSP}(2, b^-, t)$ 时，如 $u_i \geqslant 1$，记 $L = (p_i \wedge u_i)L_i$，$B_i = b \wedge (2^t \times L_i)$。那么，或者 $B_i \equiv -1 \pmod n$，或者 $\exists J_i, 0 \leqslant J_i < u_i$，使 $\Gamma_{si}[B_i \wedge (p_i \wedge J_i)] \equiv 0 \pmod n$；结论对所有 $i = 1, 2, \cdots m$ 均成立。

证明 由 $n \in \mathrm{HSP}(2, b^+, 0)$ 时，$b^L - 1 = B_i \wedge (p_i \wedge u_i) - 1 = (B_i - 1)\Delta_{si}(B_i)\Delta_{si}(B_i \wedge p_i)\cdots\Delta_{si}(B_i \wedge (p_i \wedge (u_i - 1))) \equiv 0 \pmod n$，得证，类似可证（2），证毕。

$n$ 为奇数时可分为 $n \equiv 3 \pmod 4$ 与 $n \equiv 1 \pmod 4$ 两类，$n \equiv 1 \pmod 4$ 又可分为 $n \equiv 5 \pmod 8$ 与 $n \equiv 1 \pmod 8$ 两个子类；下面指出：

当 $n \equiv 3 \pmod 4$ 及 $n \equiv 5 \pmod 8$ 时，仅需要作 $O(\log n)$ 次乘法便可求得 $\Delta_1(x) \equiv 0 \pmod n$，$\Delta_2(x) \equiv 0 \pmod n$，$\Gamma_1(x) \equiv 0 \pmod n$，$\Gamma_2(x) \equiv 0 \pmod n$ 在模 $n$ 意义下的所有解。

引理 1 设 $n$ 为奇素数，$m \in \mathbf{N}$，$c \in \mathbf{Z}$，$m \mid (n-1)$，则同余方程

$$x^m \equiv c \pmod n \tag{3}$$

有解的充要条件为 $c^{(n-1)/m} \equiv 1 \pmod n$，且有解时（3）式有 $m$ 个模 $n$ 不同的解（简称 $m$ 个解）。

推论 1 设 $n$ 为奇素数，$c = \pm 1$，$m = 2s + 1 \in \mathbf{N}$，$s \geqslant 1$，$m < n$；则当 $m \mid (n-1)$ 时（3）式有 $m = 2s + 1$ 个解，且

* 收稿日期：2003-11-24
作者简介：王泽辉（1963 年生），男，副教授；E-mail：info@gdcts.com

(1) 如 $c=+1$, 则同余方程

$$\Delta_s(x)=\sum_{i=0}^{2s}x^i\equiv 0(\bmod n)$$

有且仅有 $2s$ 个解, 记为 $x\equiv x_j^+(\bmod n)$, $j=1,2,\cdots 2s$, 连同 $x\equiv x_m^+(\bmod n)$ ($x_m^+=1$), 共同构成(3)式之全部解。

(2) 如 $c=-1$, 则同余方程

$$\Gamma_s(x)=\sum_{i=0}^{2s}(-1)^i x^i\equiv 0(\bmod n)$$

有且仅有 $2s$ 个解, 记为 $x\equiv x_j^-(\bmod n)$, $j=1,2,\cdots 2s$, 连同 $x\equiv x_m^-(\bmod n)$ ($x_m^-=-1$), 共同构成(3)式之全部解。而 $x_j^-\equiv -x_j^+(\bmod n)$。

证明 由引理1, 及 $x^{2s+1}-1=(x-1)\times\Delta_s(x)$, $x^{2s+1}+1=(x+1)\times\Gamma_s(x)$ 易证(1), (2)。令 $z=-x$, 则 $\Gamma_s(z)=\Delta_s(x)$, 故 $x_j^-\equiv -x_j^+(\bmod n)$, 证毕。

引理2 采用著名的平方-乘算法计算 $x^k(\bmod n)$, 至多需要 $2\lfloor\log k\rfloor+2$ 次乘法。引理1、引理2的证明见文[4, 2]。

引理3 设 $n$ 为奇素数, $c\in \underline{QR}_n$, 则二次同余方程

$$x^2\equiv c(\bmod n)\qquad(4)$$

之解 $x_0$ 可表示为:

(1) $n\equiv 3(\bmod 4)$ 时, $x_0=\pm c^{k+1}(\bmod n)$, $k=(n-3)/4$;

(2) $n\equiv 5(\bmod 8)$ 时, $x_0=\pm 2^{3k+1}\times c^{k+1}(2^{2k+1}+c^{2k+1})(\bmod n)$, $k=(n-5)/8$; 求(4)之解至多做 $8\lfloor\log k\rfloor+O(1)$ 次乘法。

证明 $c\in \underline{QR}_n$ 时根据欧拉(Euler)判别法及 $-2\in \underline{NQR}n$, 分别将 $x_0$ 表达式代入可证(1), (2); 由引理2知至多做 $8\lfloor\log k\rfloor$ 次乘法可得 $x_0$, 证毕。

定理2 设 $n\in\mathbf{N}$, $3\mid(n-1)$,

(1) 当 $n\equiv 3(\bmod 4)$ 时, 令 $k=(n-3)/4$, $x_0=\pm(-3)^{k+1}(\bmod n)$;

(2) 当 $n\equiv 5(\bmod 8)$ 时, 令 $k=(n-5)/8$, $x_0=\pm 2^{3k+1}\times(-3)^{k+1}(2^{2k+1}+(-3)^{2k+1})(\bmod n)$;

取+或-使 $x_0$ 的非负最小剩余 $X_0$ 为奇数, 令

$$x_1^{++}=(X_0-1)/2,\ x_2^{++}=(-X_0-1)/2,$$
$$x_j^{--}=-x_j^{++},\ j=1,2\qquad(5)$$

那么, 当 $n$ 为奇素数时, $x\equiv x_j^{++}(\bmod n)$ ($j=1,2$) 为 $\Delta_1(x)=x^2+x+1\equiv 0(\bmod n)$ 之全部解;

$x\equiv x_j^{--}(\bmod n)$ ($j=1,2$) 为 $\Gamma_1(x)=x^2-x+1\equiv 0(\bmod n)$ 之全部解。

证明 由定理1, $3\mid(n-1)$ 时 $\Delta 1(x)\equiv 0$ 有解,

$$4\Delta_1(x)=4x^2+4x+4=(2x+1)^2+3\equiv 0,$$

所以 $-3\in \underline{QR}_n$, 再应用引理3可得 $x\equiv x_j^{++}(\bmod n)$ ($j=1,2$) 为 $\Delta_1(x)=x^2+x+1\equiv 0(\bmod n)$ 之全部解; 再由推论1, $x_j^{--}=-x_j^{++}$, 故 $x\equiv x_j^{--}(\bmod n)$ ($j=1,2$) 为

$$\Gamma_1(x)=x^2-x+1\equiv 0(\bmod n)$$

之全部解; 证毕。

定理3 设 $n\in\mathbf{N}$, $5\mid(n-1)$。

(1) 当 $n\equiv 3(\bmod 4)$ 时, 令 $k=(n-3)/4$, $t_0=\pm 5^{k+1}(\bmod n)$; 取+或-使 $t_0$ 的非负最小剩余 $T_0$ 为奇数, 令

$$t_1^{++}=(T_0-1)/2,\ t_2^{++}=(-T_0-1)/2,$$
$$x_{0,j}^{++}=\pm((t_j^{++})^2-4)^{k+1}(\bmod n),$$

取+或-使 $x_{0,j}^{++}$ 的非负最小剩余 $X_{0,j}^{++}$ 与 $t_j^{++}$ 有相同奇偶性。

(2) 当 $n\equiv 5(\bmod 8)$ 时, 令 $k=(n-5)/8$, $t_0=\pm 2^{3k+1}\times 5^{k+1}(2^{2k+1}+5^{2k+1})(\bmod n)$; 取+或-使 $t_0$ 的非负最小剩余 $T_0$ 为奇数, 令

$$t_1^{++}=(T_0-1)/2,\ t_2^{++}=(-T_0-1)/2,$$
$$x_{0,j}^{++}=\pm 2^{3k+1}\times((t_j^{++})^2-4)^{k+1}$$
$$[2^{2k+1}+((t_j^{++})^2-4)^{2k+1}](\bmod n),$$

取+或-使 $x_{0,j}^{++}$ 的非负最小剩余 $X_{0,j}^{++}$ 与 $t_j^{++}$ 有相同奇偶性。

然后对 (1), (2) 均令:

$$x_1^{++}=(x_{0,1}^{++}+t_1^{++})/2,$$
$$x_2^{++}=(-x_{0,1}^{++}+t_1^{++})/2,\ x_3^{++}=(x_{0,2}^{++}+t_2^{++})/2,$$
$$x_4^{++}=(-x_{0,2}^{++}+t_2^{++})/2,$$
$$x_j^{--}=-x_j^{++},\ j=1,2,3,4\qquad(6)$$

那么, 当 $n$ 为奇素数时, $x\equiv x_j^{++}(\bmod n)$ 为 $\Delta_2(x)=x^4+x^3+x^2+x+1\equiv 0(\bmod n)$ 之全部解;

$x\equiv x_j^{--}(\bmod n)$ 为 $\Gamma_2(x)=x^4-x^3+x^2-x+1\equiv 0(\bmod n)$ 之全部解。$j=1,2,3,4$。

证明 $n$ 为素数时, 满足 $0<x<n$ 之 $x$ 可逆, 令 $t=(x+x^{-1})$, 重复两次使用引理3可得结论, 证毕。

推论2 设 $n$ 为素数, 当 $n\equiv 3(\bmod 4)$ 或者 $n\equiv 5(\bmod 8)$ 时, 求出

$$\Delta_1(x)\equiv 0(\bmod n),\ \Gamma_1(x)\equiv 0(\bmod n)$$

全部解至多需要做 $8\lfloor\log k\rfloor+O(1)$ 次乘法, 求出

$$\Delta_2(x)\equiv 0(\bmod n),\ \Gamma_2(x)\equiv 0(\bmod n)$$

全部解至多需要做 $16\lfloor\log k\rfloor+O(1)$ 次乘法。

## 2 超强伪素数的概念及素性加速检验算法 HSP

定义2 设 $n$ 为奇素数, $n-1=2^r\times L$, $2\nmid L$,

$r>0$, $L=(p_1\wedge u_1)(p_2\wedge u_2)\cdots(p_m\wedge u_m)L_0$, 其中 $p_1=3<p_2=5<\cdots<p_m$ 为前 $m$ 个奇素数, $p_i\nmid L_0$, $i=1,2,\cdots,m$; 至少有一个 $u_j\geqslant 1$, $1\leqslant j\leqslant m$, $si=(p_i-1)/2$, $p_m\leqslant h$。

(1) 当 $n\in \mathrm{HSP}(2,b^+,0)$ 时, 如 $u_i\geqslant 1$, 记 $L=(p_i\wedge u_i)L_i$, $B_i=b\wedge L_i$。这时,

1) 当 $u_1\geqslant 1$ 时, 如果 $B_1\equiv 1(\mathrm{mod}\ n)$, 或者 $\exists J_1$, $0\leqslant J_1<u_1$, 使得

① 当 $n\equiv 3(\mathrm{mod}\ 4)$ 或者 $n\equiv 5(\mathrm{mod}\ 8)$ 时, $B_1\wedge(3\wedge J_1)\equiv x_j^+(\mathrm{mod}\ n)$, $j=1$ 或 $j=2$; $x_j^+$ 如 (5) 式所定义。

② 当 $n\equiv 1(\mathrm{mod}\ 8)$ 时, $\Delta_1[B_1\wedge(3\wedge J_1)]\equiv 0(\mathrm{mod}\ n)$ 成立;

2) 当 $u_2\geqslant 1$ 时, 如果 $B_2\equiv 1(\mathrm{mod}\ n)$, 或者 $\exists J_2$, $0\leqslant J_2<u_2$, 使得

① 当 $n\equiv 3(\mathrm{mod}\ 4)$ 或者 $n\equiv 5(\mathrm{mod}\ 8)$ 时, $\exists j\in\{1,2,3,4\}$ 使 $B_2\wedge(\wedge_2^j)\equiv x_j^{++}(\mathrm{mod}\ n)$ 成立, $x_j^{++}$ 如(6) 式所定义。

② 当 $n\equiv 1(\mathrm{mod}\ 8)$ 时, $\Delta_2[B_2\wedge(5\wedge J_2)]\equiv 0(\mathrm{mod}\ n)$ 成立;

3) 当 $u_i\geqslant 1$, $2<i\leqslant m$ 时, 如果 $B_i\equiv 1(\mathrm{mod}\ n)$, 或者 $\exists J_i$, $0\leqslant J_i<u_i$, 使 $\Delta_i[B_i\wedge(p_i\wedge J_i)]\equiv 0(\mathrm{mod}\ n)$ 成立;

那么称 $n$ 是以 $b$ 为基、宽度为 $h$ ($h>5$) 的超强伪素数, 记为 $n\in \mathrm{HSP}(h,b^+,0)$; 如仅 1) 成立则记 $n\in \mathrm{HSP}(3,b^+,0)$; 如仅 1), 2) 成立则记 $n\in \mathrm{HSP}(5,b^+,0)$

(2) 当 $n\in \mathrm{HSP}(2,b^-,t)$ 时, 如 $u_i\geqslant 1$, 记 $L=(p_i\wedge u_i)L_i$, $B_i=b\wedge(2^t\times L_i)$。这时,

1) 当 $u_1\geqslant 1$ 时, 如果 $B_1\equiv -1(\mathrm{mod}\ n)$, 或者 $\exists J_1$, $0\leqslant J_1<u_1$, 使得

① 当 $n\equiv 3(\mathrm{mod}\ 4)$ 或者 $n\equiv 5(\mathrm{mod}\ 8)$ 时, $B_1\wedge(3\wedge J_1)\equiv x_j^-(\mathrm{mod}\ n)$, $j=1$ 或 $j=2$; $x_j^-$ 如(5) 式所定义。

② 当 $n\equiv 1(\mathrm{mod}\ 8)$ 时, $\Gamma_1[B_1\wedge(3\wedge J_1)]\equiv 0(\mathrm{mod}\ n)$ 成立;

2) 当 $u_2\geqslant 1$ 时, 如果 $B_1\equiv -1(\mathrm{mod}\ n)$, 或者 $\exists J_2$, $0\leqslant J_2<u_2$, 使得

① 当 $n\equiv 3(\mathrm{mod}\ 4)$ 或者 $n\equiv 5(\mathrm{mod}\ 8)$ 时, $\exists j\in\{1,2,3,4\}$ 使 $B_2\wedge(5\wedge J_2)\equiv x_j^{--}(\mathrm{mod}\ n)$ 成立, $x_j^{--}$ 如(6) 式所定义。

② 当 $n\equiv 1(\mathrm{mod}\ 8)$ 时, $\Gamma_2[B_2\wedge(5\wedge J_2)]\equiv 0(\mathrm{mod}\ n)$ 成立;

3) 当 $u_i\geqslant 1$, $2<i\leqslant m$ 时, 如果 $B_i\equiv -1(\mathrm{mod}\ n)$, 或者 $\exists J_i$, $0\leqslant J_i<u_i$, 使 $\Gamma_{si}[B_i\wedge(p_i\wedge J_i)]\equiv 0(\mathrm{mod}\ n)$;

那么称 $n$ 是以 $b$ 为基、宽度为 $h$ ($h>5$) 的超强伪素数, 记为 $n\in \mathrm{HSP}(h,b^-,t)$; 如仅 1) 成立则记 $n\in \mathrm{HSP}(3,b^-,t)$; 如仅 1), 2) 成立则记 $n\in \mathrm{HSP}(5,b^-,t)$。

推论 3　当 $n$ 为素数时, 对任意整数 $h\geqslant 2$, 对任意与 $n$ 互素的正整数 $b$, 必有 $n\in \mathrm{HSP}(h,b^+,0)$, 或者存在非负整数 $t$, 使 $n\in \mathrm{HSP}(h,b^-,t)$。

据此可构造超强伪素数检测算法 HSP($n$, $h$)

(1) 按(5)、(6) 式定义计算 $x_j^+$, $x_j^-$ ($j=1,2$); $x_j^{++}$, $x_j^{--}$ ($j=1,2,3,4$)

(2) 设 $n-1=2^r\times L$, $2\nmid L$, $r>0$, $L=(p_1\wedge u_1)(p_2\wedge u_2)\cdots(p_m\wedge u_m)L_0$, 选取随机数 $b$, $0<b<n$, 调用 Miller-Rabin 检测算法 M-R($n$, $b$), 先计算 $b\wedge(L_0)=B_0$, 并保存 $B_0$, 再计算 $b^L(\mathrm{mod}\ n)$, 如 $n$ 通不过检测则不用做(3), 否则输出"$n\in \mathrm{HSP}(2,b^+,0)$" 或"$n\in \mathrm{HSP}(2,b^-,t)$"。

(3) 利用中间结果 $B_0$, 对 $n\in \mathrm{HSP}(2,b^+,0)$ 或 $n\in \mathrm{HSP}(2,b^-,t)$ 分别利用定义 2 进行素性检测, 如 $n\in \mathrm{HSP}(h,b^+,0)$ 或 $n\in \mathrm{HSP}(h,b^+,t)$ 则输出"$n$ 为素数", 否则输出"$n$ 为合数"。

一次性计算 $x_j^+$, $x_j^-$, $x_j^{++}$, $x_j^{--}$ 后, 可供 $m$ 次重复 HSP 检测使用, 仅需 $24\lfloor\log_2 n\rfloor+O(1)$ 次乘法。当 $n$ 为大整数时, 记 $2^r\times(p_1\wedge u_1)(p_2\wedge u_2)\cdots(p_m\wedge u_m)=n_0$ 为小整数, 经过繁琐推导知进行 $m$ 次重复的 HSP 检测只比 M-R 检测增加 $O(\log_2 n)+O(m\times n_0)$ 次乘法, 相当于增加 $O((\log_2 n)^2)$ 的基本运算, 或增加一个平方时间复杂度, 却能大大提高素性检测的准确率。

## 3　对 Miller-Rabin 检验出错率的改进部分证明

定义 3　如 $n$ 为奇的合数, $1<b<n$ 中能使 $n$ 是以 $b$ 为基的强伪素数或超强伪素数的基数 $b$ 的个数为 $K^*$, 则 $K^*$ 称为致伪基数, $K^*/n$ 称伪素数的基数比例, 也称出错(比) 率。

引理 4　当 $n$ 为强素数时, $K^*/n\leqslant 1/4$, Miller-Rabin 检测的出错率最高为 $1/4$。

限于篇幅, 下面仅对超强伪素数一个子类的基数比例做出估计。

定理 3　设 $n$ 为奇的合数, $n=pq$, $p$、$q$ 为素数, $n-1=2^r\times(3\wedge u_1)\times(5\wedge u_2)L_0$, $p-1$, $q-1$ 相应有分解式,

$$p-1=2^v\times(3\wedge v_1)(5\wedge v_2)l_1,$$

$$q-1=2^{w}\times(3\wedge w_1)(5\wedge w_2)l_2,$$
$$l_1\leqslant v_{1,2},\ l_2\leqslant w_{1,2}$$

那么在区间 $0<b<n$ 中,至多有 $1/[2\times 3\wedge(v_1+w_1)\times 5\wedge(v_2+w_2)]$ 个 $b$,使 $n$ 是超强伪素数($n\in$ HSP(5, $b^{+}$, 0) 或 $n\in$ HSP(5, $b^{+}$, $t$)) 的一个子类,即

$$b\wedge(L_0)\equiv 1(\mathrm{mod}\ n)$$

或

$$b\wedge(2^{t}\times L_0)\equiv -1(\mathrm{mod}\ n)\qquad(8)$$

成立,即对此子类基数比例

$K^{*}/n\leqslant 1/[2\times 3\wedge(v_1+w_1)\times 5\wedge(v_2+w_2)]$

且只要有一个 $3\mid p$ 或 $3\mid q$,及 $5\mid p$ 或 $5\mid q$,则基数比例 $K^{*}/n\leqslant 1/30$,即出错率最高为 1/30。

证明 因 $n=pq$, $p$、$q$ 是素数, $b\wedge(L_0)\equiv 1(\mathrm{mod}\ pq)$ 等价于

$$b\wedge(L_0)\equiv 1(\mathrm{mod}\ p),$$
$$b\wedge(L_0)\equiv 1(\mathrm{mod}\ q)\qquad(9)$$

根据高次同余方程解数定理[4], 使(9)式成立的 $b$ 的个数为

$$K_1^{*}=(L_0,p-1)\times(L_0,q-1)=$$
$$(L_0,2^{v}\times(3\wedge v_1)(5\wedge v_2)l_1)\times$$
$$(L_0,2^{w}\times(3\wedge w_1)(5\wedge w_2)l_2)=$$
$$(L_0,l_1)(L_0,l_2)\leqslant l_1\times l_2$$

而 $b\wedge 2^{t}\times L_0)\equiv -1(\mathrm{mod}\ n)$ 等价于

$$b\wedge(2^{t}\times L_0)\equiv -1(\mathrm{mod}\ p),$$
$$b\wedge(2^{t}\times L_0)\equiv -1(\mathrm{mod}\ q)\qquad(10)$$

(10)式仅对满足 $t<\min\{v,w\}=v$ 的 $t$ 有解,使(10)式成立的 $b$ 的总数为

$$K_2^{*}=(1+4+42+\cdots+4^{v-1})\times l_1\times l_2=$$
$$(4^{v}-1)/(4-1)\times l_1\times l_2$$

故使(8)式成立的 $b$ 的总数(即致伪基数 $K^{*}$)为

$$K^{*}=\left[1+\frac{4^{v}-1}{4-1}\right]l_1l_2=\left[\frac{2}{3}+\frac{1}{3}\times 4^{v}\right]l_1l_2$$

因为

$$n-1>\phi(n)=(p-1)(q-1)=$$
$$2^{v}3\wedge(v_1)5\wedge(v_2)l_1)(2^{w}3\wedge(w_1))5\wedge(w_2)l_2)=$$
$$2^{u+v}3\wedge(v_1+w_1)5\wedge(v_2+w_2)l_1l_2$$

所以

$$\frac{K^{*}}{n}\leqslant\frac{(2/3+1/3\times 4^{v})l_1l_2}{2^{v+v}3\wedge(v_1+w_1)5\wedge(v_2+w_2)l_1l_2}\leqslant$$
$$\left(\frac{1}{4}\times\frac{2}{3}+\frac{1}{3}\right)\times$$
$$3\wedge(-v_1-w_1)\times 5\wedge(-v_2-w_2)$$

所以

$$\frac{K^{*}}{n}\leqslant[2\times 3\wedge(v_1+w_1)\times 5\wedge(v_2+w_2)]^{-1}$$

如 $3\mid p$ 或 $3\mid q$ 则 $v_1+w_1\geqslant 1$,如 $5\mid p$ 或 $5\mid q$ 则 $v_2+w_2\geqslant 1$,这时有

$$K^{*}/n\leqslant 1/(2\times 3\times 5)=1/30$$

证毕。

注 当 $n$ 是多个不同素数的乘积时结论相同。

下面是在长整数范围内的部分强伪素数$\{n\}$,在执行 $h=11(m=4)$ 的HSP($n$, $h$)算法后的致伪基数$\{K^{*}\}$、基数比例$\{K^{*}/n\}$ 一览表(表1)。

数值试验表明,当 $n$ 为素数时, $n$ 总能通过HSP算法的检测,当 $n$ 为伪素数时,基数比例(出错概率)由M-R检测的1/4降到1/10以下,甚至1/100以下。在长整数范围通过50次HSP检测的数均是素数。

表1 素性检测HSP($n$, $h$)方法的出错率

Tab. 1 The error rate of prime test HSP($n$, $h$) method

| $n$ | 1039 | 1111 | 1271 | 1387 | 1891 | 2101 | 3281 | 4033 | 8911 | 15841 | 16531 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $K^{*}$ | 1 | 1 | 1 | 1 | 5 | 1 | 85 | 245 | 5 | 16 | 5 |
| $K^{*}/n$ | 0.00096 | 0.0009 | 0.00079 | 0.00072 | 0.0026 | 0.00048 | 0.0259 | 0.061 | 0.00056 | 0.0010 | 0.0003 |

参考文献:


[1] 王泽辉. 一大类大整数因子分解的新算法及对RSA密码体制的解密[J]. 中山大学学报(自然科学版), 2003, 42(5): 15-18.

[2] [加] DOUGLAS R S. 密码学原理与实践[M]. 第2版. 冯登国, 译. 北京: 电子工业出版社, 2003.

[3] 华罗庚. 数论导引[M]. 北京: 科学出版社, 1957.

[4] 潘承洞, 潘承彪. 初等数论[M]. 北京: 北京大学出版社, 1992.

[5] [美] Stsve Burenett, Stephen Paine. 密码工程实践指南[M]. 北京: 清华大学出版社, 2001.

[6] DAMGARD I, LANDROCK P, POMERANCE C. Average case error estimates for the strong probable prime test[C]. Mathematics of Computation, 1993.


(下转第32页)

当狭窄尺寸（狭窄高度与狭窄长度）一定时，雷诺数越大，流动越容易产生分离。由于在生理条件下，流动分离区域中的动力学参数可能会直接或间接导致血管壁发生病变，所以如果能使狭窄附近的流动避免出现分离现象，这样对于防止动脉粥样硬化的形成颇为重要。

参考文献：

[1] SIOUFFI M, DEPLANO V, PELISSIER R. Experimental analysis of unsteady flows through a stenosis[J]. J Biomech, 1998, 31: 11—19.

[2] DEPLANO V, SIOUFFI M. Experimental and numerical study of pulsatile flows through stenosis: Wall shear stress analysis[J]. J Biomech, 1999, 32: 1081—1090.

[3] ZENDEHBUDI G R, MOAYERI M S. Comparison of physiological and simple pulsatile flows through stenosed arteries[J]. J Biomech, 1999, 32: 959—965.

[4] LONG Q, XU X Y, RAMNARINE K V, et al. Numerical investigation of physiologically realistic pulsatile flow through aterial stenosis[J]. J Biomech, 2001, 34: 1229—1242.

[5] BERTOLOTTI C, DEPLANO V. Three-dimensional numerical simulations of flow through a stenosed coronary bypss[J]. J Biomech, 2000, 33: 1011—1022.

[6] MOAYERI M S, ZENDEHBUDI G R. Effects of elastic property of the wall on flow characteristics through arterial stenoses[J]. J Biomech, 2003, 36: 525—535.

## Effect of the Poiseuille Flow Through the Stenosed Arteries on Wall Shear Stress

*LIU Guo-tao, WANG Xian-ju, AI Bao-quan, LIU Liang-gang*
(Department of Physics, Sun Yat-sen University, Guangzhou 510275, China)

**Abstract**: Poiseuille flow through the stenosed arteries is analyzed numerically and its effect on the flow field of stenosed region is studied. The incompressible Navier-Stokes equation is adopted to caleulate the flow field, and a finite difference scheme is used to implement the numerical analysis.

**Key words**: Poiseuille flow; stenosed artery; wall shear stress; numerical analysis

---

（上接第 28 页）

## Accelerating Computation Method for the Hypre-strong Pseudoprime and Prime Tests

*WANG Ze-hui*
(Department of Scientific Computation and Computer Science, Sun Yat-sen Univerity, Guangzhou 510275, China)

**Abstract**: The concept of hyper-strong pseudoprime, as well as the corresponding HSP ($n$, $h$) prime test algorithm, is proposed. It can decrease the error rate for the most extensively used prime test Miller-Rabin algorithm 1/4 to 1/30 for one sub-class, which can be repeated fom $m$ times test by increasing $O(\log_2 n)$ times multiplication. Thus, accelerating prime test method can be established and used to generate large prime.

**Key words**: hyper-strong pseudoprime; prime test; square of timing complexity; generation of large prime