Jacobi 和素性测定算法在 PC 上的实现*

Implementation of the Primality Testing Algorithm with Jacobi Sums on PCs

张振祥
Zhang Zhenxiang
(安徽师范大学数学系，芜湖，241000)
(Mathematics Department, Anhui Normal University, Wuhu, 241000)

摘 要 我们在 PC 机上实现了 Adleman-Pomerance-Rumely 的 Jacobi 和素性测定算法的 Cohen-Lenstra 版本。我们的 Pascal 程序在 486 微机上对 104 位素数的严格素性证明在 5 分钟内完成。特别地，我们证明了 $10^{103}+129$ 是素数。本文给出我们的程序对此数的严格素性证明所用的主要参数、一些中间数据和算法各步骤实际耗时。

ABSTRACT We have implemented the Cohen-Lenstra versoin of the Adleman-Pomerance-Rumely primality test with Jacobi sums on PCs. With our Pascal program, a rigorous proof for primality of a 104-digit prime can be done within five minutes on a PC486. Especially we have proved that $10^{103}+129$ is prime. In this report we give some main parameters we used for the proof of the primality of this number, some in termediate data and the running time for each step of the algorithm.

关键词 素性测定，Jacobi。
KEY WORDS primality test, Jacobi sums.

一、引 言

Adleman-Pomerance-Rumely 的 Jacobi 和素性测定算法[1]是一个严格素性证明算

* 收稿日期：1996 年 2 月 26 日。
作者简历：张振祥，1947 年出生，1970 年毕业于清华大学自动控制系，1981 年毕业于安徽师大代数研究班，1993 年获法国 Limoges 大学博士学位，现任副教授、客座教授，主要研究方向：计算数论及其应用。
通讯地址：241000 安徽芜湖市安徽师范大学数学系。

法，Cohen-H. W. Lenstra[2]从理论和算法上对此算法做了简化，Cohen-A. K. Lenstra[3]详细描述了此算法的实现，他们在巨型机 CDC Cyber 170/750 上完成一个 213 位(十进制，全文同)数的严格素性证明用时 10 分钟。第九个 Fermat 数的两个大素因子(49 位和 99 位)就是用此算法在巨型机 Cray-XMP 上进行严格素性证明的[4]。

算法的基本思想是：在分园域中对被测数 n 施一系列伪素性测试(这里的主要运算是分园域中的算术)，若某一测试失效，则 n 是合数；若 n 通过所有这些测试，就意味着对 n 的任一因子 r 必有

$$i \in \{0, 1, \cdots, t-1\} \quad \text{使得} \quad r \equiv n^i \bmod s,$$

这里 t 和 s 是预先确定的整数，t 很小，$s > n^{1/2}$，而且对与 s 互素的任何整数 a 有 $a^t \equiv 1 \bmod s$；由于 t 很小，最后不需太多的运算就可定出 n 的全部因子，从而确认 n 是否素数。

我们根据文献[3]的实现方案在 PC 微机上也实现了此算法，我们[5]曾用我们的软件验证过一个 53 位数的三个素因子。现在我们的 Pascal 程序在 486 微机上对 104 位素数的严格素性证明在 5 分钟内完成。特别地，我们证明了 $10^{103}+129$ 是素数。本文给出我们的程序对此 104 位素数的严格素性证明所用的主要参数、一些中间数据和算法各步骤在 PC 微机上实际耗时。

如不特别说明，本文所用记号都与文献[3]的相同。特别地，我们用 Z 表整数环，Q 表有理数域。素数 p 在整数 m 中出现次数记作 $v_p(m)$，素数幂 p^k 次单位根记作 ζ_{p^k}。我们用向量 $(a_i)_{0\leqslant i<(p-1)p^{k-1}}$ 表环 $Z[\zeta_{p^k}]$ 中的元素 $\sum_{0\leqslant i<(p-1)p^{k-1}} a_i \zeta_{p^k}^i$。对 $x \in Z$，$x \not\equiv 0 \bmod p$，记 σ_x 为分园域 $Q(\zeta_{p^k})$ 的自同构，满足：$\sigma_x(\zeta_{p^k}) = \zeta_{p^k}^x$。不超过实数 y 的最大整数记作 $[y]$。

二、表的准备

(a) 为了能判定 $< 10^{104}$ 的整数是否素数，我们取

$$t = 2^4 \cdot 3^2 \cdot 5 \cdot 7 = 5040;$$

$$e(t) = 2 \cdot \sum_{q\text{素数}, q-1 \mid t} q^{v_q(t)+1}$$

$$= 2^6 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 71 \cdot 73 \cdot 113 \cdot 127 \cdot 181 \cdot 211 \cdot 241 \cdot 281 \cdot 337 \cdot 421 \cdot 631 \cdot 1009 \cdot 2521$$

(b)对每个奇素数 $q \mid e(t)$ 做(b1)和(b2)：

(b1)设 g 是 mod q 的本原根，即

$$g \not\equiv 0 \bmod q \text{ 且对任意素数 } p \mid q-1 \text{ 有 } g^{\frac{q-1}{p}} \not\equiv 1 \bmod q.$$

设函数 $j: \{1, 2, \cdots, q-2\} \to \{1, 2, \cdots, q-2\}$ 定义为

$$1 - g^i \equiv g^{j(i)} \bmod q.$$

(b2)对每个素数 $p \mid q-1$(因此 $p \mid t$)做如下事：

令 $k = v_p(q-1)$；

若 $p^k \neq 2$，计算 Jacobi 和 $j_{p,q} = \sum_{i=1}^{q-2} \zeta_{p^k}^{i+j(i)} \in Z[\zeta_{p^k}]$；

若 $p = 2$，$k \geqslant 3$，计算 Jacobi 和

$$j^{*}_{2,q}=\sum_{x=1}^{q-2}\zeta_2^{3x+j(x)}\in Z[\zeta_{2^t}],\ j^{\#}_{2,q}=\sum_{x=1}^{q-2}\zeta_{2^t}^{2^{t-3}(3x+j(x))}\in Z[\zeta_{2^t}]。$$

我们得到$j_{2,5}=(-1,-2)\in Z[\zeta_{2^2}]$，$j_{3,7}=(-1,-3)\in Z[\zeta_3]$，…，

$j_{2,2521}=(37,-24,0,-24)\in Z[\zeta_{2^3}]$，

$j_{3,2521}=(-4,16,-8,42,11,-22)\in Z[\zeta_{3^2}]$，

$j_{5,2521}=(-29,-51,-39,-57)\in Z[\zeta_5]$，

$j_{7,2521}=(33,5,1,-23,21,25)\in Z[\zeta_7]$，

$j^{*}_{2,2521}=(35,0,36,0)$，$j^{\#}_{2,2521}=(37,-24,0,-24)\in Z[\zeta_{2^3}]$。

三、素性测定：$10^{103}+129$ 是素数

表准备好作为磁盘文件储存，以后每次运行程序只需查表(读磁盘文件)，不必再将表中数据重算一遍。

从本节以后，令 $n=10^{103}+129$。我们按[3]的方案证明 n 是素数。主要步骤有：初步测试，Lucas-Lehmer 测试，参数 t 和 s 的选取，Jacobi 和伪素性测试，最后的试除。

3.1 初步测试

(a)算得 $\gcd(t\cdot e(t),n)=1$；

(b)取试除界 $B=65535$，计算

$l^{-}=\{$奇素数 $p\leqslant B:p\mid n-1\}=\{3,449,947\}$，

$n-1$ 的不含$\leqslant B$ 的素数为因子的最大奇因子 $r^{-}=61245\cdots61289$(95 位)，

$f^{-}=\dfrac{n-1}{r^{-}}=2^7\cdot3\cdot449\cdot947=163277952$，

$l^{+}=\{$奇素数 $p\leqslant B:p\mid n+1\}=\{5,7,32771\}$，

$n+1$ 的不含$\leqslant B$ 的素数为因子的最大奇因子 $r^{+}=43592\cdots17529$(97 位)，

$f^{+}=\dfrac{n+1}{r^{+}}=2\cdot5\cdot7\cdot32771=2293970$；

(c)进行 5 次 Rabin-Miller 概率合性测试。令 u 为 $n-1$ 的最大奇因子，则 $n-1=2^7\cdot u$。对于正整数 b，若

$$b^{u}\equiv1 \bmod n \text{ 或对某个 } i:0\leqslant i\leqslant6,\text{ 有 } b^{2^iu}\equiv-1 \bmod n,$$

就说 n 对于基 b 通过 Miller 测试。我们测试结果为，n 对于随机选取的五个基都通过 Miller 测试，因而得知 n 很可能是素数；

(d)对素数幂 $p^k\mid t$，若 $n\equiv1\pmod{p^k}$置 $\mathrm{flag}_{p^k}=$"true"否则置 $\mathrm{flag}_{p^k}=$"false"。我们有当 $p^k=2,3,4,8,16$ 时，$\mathrm{flag}_{p^k}=$"true"。

3.2 Lucas-Lehmer 测试

在 Z/nZ 中置 prod=1。

(a)对每个素数 $p\in l^{-}$验证 n 通过 $n-1$ 测试，即找一个素数 $x\in\{p_1,p_2,\cdots,p_{50}\}$满足

$$x^{(n-1)/p}\not\equiv1 \bmod n \text{ 且 } x^{n-1}\equiv1 \bmod n;$$

设 x 已求得，再用 $\mathrm{prod}\cdot(x^{(n-1)/p}-1) \bmod n$ 代替 prod。

我们求得 $x=2$ 对每个 $p\in l^-$ 都满足上式。

因 $\text{flag}_3=$"true"，置 $\beta_3^0=1$，

$\beta_3^1=2^{(n-1)/3} \bmod n=70876\cdots23164$(103 位)，

$\beta_3^2=2^{2(n-1)/3} \bmod n=29123\cdots76964$(103 位)。

(b)对于 r^- 证得 n 也通过 $n-1$ 测试，所求 $x=2$。

(c)因 $n\equiv1 \bmod 4$，令 $u=0$，求得 $a=7$ 满足 $a^{(n-1)/2}\equiv-1 \bmod n$。

令环 $A=(Z/nZ)[T]/(T^2-a)$，环中元素表为 x_0+x_1a，

这里 $a=T \bmod T^2-a$。

因对于 $l=1, 2, 3, 4$ 有 $\text{flag}_{2^l}=$"true"，置

$$\beta_{2^l}^i = a^{i(n-1)/2^l} \bmod n,\ i = 0, 1, \cdots, 2^l - 1。$$

我们有 $\beta_2^0=1$，$\beta_2^1=-1$，$\cdots$，$\beta_{16}^0=1$，

$\beta_{16}^1=45205\cdots55116$(103 位)，$\cdots$，$\beta_{16}^{15}=76677\cdots20666$(103 位)。

(d)对每个素数 $p\in l^+$ 验证 n 通过 $n+1$ 测试，即找一个元素 $x\in A$，x 的范数为 1，满足

$$x^{(n+1)/p}\neq1 \text{ 且 } x^{n+1}=1;$$

设 x 已求得，再令 $x^{(n+1)/p}=x_0+x_1a\in A$，若 $x_i\neq0$，$i\in\{0, 1\}$，

用 $\text{prod}\cdot x_i \bmod n$ 代替 prod。

我们求得 $x=\dfrac{1+a}{1-a}+\dfrac{2}{1-a}a$ 对每个 $p\in l^-$ 都满足上式。

(c)对于 r^+ 证得 n 也通过 $n+1$ 测试，所求 x 与(d)中的相同。

(f)验查 $\gcd(\text{prod}, n)=1$，宣布 n 通过 Lucas-Lehmer 测试，因而 n 极可能是素数。

3.3 参数 t 和 s 的选取

令 t' 为 t 的一个偶因子，

$$s_1 = \frac{1}{2}\cdot\prod_{p\text{素数},\ p\mid f^-\cdot f^+} p^{v_p(t')+v_p(f^-\cdot f^+)},$$

$$s_2^{\sim} = \prod_{q\text{为素数},\ q-1\mid t',\ q\text{不整除}s_1} q,$$

$$s_2 = s_2^{\sim}\cdot\prod_{p\text{素数},\ p\mid t',\ p\mid s_2^{\sim}} p^{v_p(n^{p-1}-1)+v_p(t')-1}。$$

取 t' 尽可能小使得 $s=s_1\cdot s_2>n^{1/2}$，我们得到 $t'=2520$ 为所求，此时

$s_1=2^{10}\cdot3^3\cdot5^2\cdot7^2\cdot449\cdot947\cdot32771=471938951672294400$，

$s_2=11\cdot13\cdot19\cdot29\cdot31\cdot37\cdot41\cdot43\cdot61\cdot71\cdot73\cdot127\cdot181\cdot211\cdot281\cdot421\cdot631\cdot2521$

$=45980\cdots83793$(35 位)，

$s=s_1\cdot s_2=21699\cdots59200$(53 位)。

再令 $t=t'=2520$，我们有 $n'\equiv1 \bmod s$ 且 $s>n^{1/2}$。

3.4 Jacobi 和伪素性测试

对每个素数 $p\mid t$，每个素数 $q\mid s_2$ 满足 $p\mid q-1$，验证[2]中条件(7.9)，即求

$h \in \{0, 1, \cdots, p^k - 1\}$，使得 $J_{p,q} = \zeta_{p^k}^h \bmod nZ[\zeta_{p^k}]$，

这里 $k = v_q(q-1)$，分圆域 $Z[\zeta_{p^k}]$ 中的元素 $J_{p,q}$ 定义如下：

(1)当 $p>2$，令 $M=\{x\in Z: 1\leqslant x<p^k,\ p\nmid x\}$，

$$J_{p,q} = \prod_{x\in M}\sigma_x^{-1}\left((j_{p,q})^{\left[\frac{nx}{p^k}\right]}\right) \bmod nZ[\zeta_{p^k}];$$

(2)当 $p^k=2$，$j_{2,q}=q^{\frac{n-1}{2}} \bmod n$；

(3)当 $p^k=4$，因 $n\equiv 1 \bmod 4$，

$$J_{2,q} = (j_{2,q})^{\frac{n-1}{2}} \cdot q^{\frac{n-1}{4}} \bmod nZ[\zeta_4];$$

(若 $n\equiv 3 \bmod 4$，$J_{2,q}=(j_{2,q})^{\frac{n+3}{2}} \cdot q^{\frac{n-1}{4}} \bmod nZ[\zeta_4]$。)

(4)当 $p=2$，$k\geqslant 3$ 令 $M=\{x\in Z: 1\leqslant x<2^k,\ x\equiv 1 \text{ 或 } 3 \bmod 8\}$，

因 $n\equiv 1 \bmod 8$(若 $n\equiv 3 \bmod 8$，亦如此)，

$$J_{2,q} = \prod_{x\in M}\sigma_x^{-1}\left((j_{2,q}^* \cdot j_{2,q})^{\left[\frac{nx}{2^k}\right]}\right) \bmod nZ[\zeta_{2^k}]。)$$

(若 $n\equiv 5$ 或 $7 \bmod 8$，$J_{2,q}=(j_{2,q}^*)^2 \cdot \prod_{x\in M}\sigma_x^{-1}\left((j_{2,q}^* \cdot j_{2,q})^{\left[\frac{nx}{2^k}\right]}\right) \bmod nZ[\zeta_{2^k}]$。)

注 1. 这里 $J_{p,q}$ 即[3]中的 $j_{0,p,q}^* \cdot j_{v,p,q}$。

注 2. 若 $\text{flag}_{p^k}=$"true"，利用环同态

$$\lambda: Z[\zeta_{p^k}]/nZ[\zeta_{p^k}] \to Z/nZ,\ \lambda(\zeta_{p^k}) = \beta_{p^k},$$

把环 $Z[\zeta_{p^k}]/nZ[\zeta_{p^k}]$ 中的算术运算转换为 Z/nZ 中的算术运算，从而加快了运算速度。

我们的计算表明 n 顺利通过 Jacobi 和伪素性测试，所求的 h 值如下。

$p=2$：

q	11	13	19	29	31	37	…	181	211	281	421	631	2521
k	1	2	1	2	1	2	…	2	1	3	2	1	3
h	1	0	0	2	0	2	…	2	1	0	0	1	3

$p=3$：

q	13	19	31	37	43	61	…	127	181	211	421	631	2521
k	1	2	1	2	1	1	…	2	2	1	1	2	2
h	2	2	1	4	1	0	…	2	1	1	2	2	2

$p=5$：

q	11	31	41	61	71	181	211	281	421	631	2521
k	1	1	1	1	1	1	1	1	1	1	1
h	2	2	0	0	0	3	0	0	0	0	1

$p=7$：

q	29	43	71	127	211	281	421	631	2521
k	1	1	1	1	1	1	1	1	1
h	4	4	4	0	4	3	0	0	1

由于每一个素数 $p|t$ 都有 $p|f^- \cdot f^+$(即[3]中所谓 $\lambda_p=$"true")，所以没有附加测试而直接进入最后的试除阶段。

3.5 最后的试除

至此我们证明了，对 n 的任一因子 r 必有

$$i \in \{0, 1, \cdots, t-1\} \text{ 使得 } r \equiv n^i \bmod s,$$

若 n 是合数，由于 $s > n^{1/2}$，所以至多需 $3n = 7560$ 次(多精度)乘除法就可找出 n 的真因子。我们计算结果表明 n 没有真因子，因而 n 是素数。

四、运行时间

下表给出我们的 Pascal 程序在我们的 Jcc486(一台 IBM PC486 兼容机)上运行时间(秒)。

被测数位数	50	75	104
初步测试	1.81	2.86	5.06
Lucas-Lehmer 测试	5.38	6.32	21.86
t 和 s 的选取	0.01	0.05	0.05
Jacobi 和测试	4.51	70.63	227.06
最后的试除	0.01	1.32	3.99
总运行时间	11.72	81.18	257.93

所用的被测数分别为 $10^{49}+9$，$10^{74}+207$，$10^{103}+129$，它们都是素数。

参 考 文 献

[1] L. M. Adleman, C. Pomerance and R. S. Rumely, On distinguishing prime numbers from composite numbers, Annals of Math., 117(1983), 173—206.

[2] H. Cohen and H. W. Lenstra, Jr., Primality testing and Jacobi sums, Math. Comp., 42(1984), 297—330.

[3] H. Cohen and A. K. Lenstra, Implementation of a new primality test, Math. Comp., 48(1987), 329—339.

[4] 张振祥，曾肯成，一个 53 位数的分解，计算机研究与发展，32:6(1995)，1—4。

(上接第 78 页)

下的实现。符号移位方法是实现动态控制 GI^{m} 的简便有效的手段。

进一步的工作，是在应用动态方向准则的两原则下，构造更多的实现动态方向准则的具体方法，并将它们推广到 $3D$。

参 考 文 献

[1] B. B. Mandelbrot, *the Fractal Geometry of Nature*, W. H. Freeman, San Francisco, 1982.

[2] H. O. Peitgen and P. H. Richter, *The Beauty of Fractals: Images of Complex dynamical system*, Springer-Verlag, Berlin, 1986.

[3] A. Fournier, D. Fussel and L. C. Carpenter, *Computer Rendering of Stochastic Modes*, Comm ACM, V25, n6, pp371-384, June 1982.