Advances in Applied Mathematics 应用数学进展, 2024, 13(5), 2062-2068
Published Online May 2024 in Hans. https://www.hanspub.org/journal/aam
https://doi.org/10.12677/aam.2024.135193

Hans汉斯

坎特伯雷难题集中全一数R19是素数的证明

冯贝叶

中国科学院数学与系统科学研究院应用数学所，北京

收稿日期：2024年4月23日；录用日期：2024年5月17日；发布日期：2024年5月28日

摘　要

一个正整数的素性判别是数论中一个有意义和有兴趣的问题，全一数R19是否是一个素数的问题虽在文献中提到已被用$n-1$法解决，但国内一直未见有证明方法的介绍，本文借助于数学软件Mathematica12.0用个人计算机证明了坎特伯雷难题集中全一数R19是一个素数。这对证明其他整数的素性判定提供了一个参考。

关键词

全一数R19，素数，Mathematica12.0，个人计算机

Proof That Repunit R19 in the Canterbury Problem Set Is a Prime Number

Beiye Feng

Institute of Applied Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing

Received: Apr. 23rd, 2024; accepted: May 17th, 2024; published: May 28th, 2024

Abstract

The primality criterion of a positive integer is a meaningful and interesting problem in number theory. Although the question of whether Repunit R19 is a prime has been solved by the $n-1$ method in literature, there is no introduction to a proven method in China. This article uses the mathematical software Mathematical12.0 to prove on a personal computer that the Repunit R19 in the Canterbury problem set is a prime number. This provides a reference for proving the primality of other integers.

文章引用: 冯贝叶. 坎特伯雷难题集中全一数 R19 是素数的证明[J]. 应用数学进展, 2024, 13(5): 2062-2068.
DOI: 10.12677/aam.2024.135193

Keywords

Repunit R19, Prime Number, Mathematica12.0, Personal Computer

1. 引言

关于一个正整数是否是一个素数的问题或者称素性判定问题是数学上一个非常古老的问题，随着近年来计算机技术和算法数论飞速的发展，这一问题近年来取得了丰富的成果。在所有数目中，存在一些特殊形式的数，例如 Mersenne 数、Ferma 数等等，针对这些特殊形式的数，有一些特殊的判据，例如 Pipin 判据。

在本文中，主要应用几个适用于任何形式的数的被称为 $n-1$ 方法的初等判据，这些判据都要求知道 $n-1$ 的所有因子或部分因子的信息。

在这一节中，我们首先回顾素性判定的几个初等结果，150 多年来，Lucas 首先证明了一个初等的素数判定定理：

定理 1 (Lucas, 1876) (见[1] [2] [3])设 n 是一个正整数，如果存在正整数 a，使得对于小于 $n-1$ 的所有素因子 q 成立

$$a^{n-1} \equiv 1 \pmod{n}$$

$$a^{q} \not\equiv 1 \pmod{n},$$

则 n 必是一个素数。

上面这个结果，经常会被称为 Lucas 判据，但已有文献指出，它实际上并不是由法国数学家 Luucas 提出的(其中[1]是在法国期刊上发表的一篇关于 Lucas 的传记)，而是由美国数学家 D. H. Lehmer [3]提出的(当时他还是个学生，发表论文当年，他从伯克利毕业，获得物理学学士。后前往芝加哥大学师从 L. E. Dikson 攻读数学博士学位[4]。[2]指出 D. H. Lehmer 是 Lucas 的主要继承人，他还完善了与 Mersenne 数有关的素数判据)。

1927 年 D. H. Lehmer 建立了下面的基本结果。

定理 2 (D. H. Lehmer, 1927) [3]设 n 是一个正整数，并且对 $n-1$ 的所有素因子 p，存在一个整数 a 使得

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

$$a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$$

则 n 必是一个素数。

上面这个定理要求对 $n-1$ 的所有的素因子都存在一个统一的具有上述性质的 a，这对有些问题是不方便的，针对这一缺陷，1975 年 J. Brillhart，D. H. Lehmer，L. Selfridge 对此做出了实质性的一个改进，提出了下面的：

定理 3 (J. Brillhart, D. H. Lehmer, L. Selfridge, 1975) (见[5] [6])设 n 是一个正整数

$$n-1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

如果对每一个 p_i 都存在一个整数 a_i 使得

$$a_i^{n-1} \equiv 1 \pmod{n}$$

$$a_i^{\frac{n-1}{p_i}} \not\equiv 1 \pmod{n}$$

则 n 必是一个素数。

上面几个定理都要求知道 $n-1$ 的所有的因子的信息，这是一个很强的要求和限制。上面的 1975 的论文指出如果能对 $n-1$ 的部分分解，得出一个足够大的素因子，那么就会有一个对定理 3 的减小计算量的改进，这就是下面的 Proth 定理。

定理 4 (Prorh [7])设 n 是一个奇数，$n-1=mp$，其中 p 是一个奇素数且满足 $2p+1>\sqrt{n}$，同时又存在正整数 a 使得

$$a^{n-1} \equiv 1 \pmod{n}$$

$$a^{m} \not\equiv 1 \pmod{n}$$

则 n 必是一个素数。

上面这个定理要求 p 必须是一个素数。这仍然在 p 不大的情况下，并不能有效的减小计算量，结合 Pocklington 在 1914 年提出的一个定理，可以解除这一限制，从而可以得出以下的定理。

定理 5 (Proth, Pocklington) ([7] [8])设 $n-1=PR$，其中 F 是 $n-1$ 的已经分解出来的部分(即已知的素因子及其幂次)，R 是 $n-1$ 的未分解部分(即 $R=\dfrac{n-1}{F}$，我们不知道它是素数还是合数，或者即使知道它是一个合数但并不能知道它的素因子分解式。)并且 $F>\sqrt{n}$，若 $(F,R)=1$，且对 F 的每个素因子 p_i，都存在一个正整数 a_i 使得

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

$$\left(a_i^{\frac{n-1}{p_i}}-1, n\right)=1,$$

则 n 必是一个素数。

2. 两个应用例子

本节中的两个例子和下面第 3 节中的 R19 是素数的证明，[7]都已讨论过，但由于[7]中的有关计算都是错误的，因此并不有效。为了减小篇幅，本文就不一一加以对比，具体指出[7]中的错误在哪里，读者只要自行对照本文和[7]便可知道。

例 1. 证明 4093 是素数

本题用手算 + 一个手持科学计算器解决。

证明 设 $n=4093$，则 $n-1=4092=31\times 11\times 3\times 2^2$。

$$p_1=31,\ p_2=11,\ p_3=3,\ p_4=2。$$

取 $a=2$，则 $m_1=2^{\frac{n-1}{p_1}}=2^{132}$，$m_2=2^{\frac{n-1}{p_2}}=2^{372}$，$m_3=2^{\frac{n-1}{p_3}}=2^{1364}$，$m_4=2^{\frac{n-1}{p_4}}=2^{2046}$。

对模 4093，有

$$2^{10}\equiv 1024,\ 2^{20}\equiv 1024^2\equiv 768,\ 2^{40}\equiv 768^2\equiv 432,\ 2^{60}\equiv 768^3\equiv 243,$$

$$2^{100}\equiv 432\times 243\equiv 2651,\ 2^{30}\equiv 1024\times 768\equiv 576,\ 2^{32}\equiv 576\times 4\equiv 2304$$

$$2^{132}\equiv 2651\times 2304\equiv 1148\neq 1\pmod{4093} \tag{1}$$

$2^{200}\equiv 2651^2\equiv 120$， $2^{200}\equiv 2651^2\equiv 120$， $2^{30}\equiv 2^{10\times 3}\equiv 1024^3\equiv 576$，

$2^{31}\equiv 576\times 2\equiv 1152$， $2^{93}\equiv 1152^3\equiv 2355$， $2^{186}\equiv 2355^2\equiv 10$，

$$2^{372}\equiv 10^2\equiv 100\neq 1\pmod{4093} \tag{2}$$

$2^{400}\equiv 120^2\equiv 2121$， $2^{800}\equiv 2121^2\equiv 434$， $2^{1000}\equiv 120\times 434\equiv 2964$，

$2^{120}\equiv 243^2\equiv 1747$， $2^{240}\equiv 1747^2\equiv 2724$， $2^{248}\equiv 2724\times 256\equiv 1534$

$$2^{1116}\equiv 2^{372\times 3}\equiv 100^3\equiv 1308$$

$$2^{1364}\equiv 2^{268}\times 2^{1116}\equiv 1534\times 1308\equiv 902\neq 1\pmod{4093} \tag{3}$$

$$2^{2000}\equiv 2964^2\equiv 1718,\quad 2^{46}\equiv 432\times 64\equiv 3090$$

$$2^{2046}\equiv 1718\times 3090\equiv 4092\equiv -1\pmod{4093} \tag{4}$$

$$2^{4092}\equiv 1\pmod{4093} \tag{5}$$

由(1)~(5)和定理 2 即得 4093 是一个素数。

例 2. 证明 823,001 是一个素数

本例用手算 + Matheatica12.0 完成。

证明 设 n = 823,001，则 $n-1=823000=1000\times 823=mp$ 其中 m = 1000，p = 823 是一个素数。

$$2p+1=1847>908>\sqrt{823001}=\sqrt{n}\ 。 \tag{6}$$

对模 823,001，取 a = 2，则

$2^{10}\equiv 1024$， $2^{20}\equiv 1024^2\equiv 225575$， $2^{23}\equiv 225575\times 8\equiv 158598$，

$2^{25}\equiv 225575\times 32\equiv 634392$， $2^{50}\equiv 634392^2\equiv 782658$， $2^{100}\equiv 782658^2\equiv 484672$，

$2^{200}\equiv 484672^2\equiv 241157$， $2^{400}\equiv 241157^2\equiv 155985$， $2^{800}\equiv 155985^2\equiv 118661$，

$$2^{m}\equiv 2^{1000}\equiv 118661\times 241157\equiv 186007\neq 1\pmod{823001} \tag{7}$$

$2^{823}\equiv 118661\times 158598\equiv 656412$， $2^{1646}\equiv 656412^2\equiv 301201$，

$2^{3292}\equiv 301201^2\equiv 173168$， $2^{4115}\equiv 173168\times 656412\equiv 770101$，

$2^{8230}\equiv 770101^2\equiv 206600$， $2^{16460}\equiv 206600^2\equiv 259137$，

$2^{20575}\equiv 143927\times 770101\equiv 380357$， $2^{41150}\equiv 380357^2\equiv 216664$，

$2^{82300}\equiv 216664^2\equiv 134857$， $2^{102875}\equiv 134857\times 380357\equiv 266624$，

$2^{205750}\equiv 266624^2\equiv -1$， $2^{411500}\equiv (-1)^2\equiv 1$，

$$2^{n-1}\equiv 2^{823000}\equiv 2^{411500\times 2}\equiv 1^2\equiv 1 \tag{8}$$

由(6) (7) (8)和定理 4 即得 833,001 是一个素数。

3. 全一数 R19 是素数的证明

全一数(Repunits)是指各位数字都是 1 的数字，一般用 Rn 表示，其中 n 指全一数中 1 的个数([7] [8] [9] [10])。在 1904 年出版的坎特伯雷难题集中(见[9])，有一个问题是问11…1 (19 个 1)是否是一个素数，这问题一直没有解决，直到 1978 年以后，文献中才提到有人用 n−1 方法解决了此问题，但并没有见到具体的解

法(见[7]-[13])。在文献[7]中给出了一个证明，不过由于这个证明一开始就出现了一个明显的计算错误而无效(在[8]中设 $n=11\cdots1$ (19 个 1)，并说 $n-1=F_1R_1$，其中 $F_1=3333330=2\times3^2\times5\times11\times31\times37\times91$，由于显然 F_1 的因子必须是 $n-1$ 的因子，而 $n-1$ 并没有 91 这个因子，因此这一分解显然是错误的，而以下的计算也就无效了)。

以下完全借助于 Mathematica12.0 完成计算。

下面我们证明 R19 是一个素数。

设 $n=1111111111111111111$，则 $n-1=1111111111111111110=FR$

其中 $F=1062200958=52579\times37\times13\times7\times3\times2$， $R=\dfrac{n-1}{F}$。

由于 $1062200958^2-1111111111111111111>0$，所以

$$F=1062200958>\sqrt{1111111111111111111}=\sqrt{n} \tag{9}$$

$$F=p_1p_2p_3p_4p_5p_6$$

其中 $p_1=52579$， $p_2=37$， $p_3=13$， $p_4=7$， $p_5=3$， $p_6=2$。

对模 $n=1111111111111111111$ 有

$$m_1=\frac{n-1}{p_1}=333667\times37\times19\times13\times11\times7\times5\times3^2\times2$$

对 p_1,p_2,p_3,p_4，取 $a=2$，则

$$2^{333667}\equiv686033429761844421=r_1,$$

$$r_1^{52579}\equiv686033429761844421^{52579}\equiv10833065941756886=r_2,$$

$$r_2^{37}\equiv10833065941756886^{37}\equiv25038712834380145=r_3,$$

$$r_3^{19}\equiv25038712834380145^{19}\equiv659804149831953774=r_4,$$

$$r_4^{13}\equiv659804149831953774^{13}\equiv219095598444019794=r_5,$$

$$r_5^{11}\equiv219095598444019794^{11}\equiv314626805515060544=r_6,$$

$$r_6^{35}\equiv314626805515060544^{35}\equiv933000903779960656=r_7,$$

$$2^{n-1}\equiv r_7^{18}\pmod{n}\equiv r_7^{18}\pmod{1111111111111111111}\equiv1 \tag{10}$$

$$m_1=\frac{n-1}{p_1}=2113222201090=333667\times37\times19\times13\times11\times7\times5\times3^2\times2,$$

$$2^{333667}\equiv686033429761844421=r_{11},$$

$$2^{37\times333667}\equiv r_{11}^{37}\equiv980823581211748537=r_{12},$$

$$2^{19\times37\times333667}\equiv r_{12}^{19}\equiv1077616254044116588=r_{13},$$

$$2^{13\times19\times37\times333667}\equiv r_{13}^{13}\equiv62778917655367695=r_{14},$$

$$2^{11\times13\times19\times37\times333667}\equiv r_{14}^{11}\equiv191685422932804908=r_{15},$$

$$2^{5\times7\times11\times13\times19\times37\times333667}\equiv r_{15}^{35}\equiv648182400500105952=r_{16},$$

$$2^{m_1}\equiv2^{2\times3^2\times5\times7\times11\times13\times19\times37\times333667}\equiv r_{16}^{18}\equiv390068371006902754,$$

$$\left(2^{m_1}-1,n\right)=1 \tag{11}$$

$$m_2=\frac{n-1}{p_2}=333667\times52579\times19\times13\times11\times7\times5\times3^2\times2,$$

$$2^{19\times13\times11\times7\times5\times3^2\times2}\equiv828428136044625569=r_{21},$$

$$2^{333667\times19\times13\times11\times7\times5\times3^2\times2}\equiv r_{21}^{333667}\equiv564791157091879790=r_{22},$$

$$2^{m_2}\equiv r_{22}^{52579}\equiv207863854007559622,$$

$$\left(2^{m_2}-1,n\right)=1 \tag{12}$$

$$m_3=\frac{n-1}{p_3}=333667\times52579\times37\times7\times3^2\times2,$$

$$2^{37\times7\times3^2\times2}\equiv716086219179556333=r_{31},$$

$$2^{333667\times37\times7\times3^2\times2}\equiv r_{31}^{333667}\equiv572163650030706066=r_{32},$$

$$2^{m_3}\equiv r_{32}^{52579}\equiv786092545290328404,$$

$$\left(2^{m_3}-1,n\right)=1 \tag{13}$$

$$m_4\equiv\frac{n-1}{p_4}=333667\times52579\times37\times19\times13\times11\times5\times3^2\times2,$$

$$2^{2\times3^2\times5\times11\times13\times13\times19\times37}\equiv454564979521137587=r_{41},$$

$$2^{2\times3^2\times5\times11\times13\times13\times19\times37\times333667}\equiv r_{41}^{333667}\equiv291103097675451058=r_{42},$$

$$2^{m_4}\equiv r_{42}^{52579}\equiv624671632919673247,$$

$$\left(2^{m_4}-1,n\right)=1 \tag{14}$$

对 p_5,p_6，取 $a=3$，

$$3^{2\times3\times5\times7\times11\times13\times19\times37}\equiv413091562820750497=r_{51}$$

$$3^{2\times3\times5\times7\times11\times13\times19\times37\times333667}\equiv r_{51}^{333667}\equiv719013698222911823=r_{52},$$

$$3^{m_5}\equiv r_{52}^{52579}\equiv933000903779960656,$$

$$\left(3^{m_5}-1,n\right)=1 \tag{15}$$

$$m_6=\frac{n-1}{p_6}=3^2\times5\times7\times11\times13\times19\times37\times52579\times333667,$$

$$3^{3^2\times5\times7\times11\times13\times19\times37}\equiv439165546220198935=r_{61}$$

$$3^{3^2\times5\times7\times11\times13\times19\times37\times333667}\equiv439165546220198935^{333667}\equiv125757480451062679=r_{62},$$

$$3^{m_6}\equiv r_{62}^{52579}\equiv125757480451062679^{52579}\equiv-1$$

$$\left(3^{m_6}-1,n\right)=1 \tag{16}$$

由(9)~(16)和定理 5 即得 R19 是一个素数。

讨论：本文的例子及第 3 节的方法提供了素性判定的一种初等方法及其具体的集散过程，具体的应用成果就是解决了 R19 的素性判定。这可对类似问题给出一种参考方法，从本文的方法看出这种方法随

着 n 的增大，难度将越来越大。因此对大整数的素性判定是否能继续应用这种方法需要继续探讨。

参考文献

[1] Lucas, E. (1876) Sur la recherche des grands nombres premiers. *Association Française pour l'Avancement des Sciences*, **5**, 61-68.

[2] Décaillot, A.M. and Lucas, L.É. (1998) Théorie Instrumentation. *Revue d'Histoire des Mathématiques*, No. 2, 191-236.

[3] Lehmer, D.H. (1927) Test for Primality by Converse of Fermat's Theorem. *Bulletin of the American Mathematical Society*, **33**, 327-340.

[4] Derrick Henry Lehmer (1905-1991) Biography, MacTutor History of Mathematics Archive. https://mathshistory.st-andrews.ac.uk/Biographies/Lehmer_Derrick/

[5] Brillhart, J., Lehmer, D.H. and Selfridge, J.L. (1975) New Primality Criteria and Factorization of 2^m±1. *Mathematics of Computation*, **29**, 620-647. https://doi.org/10.2307/2005583

[6] Pocklington, H.C. (1914) The Determination of the Prime or Composite Nature of Large Numbers by Fermat's Theorem.

[7] 孙琦, 旷京华. 素数判定与大数分解[M]. 哈尔滨: 哈尔滨工业大学出版社, 2014.

[8] 刘醉白. 素数证明: 在满足费马小定理的部分条件下, 结合图中条件, 请问如何证明 n 是一个素数? [EB/OL]. https://www.zhihu.com/answer/574767625, 2024-04-25.

[9] (英)亨利·杜德尼. 坎特伯雷趣题[M]. 陈以鸿, 译. 上海: 上海科技教育出版社, 2007.

[10] Wells, D. (2005) Prime Numbers, the Most Mysterious Figures in Math. Wiley, Hoboken.

[11] Ribenboim, P. (2006) The Little Book of Bigger Primes. Springer-Verlag, New York.

[12] 颜松远. 计算数论[M]. 第二版. 杨思熳, 刘巍, 齐璐璐, 陶红伟, 译. 北京: 清华大学出版社, 2008.

[13] Yates, S. (1982) Repunits and Repetends. Star Publishing Co. Inc., Boynton Beach.