素数的序乘以及与序乘相关的素数的生成公式[1]

陈惟昌[1]， 陈志义[2]， 陈志华[1]， 王自强[1]
[1]卫生部中日友好临床医学研究所，北京 (100029)
[2]中国科学院自动化研究所国家模式识别实验室，北京 (100080)
E-mail: chenweic@ht.rol.cn.net

摘 要：素数的序乘是指素数按大小顺序的连乘积。第 n 个素数的序乘称为第 n 个欧几里德合数。根据欧几里德合数可将自然数列依次划分为欧几里德区间。欧几里德合数及其后续的各素数之和组成的素数系列称为超序素数系列。应用超序素数的生成公式可以产生一系列的大型素数。这在 RSA 密钥的编码中有一定实用价值。本文对与序乘相关素数的性质进行了讨论，并提出与序乘有关素数的综合猜想。

关键词：素数序乘；欧几里德区间；超序素数；素数生成公式；RSA 密钥系统
中图分类号：0156.1

1. 引言

多年来数学家一直致力于寻找产生素数的普适公式。最著名的如麦森数 $M_p = 2^p - 1$，费马数 $F_m = 2^{2^m} + 1$ 以及欧拉公式 $f(n) = n^2 + n + 41$，欧拉公式可产生 41 个素数（当 n = 0，1，… 40 时）。但 $f(41)$却为合数[1]。麦森数的发现与测试，十分复杂，而费马数 F_m 当 $m > 4$ 时是否仍为素数尚不明确。本文提出应用素数序乘公式 $P_\omega(n, d) = P_n(!) + P_{n+d}$ 以产生任意大的素数的方法。式中 $P_n(!)$为素数 P_n 的序乘。100 位以上的大型素数在 RSA 密钥的编码中有一定实用价值。

2. 素数的序乘

2.1 序乘的概念

参考数字阶乘的定义：

$$n! = 1 \bullet 2 \bullet \ldots \bullet (n-1) \bullet n \quad \ldots\ldots (2.1)$$

以及 $0! = 1$ ……(2.2)

可以对有序函数或数列的序乘(sequential factorial，或简称 sequorial)进行定义：

$$X_n(!) = X_1 \bullet X_2 \bullet \ldots \bullet X_{n-1} \bullet X_n \quad \ldots\ldots (2.3)$$

以及 $X_0(!) = 1$ ……(2.4)

n 称为序乘的阶数(rank)。

2.2 素数序乘的定义

根据序乘的概念，可对素数的序乘进行定义：

$$p_n(!) = \omega_n = p_1 \bullet p_2 \bullet \ldots \bullet p_{n-1} \bullet p_n \quad \ldots\ldots (2.5)$$

以及 $p_0(!) = \omega_0 = 1$ …… (2.6)

$p_0 = 1$ 称为原素数(proprimer)，而 $p_1 = 2$，$p_2 = 3$，… 等真正的素数称为真素数 p_i (euprimers)。一些 ω_n 之值如下：$\omega_1 = 2$，$\omega_2 = 6$，$\omega_3 = 30$，$\omega_4 = 210$，$\omega_5 = 2310$，$\omega_6 = 30030$，$\omega_7 = 510510$，$\omega_8 = 9699690$，$\omega_9 = 223092870$，$\omega_{10} = 6469693230$，$\omega_{54} = 6.520453402\ldots \times 10^{100}$，… $\omega_{93} = 5.136943898\ldots \times 10^{200}$。

素数的序乘与素数的阶乘(prime factorial) $P_n!$ 不同，

[1]本课题得到国家自然科学基金(60171040)项目的资助。

$$p_n! = 1 \bullet 2 \bullet \ldots \bullet (p_n - 1) \bullet p_n \quad \ldots\ldots (2.7)$$

显然 $p_n! \geq p_n(!)$。

一些文献用 primoral 表示素数的序乘，容易和素数的阶乘混淆，故我们应用 prime sequorial 表示素数的序乘以示和 prime factorial 相区别。

3. 自然数列的欧几里德区间及其相关的素数

3.1 自然数列的欧几里德区间

应用欧几里德合数(Euclid composites) $\omega_n = p_n(!)$可将自然数列划分为不同的欧几里德区间(Euclid intervals)。第 n 个欧几里德区间定义为：

$$I_d(n) = [\omega_n, \omega_{n+1} - 1] \quad \ldots\ldots (3.1)$$

3.2 阳性欧几里德素数和阴性欧几里德素数

3.2.1 阳性欧几里德素数

形如 $p_\omega^+(n) = \omega_n + 1$ 且为 $6n+1$ 型的素数称为阳性欧几里德素数(yang Euclid primes)。例如：

$p_\omega^+(1) = \omega_1 + 1 = 3$， $p_\omega^+(2) = \omega_2 + 1 = 7$， $p_\omega^+(3) = \omega_3 + 1 = 31$，

$p_\omega^+(4) = \omega_4 + 1 = 211$， $p_\omega^+(5) = \omega_5 + 1 = 2311$。

目前已知的最大阳性欧几里德素数为 $p_\omega^+(2673) = \omega_{2673} + 1 = 1 \bullet 2 \bullet \ldots \bullet 24029 + 1$，是 Caldwell 在 1993 年发现的[2]。其中 $p_{2673} = 24029$。是否有无穷多个阳性欧几里德素数问题称为阳性欧几里德素数猜想，目前尚未证明。

3.2.2 阴性欧几里德素数

形如 $p_\omega^-(n) = \omega_n - 1$ 且为 $6n-1$ 型的素数称为阴性欧几里德素数(yin Euclid primes)。例如：

$p_\omega^-(2) = \omega_2 - 1 = 5$， $p_\omega^-(3) = \omega_3 - 1 = 29$， $p_\omega^-(5) = \omega_5 - 1 = 2309$， $p_\omega^-(6) = \omega_6 - 1 = 30029$。

是否有无穷多个阴性欧几里德素数问题称为阴性欧几里德素数猜想。

3.2.3 欧几里德孪生素数

形如 $p_\omega^-(n)$和 $p_\omega^+(n)$组成的孪生素数 $T_\omega(n)$称为欧几里德孪生素数(Euclid twin primes)。已知的前 3 个欧几里德孪生素数为：

$T_\omega(2)=(5, 7)$；$T_\omega(3)=(29, 31)$；$T_\omega(5)=(2309, 2311)$。

是否有无穷多个欧几里德孪生素数问题称为欧几里德孪生素数猜想。欧几里德孪生素数猜想是孪生素数猜想的特例，其证明或否定证明亦更加困难。

4. 超序素数

4.1 加性超序素数

形如 $p_\sigma^+(n, k, d) = \omega_n + p_{n+d}$的素数称为加性超序乘素数或加性超序素数(additive super sequorial primes)。式中 n 为素数序乘的阶数(rank)，$\omega_n = p_n(!)$，k 为 n 阶超序素数的顺序数(order)，d 为后续素数的增量数(increment)，一般 $d \geq k$。相应欧几里德区间的前 3 位加性超

序素数如下：

4.1.1 $p_\sigma^+(0, 1, 1) = \omega_0 + p_1 = 1+2 = 3$

4.1.2 $p_\sigma^+(1, 1, 1) = \omega_1 + p_2 = 2+3 = 5$

4.1.3 $p_\sigma^+(2, 1, 1) = \omega_2 + p_3 = 6+5 = 11$

$p_\sigma^+(2, 2, 2) = \omega_2 + p_4 = 6+7 = 13$

$p_\sigma^+(2, 3, 3) = \omega_2 + p_5 = 6 +11 = 17$

4.1.4 $p_\sigma^+(3, 1, 1) = \omega_3 + p_4 = 30 + 7 = 37$

$p_\sigma^+(3, 2, 2) = \omega_3 + p_5 = 30 +11 = 41$

$p_\sigma^+(3, 3, 3) = \omega_3 + p_6 = 30 +13 = 43$

4.1.5 $p_\sigma^+(4, 1, 2) = \omega_4 + p_6 = 210 +13 = 223$

$p_\sigma^+(4, 2, 3) = \omega_4 + p_7 = 210 +17 = 227$

$p_\sigma^+(4, 3, 4) = \omega_4 + p_8 = 210 + 19 = 229$

4.1.6 $p_\sigma^+(5, 1, 4) = \omega_5 + p_9 = 2310 + 23 = 2333$

$p_\sigma^+(5, 2, 5) = \omega_5 + p_{10} = 2310 + 29 = 2339$

$p_\sigma^+(5, 3, 6) = \omega_5 + p_{11} = 2310 + 31 = 2341$

4.1.7 $p_\sigma^+(6, 1, 1) = \omega_6 + p_7 = 30030 + 17 = 30047$

$p_\sigma^+(6, 2, 3) = \omega_6 + p_9 = 30030 + 29 = 30059$

$p_\sigma^+(3, 3, 7) = \omega_6 + p_{13} = 30030 + 41 = 30071$

4.1.8 $p_\sigma^+(7, 1, 1) = \omega_7 + p_8 = 510510 + 19 = 510529$

$p_\sigma^+(7, 2, 6) = \omega_7 + p_{13} = 510510 + 41 = 510551$

$p_\sigma^+(7, 3, 7) = \omega_7 + p_{14} = 510510 + 43 = 510553$

4.1.9 $p_\sigma^+(8, 1, 1) = \omega_8 + p_9 = 9699690 + 23 = 9699713$

$p_\sigma^+(8, 2, 4) = \omega_8 + p_{12} = 9699690 + 37 = 9699727$

$p_\sigma^+(8, 3, 5) = \omega_8 + p_{13} = 9699690 + 41 = 9699731$

4.2 减性超序素数

形如 $p_\sigma^-(n, k, d) = \omega_n - p_{n+d}$ 的素数称为减性超序素数(subtractive super sequorial primes)。相应的欧几里德区间的前 3 位减性超序素数如下：

4.2.1 $p_\sigma^-(3, 1, 1) = \omega_3 - p_4 = 30 - 7 = 23$

$p_\sigma^-(3, 2, 2) = \omega_3 - p_5 = 30 -11 = 13$

$p_\sigma^-(3, 3, 3) = \omega_3 - p_6 = 30 -13 = 17$

4.2.2 $p_\sigma^-(4, 1, 1) = \omega_4 - p_5 = 210 -11 = 199$

$p_\sigma^-(4, 2, 2) = \omega_4 - p_6 = 210 -13 = 197$

$p_\sigma^-(4,3,3)=\omega_4-p_7=210-17=193$

4.2.3 $p_\sigma^-(5,1,2)=\omega_5-p_7=2130-17=2113$

$p_\sigma^-(5,2,3)=\omega_5-p_8=2130-19=2111$

$p_\sigma^-(5,3,6)=\omega_5-p_{11}=2130-31=2099$

4.2.4 $p_\sigma^-(6,1,1)=\omega_6-p_7=30030-17=30013$

$p_\sigma^-(6,2,2)=\omega_6-p_8=30030-19=30011$

$p_\sigma^-(6,3,7)=\omega_6-p_{13}=30030-41=29989$

4.2.5 $p_\sigma^-(6,1,1)=\omega_7-p_{10}=510510-29=510481$

$p_\sigma^-(6,2,2)=\omega_7-p_{15}=510510-47=510463$

$p_\sigma^-(6,3,7)=\omega_7-p_{16}=510510-53=510457$

4.2.6 $p_\sigma^-(8,1,1)=\omega_8-p_9=9699690-23=9699667$

$p_\sigma^-(8,2,4)=\omega_8-p_{12}=9699690-37=9699653$

$p_\sigma^-(8\ 3,5)=\omega_8-p_{13}=9699690-41=9699649$

5. 欧几里德区间的最小素数和最大素数

5.1 第 n 个欧几里德区间的最小素数

在第 n 个欧几里德区间 $I_d(n)=[\omega_n,\ \omega_{n+1}-1]$中，$\omega_n+1$ 是该区间中的最小奇数，若 $\omega_n+1=p_\omega^+(n)$为阳性欧几里德素数，则 $p_\omega^+(n)$为 $I_d(n)$中的最小素数。

若 ω_n+1 不是素数，则有以下定理：

5.2 最小超序素数定理

$I_d(n)$中的最小超序素数 $\min p_\sigma^+ \geq \omega_n+p_{n+1}$。

为了证明以上定理，需先证明素数因子定理。

5.3 素数因子定理

若 x 为大于 1 且小于 p_{n+1} 的数，$1<x<p_{n+1}$。，则 x 必能被 p_1，p_2，…p_n 之 1 所整除。

证明：若 x 为素数。则只能为 p_1，p_2，…p_n 之 1，故能为 p_1，p_2，…p_n 之 1 所整除；若 x 为合数，其因子只能是 p_1，p_2，…p_n 之 1，故亦能为 p_1，p_2，…p_n 之 1 所整除。

设 $1<x<p_{n+1}$，由素数因子定理，x 必能被 p_1，p_2，…p_n 之 1 所整除，则 ω_n+x 亦必能被 p_1，p_2，…p_n 之 1 所整除，故 $\omega+x$ 不可能为素数，所以 $\min p_\sigma^+ \geq \omega_n+p_{n+1}$，即在 $I_d(n)$中的最小超序素数必大于或等于 ω_n+p_{n+1}。

5.4 最大减性超序素数

同理可证在 $I_d(n)$中，若 $\omega_{n+1}-1$ 不是素数，则其最大的减性超序素数 $\max p_\sigma^- \leq \omega_{n+1}-p_{n+2}$。

5.5 正规最小超序素数及正规最大超序素数

若 $p_c^+(n)=\omega_n+p_{n+1}$ 为素数，则称为 $I_d(n)$中的正规最小超序素数(canonical minimal super sequorial primes)。例如 3，5，11，37，30047，510529，9699713 等。是否有无穷多个 $p_c^+(n)$ 素数，称为正规最小超序素数猜想。同理，若 $p_c^-(n)=\omega_{n+1}-p_{n+2}$ 为素数，在称为 $I_d(n)$中的正规最大超序素数(canonical maximal super sequorial primes)。例如：23，199，30013，9699667 等。是否有无穷多个 $p_c^-(n)$素数称为正规最大超序素数猜想。

6. 欧几里德区间相关素数的综合猜想

6.1 阳性欧几里德素数猜想

是否有无穷多个阳性欧几里德素数 $p_\omega^+(n)=\omega_n+1$ ？

6.2 阴性欧几里德素数猜想

是否有无穷多个阴性欧几里德素数 $p_\omega^-(n)=\omega_n-1$ ？

6.3 欧几里德孪生素数猜想

是否有无穷多个欧几里德孪生素数 $T_\omega(n)=(\omega_n-1，\omega_n+1)$ ？

6.4 正规最小超序素数猜想

是否有无穷多个 $I_d(n)$的正规最小超序素数 $p_c^+(n)=\omega_n+p_{n+1}$ ？

6.5 正规最大超序素数猜想

是否有无穷多个 $I_d(n)$的正规最大超序素数 $p_c^-(n)=\omega_{n+1}-p_{n+2}$ ？

7. 结束语

大于 10 的 100 次方的大型素数，可以应用于构建 RSA 密钥的编码[3]。RSA 密钥是指给定 2 个大于 10 的 100 次方的素数 p_i 和 p_j 的乘积 $m=p_i\bullet p_j$，$i<j$。通过因子分解由 m 计算出 p_i 及 p_j 从而破解 RSA 密钥。由于因子分解的运算量很大，因此即使使用电子计算机亦无法求解。据估计对一个 10 的 400 次方的数 m 进行因子分解，用现有的电子计算机的运算速度求解，约需 100 亿年的时间。因此 RSA 密钥在目前是无法破解的。本文用超序素数生成公式可以方便的产生任意大的大型素数，对 RSA 密钥的编码有一定实用价值。

参考文献

[1] 盖伊(Guy R. K.)著，张明尧译. 数论中未解决的问题(第二版). 科学出版社，北京，2003，p.12
[2] Caldwell, C. K. The prime pages[J]. http://www.utm.edu/research/primes/,1993
[3] Silverman J. H. A friendly introduction to number theory(Third Edition)[J]. China Machine Press, Beijing 2006, p.117-121

Prime Sequorial and Generation Formulae Of Sequorial Related Primes

Chen Weichang[1], Chen Zhiyi[2], Chen Zhihua[1], Wang Ziqiang[1]
1 Institute of Clinical Medical Sciences, China Japan Friendship Hospital, Beijing PRC (100029)
2 National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, Beijing, PRC (100080)

Abstract

Prime sequorial is a continuous product of primes. The sequorial of *n*-th primes is called the *n*-th Euclid composite. According to Euclid composites, natural number series can be subdivided into Euclid intervals. Primes formed from the sum of Euclid composite and its successive primes are called the super sequoriql primes. A series of large primes can be generated from the generation formula of super sequorial primes and large primes can be used to code the RSA public key crytosystem in practice. Properties of related sequorial primes were discussed and a series of conjectures of sequorial related primes were also suggested.

Keywords: prime sequorial, Euclid intervals, super sequorial primes, generation formula of primes, RSA cryptosystem

作者简介：陈惟昌(CHEN Weichang，1932.05.06)，男，广东吴川市人。1955 年，北京大学医学院医学系毕业。1983 ~ 1984 年，美国洛杉矶加州大学(UCLA)医用电子计算机中心高级访问学者。历任卫生部中日友好临床医学研究所副所长兼生物物理研究室主任，中国生物物理学会常务理事，国家科技部重大基础研究项目(973)人口与健康领域咨询组专家，国家自然科学基金委员会生物物理与生物医学工程学科评审组长。现任中日友好临床医学研究所研究员，《科学通报》特邀编辑。1958 年在国内首先介绍新兴学科“生物学控制论”(biocybernetics)并率先开展针刺的电兴奋特性、脑电频谱分析、肌电幅谱分析和和心电图电子计算机识别与诊断以及心磁图等研究工作。参与中国第一台正电子发射断层图(PET)的研发工作,获 1995 年亚洲 CT 科技进步奖。提出神经信息二重编码理论以及大脑神经网络信息高维空间编码理论。开展大脑功能变化的激光拉曼光谱研究，发现遗传密码简并的高维空间连通性法则和提出 DNA 序列的高维空间数字编码法则，发表论文 80 余篇，E-mail：zychen63@gmail.com。