素数研究与应用

参考手册（第2版）

高红卫 著

科学出版社

素数研究与应用参考手册

（第 2 版）

高红卫　著

科学出版社

北　京

内 容 简 介

素数是数字的基因。本手册围绕素数研究与应用的若干核心问题，提供较为系统、较为深入的参考资料与相关统计分析数据。其中，“概述”简要地给出了素数研究的若干重要概念及若干最新研究成果；“基本数据表”主要面向素数的基础性研究；“部分区间素数统计数据表” 主要面向素数的专业性研究；“合数分割专题”以及“附录”内容，则主要面向加密/解密技术应用研究。为获得本手册数据内容所使用的创新性分析思路与方法，对于普及研究和应用研究均具有系统性的参考价值。

本手册适合于相关领域研究人员、工程技术人员、软件工程师、大专院校师生、中小学数学教师、数论研究爱好者、信息加密与解密技术工作者、相关研究爱好者阅读。

图书在版编目(CIP)数据

素数研究与应用参考手册/高红卫著．—2 版．—北京：科学出版社，2013
ISBN 978-7-03-036139-4

Ⅰ．素… Ⅱ．高… Ⅲ．素数-研究 Ⅳ．O156.2

中国版本图书馆 CIP 数据核字(2012)第 293058 号

责任编辑：魏英杰 杨向萍 / 责任校对：宋玲玲 刘小梅
责任印制：张 倩 / 封面设计：陈 敬

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司印刷
科学出版社发行 各地新华书店经销
*
2013 年 1 月第 一 版 开本：787×1092 1/16
2013 年 1 月第一次印刷 印张：37 3/4
字数：833 000

定价：98.00 元

（如有印装质量问题，我社负责调换）

第 1 版前言

这是一本兼顾研究与应用，关于素数的数据参考手册。并且就笔者所知，这是世界上关于素数研究与应用的第一本数据参考手册。

编著这本手册的动因，可以一直追溯到笔者在清华大学学习期间受到一篇关于数论研究的著名报告文学的影响，尤其是受到曾在清华从事数学教学与研究的钟家庆老师献身数学研究的精神感染。

素数是数字基因，它本身不能被因子分解，但它却是所有合成数的因子。整数是最基本的数字，除 0 和 1 以外，全部的正整数由全部的素数及其合成数构成。人类研究素数已经有几千年的历史，获得了数不尽的研究成果，这些成果广泛地惠及几乎所有科学技术领域，但是笔者没有查到任何专门的关于素数研究成果的数据参考手册。

近些年来，由于信息技术的发展和进一步发展信息技术的迫切需要，关于素数（含合数之素因子分解）的研究异常活跃，在数论及相关领域事实上已经掀起了新一轮世界性的竞争热潮（尤其是在数字加密与解密技术领域），世界各主要国家都在竞相争夺无限数字空间的无限宝藏。自古以来，中国都是数论研究大国，但是近些年我国的数论研究成果多为高深的专业性成果，普及研究的范围和深度与当代数论大国的地位多少有些反差。

正如一国的某项竞技体育运动水平高低很大程度上与这个国家民众普及该项运动的程度呈正相关特性一样，某些基础学科的理论研究水平也与参与研究的人数多寡及平均素质情况有一定的关联度。编著这本手册的目的，一方面是为满足相关研究机构、企业和专业人士展开和深化数论及相关领域研究的需要，另一方面也是为了满足广大数论研究爱好者对于比较系统的素数基础数据的渴望与需求，助推我国数论及相关领域研究的均衡发展。

为同时照顾基础研究和应用研究两个方面的需要，又限于篇幅，本手册包括了 $2\sim(1.26\times10^{12}+1)$、$(6\times10^{100}+2)\sim(6^{100}+1.08\times10^{11}+1)$ 两个区间关于素数、孪生素数、孪生素数族（按升序排列），以及素数间隙（按升序排列）等有关统计数据，包括了范围在 $6\times10^{5}+1$ 以内自然数中的全部素数，以及低端区间（3×10^{4} 个含≥5 素数）连续一阶合数表、低端区间（$3\times10^{4}+1$ 以内，含≥7 素数的）合数一次分解表。最后是 RSA-576、RSA-640、RSA-704、RSA-768、RSA-896、RSA-1024、RSA-1536 以及 RSA-2048 的完全素分割表。

本手册提供的数据，不仅在研究素数分布规律以及自然数的素性判定时经常用到，而且对于研究合数分解方法具有较高的应用价值。特别是给出的几个 RSA 大合数完全素分割表，能为分解 RSA 中的大合数提供有价值的参考——因为加法表达式与乘法表

达式之间存在确定的转换关系。

本手册的数据来源于笔者独立发现的、不同于经典算法的新算法自行生成的数据库。由于数据库的数据量巨大(TB数量级),无法一一列印出来,只能部分列举,需要超出本手册范围数据的读者可与笔者联系。

编著这本手册的工作量之巨大,超出笔者初期的想象。由于笔者找到了一些不同于经典理论的(相对快速)分析方法,所以直到近期相关分析计算工作才得以迅速进展。在经历了无数个不眠之夜和紧张忙碌的周末之后,虽然摆在读者面前的只是一本不起眼的小册子,但是笔者为此投入的精力却是巨大的。

令笔者感到非常欣慰的是,毕竟它(凝聚了前人成果和本人心血的手册)出版了,能够与大家分享研究成果,实为一件快事。在此,我要特别感谢科学出版社的支持,使得这本手册能以最快的速度出版发行。当然我还要特别感谢我的妻子和家人,她和他们忍受了因为计算机满负荷运行而产生的日夜不停的噪声,并承担了全部繁琐而细致的家务,且对于不断更新计算机系统的开销和不断攀升的电费支出,以及不能陪同他们享受完整节假日及业余生活,都没有任何抱怨,使笔者能够把业余时间的主要精力和较大份额的家庭收入用于业余研究。对此,笔者十分感激。

由于本手册初次编著,限于笔者的能力,也没有成体系的参考与借鉴资料,并且在将大量原始数据表格化的过程中,笔者虽尽全力避免出现数据转录错误,但是由于数据量巨大,错误和疏漏在所难免,还望读者不吝指正,以便在将来有机会修订这个手册时充实、完善。

笔者邮件地址:gaohw191@sina.com

2008年元旦于北京　航天大院

第 2 版前言

随着科学技术与社会生活信息化、数字化的不断深入发展，人类将面临“数字无孔不入，数据无处不在”的机遇与挑战。目前国际上掀起研究开发大数据(big data)的热潮。2012 年 3 月 29 日，美国政府六部委(国家科学基金会 NFS、国家卫生研究院 NIH、能源部 DOE、国防部 DOD、美国地质勘探局 USGS、白宫科技政策办公室 OSTP)发布了“大数据研发倡议”，并新增 2 亿多美元投资，旨在鼓励美国的科研机构与研究人员开发对大数据进行访问、组织、检索的工具与技术，提高美国相关领域从大量复杂数据中获取信息、汲取知识的能力，从而确保美国在日新月异的信息化、数字化时代继续引领世界科技创新与生产方式、生活方式变革的潮流。目前，我国科技界也开始关注大数据的概念研究与应用研究，相信一旦形成政府与全社会的共识，我国的大数据研究、开发与应用也将出现蓬勃发展、欣欣向荣的局面。

大数据通常指那些规模与复杂性超常的数据集。素数是数字的基因，其规模与复杂性都是超常的。通过已知素数可以发现新的素数、偶数及奇合数。由于素数集的元素趋于无穷多，且素数在整数中的分布“无规则”，因此素数集理所当然地属于大数据的范畴。

在本手册中读者将会看到，事实上素数在整数中的分布并不是通常认为的那样“无规则”，它们在整数中的分布满足确定的精确规则，这或许是本手册提供给读者最有价值的信息；其次，素数对于偶数的求和表达等数论研究的基础性问题，本手册也给出了相关研究成果及其分析数据，这对于深化数论相关问题的研究提供了一个全新的视角。

素数在信息技术与数字化技术中发挥着不可替代的重要作用，因此对于素数的研究与应用，一直受到学界与研究爱好者的高度重视。本手册的第 1 版出版发行后，得到读者的肯定，作者深受鼓舞。许多读者来函询问研究进展情况与研究方法、索要用于进一步研究的相关数据，以及联系合作研究事宜等。

考虑到素数研究领域成果日新月异，读者需要的数据内容也在发生变化，为满足读者需要，同时反映最新研究成果，作者重新编写了这本手册。

与第 1 版相比，第 2 版的内容作了如下主要变动：

首先，将第 1 版第 3 篇的“低端区间分析数据表”合并改编为“2～12001 区间素数与奇合数完全分解混编数据表”，内容更加精炼，并方便于读者查阅与使用；新增了“部分胚数、素数、合数之参数配合表”和“基本表达式生成合数相关参数对照表”，以便揭示素数在胚数(乃至整数)中的分布规律。为了揭示素数求和表达偶数的规律，还新增了“$[p_1, p_k]$区间素数求和表达$[2p_1, 2p_k]$区间偶数冗余表达式数量表”以及“从$[p_1, p_{k-1}]$向$[p_1, p_k]$过渡形成的素数求和表达式覆盖$[2p_{k-1}, 2p_k]$偶数分析表”。同时将第 2 篇与第 3 篇的顺序进行了对调，使得查阅使用更加流畅与自然。

其次，对第 1 版第 1 篇的内容进行了大幅扩充，并对原内容进行了适应性修订。其中包含了作者的最新研究成果，以及与手册中数据内容相关的基础性概念、查阅范例，同时还给出了一些延伸研究成果与应用方向提示，以便有特殊需求的读者参考使用。

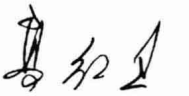
第三，第 2 版对“附录”内容进行了更新和补充，给出了 RSA 实验室列举的全部 RSA 数字及其基本参数，并且对手册第一版出版后分解 RSA 合数取得的新进展也全部予以更新。为方便读者对于大合数快速分解规律的研究，对应地在第 4 篇修订并增补了：RSA-330至 RSA-2048 方幂分割与素分割数据表；RSA-330 至 RSA-2048 作为胚数的类别、素因子结构、Δv 值、m 值及其性质。

第四，补正了在第 1 版内容中发现的错漏。虽然篇幅与第 1 版大体相当，但第 2 版比第 1 版的编排更为合理，内容更为丰富。

作者对于第 1 版中存在的瑕疵给读者带来的不便表示歉意，同时对于读者的批评与建议表示感谢。欢迎读者继续就本手册的内容提出批评建议，以便今后有机会再次完善充实。

本手册第 2 版的出版，得益于科学出版社的支持，得益于同事、朋友与读者的热情鼓励，也得益于家人的一贯宽容与奉献，在此一并致谢。

作者邮箱地址：gaohw191@sina.com



2012 年 7 月 15 日于北京

目　录

第1篇　概　　述

为了读者查阅本手册时了解相关数据的含义及运用方法，本篇提供了与数据获取、查阅、使用密切相关的信息，并给出了若干重要概念的简要推导过程。

§1.1 关于 n 选 2 奇素数求和及 n 个奇素数自求和表达≥6 的偶数

公理 1 任何 2 个整数之和必为整数。

引理 1 根据公理 1，整数 1 次不定方程 $a+b=c$ 必有整数解，且对于 a、b、c 中 2 个变量取确定值而言，方程仅有唯一的解；对于 a、b、c 中仅 1 个变量取确定值而言，方程至少有 1 个解。

公理 2 任何 2 个奇数之和必为偶数。

推论 1 设 j 为任意大奇数，根据公理 1、2 以及引理 1 知，闭区间[1，j]中任意 2 个整数之和必为≥2 的偶数；若 c 为≥2 的偶数且值确定，则至少有 1 对奇数求和的表达式与之对应。

证明：

记奇数 1 为 j_1，奇数 3 为 j_2，则奇数集合$\{j_1,\cdots,j_i,\cdots,j_k\}$(以下简记为$[j_1,j_k]$)中元素与偶数集合$\{2j_1,\cdots,2j_i,\cdots,2j_k\}$(以下简记为$[2j_1,2j_k]$)中元素是一一对应的。因为对于每一个 i，$1\leqslant i\leqslant k$，$[2j_1,2j_k]$中的偶数，可按升序以下述两种形式为一组循环递进由奇数求和表达：j_i+j_i，j_i+j_{i+1}，直至最后一组时舍弃 j_k+j_{k+1}(因为它不是$[2j_1,2j_k]$的元素)，即可获得$[j_1,j_k]$中元素与$[2j_1,2j_k]$中元素的一一对应关系。推论 1 成立。证毕。

设 p 为任意大奇素数，由于奇素数集合 $G=[3,p]$之元素必皆为奇数，根据公理 1、2 以及引理 1 知，奇素数集合[3，p]中任意 2 个元素之和必为≥6 的偶数。

命题 1 对于偶数集合 $H=[6,2p]$中的任意元素，至少存在 2 个奇素数求和或者 1 个奇素数自求和的表达式与之对应。

证明：

(1) 首先研究 $G=[3,p]$中素数 n 选 2 互求和及素数自求和能否完整表达偶数集合 $H=[6,2p]$中的偶数问题。

(2) 考虑到集合 G 的元素 n 选 2 求和表达式个数为 $\binom{n}{2}=\dfrac{n!}{(n-2)!\ 2!}$，再考虑 n 个元素自求和表达式个数为 n，则集合 G 的元素通过特定求和运算表达偶数的表达式总数为 $\binom{n}{2}+n=\dfrac{n!}{(n-2)!\ 2!}+n=\dfrac{n(n-1)}{2}+n$，记为 d。

(3) 集合$[6,2p]$中≥6 的偶数个数为 $\dfrac{2p}{2}-2=p-2$，即 $2p$ 及以下的全部偶数中仅将 2 及 4 排除在外，记为 $f=p-2$。

(4) 性质判断：设 $d=f$，即 $\dfrac{n(n-1)}{2}+n-(p-2)=0$，解此整数不定方程，得到一个

解为 $p=\frac{1}{2}(4+n+n^2)$，其中 p 为素数。这意味着如果恒等式 $d\equiv f$ 存在，则 p 必为素数。然而不难验证，仅当 $n=4a+1$ 及 $n=4a+2(a\geqslant 0$ 为整数)时 p 为奇数，且并非全部为素数；当 $n=4a+0$ 及 $n=4a+3(a\geqslant 0$ 为整数)时 p 为偶数(仅仅 $n=4a+0$ 且 $a=0$ 时可表达唯一偶素数 2)。这表明 $d\equiv f$ 并不成立，集合 G 的元素对集合 H 元素进行求和表达不存在像推论 1 中那样的简单一一对应关系，或者说集合[3，p]中的素数求和表达集合[6，$2p$]中的偶数不能采用证明推论 1 成立的方法。

(5) 以下解析集合 G 的元素对集合 H 元素进行求和表达不存在简单一一对应关系的具体证据。

(6) 记 $m=d-f=\frac{n(n-1)}{2}+n-(p-2)$ 为集合 G 的元素对集合 H 元素表达的冗余表达式数量。

设 k 为集合[3，p]中素数的升序序数，第一个奇素数 3 记为 p_1，第 n 个奇素数 p 记为 p_n，G 的任意一个元素记为 p_k，$1\leqslant k\leqslant n$，则有集合[p_1，p_k]中 2 个元素互求和与某个元素自求和表达集合[$2p_1$，$2p_k$]中偶数的表达式冗余个数为 $m_k=d_k-f_k=\frac{k(k-1)}{2}+k-(p_k-2)$。

(7) 奇素数集合[3，p_k] 中全部元素所能形成的求和表达式个数满足以下关系式 $q_k=5+\frac{(k^2+k-6)}{2}$。同时，当 $k\geqslant 2$ 时，等价地有 $q_k=p_k+m_k=5+\sum_{i=3}^{k} i$。这两个等式表明，奇素数集合[3，$p_k$] 中全部元素所能形成的求和表达式个数是确定的，且集合[3，p_k] 中 k 取每个确定值时所能形成的求和表达式的冗余数量也是确定的，即 $m_k=\frac{k(k-1)}{2}+k-(p_k-2)$。等价地，存在以下几种形式，即 $m_k=\sum_{i=3}^{k} i-p_k+5$，$m_k=5+\frac{(k^2+k-6)}{2}-p_k$ 以及 $m_k=\frac{1}{2}(4+k+k^2-2p_k)$。

(8) 虽然 $k\geqslant 3$ 时，$m_k\geqslant 1$，但这并不意味着集合[p_1，p_k]中奇素数求和表达集合[$2p_1$，$2p_k$]中偶数必然地具有完整覆盖性。事实上，当 $k=4$ 时，$p_4=11$，$q_4=12$，$m_4=1$；但与此同时，被遗漏的偶数个数为 1，即[$2p_1$，$2p_k$]中的偶数 20 并不能被{3，5，7，11}任意配对求和与自求和表达式所表达。这表明，闭区间[p_1，p_k]中奇素数集合元素求和表达集合[$2p_1$，$2p_k$]中偶数存在着数量“冗余”与“覆盖不完全”两种情形。

设 $\geqslant p_1$ 且 $\leqslant p_k$ 的奇合数个数为 x。相对于 $\geqslant p_1$ 且 $\leqslant p_k$ 的全部奇数 k 选 2 求和及自求和表达式而言，奇合数被剔除所减少的求和表达式个数为 $y_k=\frac{x(x-1)}{2}+x+kx$，而剔除奇合数之后的集合[$p_1$，$p_k$]中所包含的奇素数求和表达式数量为 $q_k=\frac{k(k-1)}{2}+k$，其中，$k\geqslant 1$，$x\geqslant 0$。不难验证，当 $k\geqslant 9$ 时，$y_k>q_k$，即 $p\geqslant 29$ 时，因奇合数被剔除所减少的求和表达式个数就稳定地多于奇素数求和表达式数量。这说明，以集合[p_1，p_k]为基础的奇素

数求和表达式表达集合$[2p_1,2p_k]$中偶数必然存在遗漏。

(9) 以下研究集合$[p_1,p_k]$中元素求和表达集合$[2p_1,2p_k]$中偶数的遗漏规律(仅仅了解 k 取部分值时遗漏表达的偶数数量)。当 k 取值为 1～20 时,对应的遗漏表达的偶数数量分别为 0,0,0,1,0,1,0,1,4,1,4,2,1,1,4,7,2,4,3,1。由此可知,$[p_1,p_k]$中奇素数集合元素求和不可能完整表达集合$[2p_1,2p_k]$中的偶数确认无疑。

(10) 上述研究表明,欲确保奇素数配对求和及自求和表达集合$[2p_1,2p_k]$中的偶数无遗漏,必须突破集合$[p_1,p_k]$的取值约束。以下研究突破闭区间$[p_1,p_k]$取值限制,以$[p_1,p_{k+a}]$中素数互求和及自求和表达闭区间$[2p_1,2p_k]$中全部偶数的可能性。

(11) 设两个相邻奇素数 p_{k-1}与 p_k 之间的奇合数个数为 x,$x\geqslant 0$。当 x 个奇合数被剔除时,考虑扩大素数范围来构造求和表达式予以弥补。问题的关键是:扩大素数范围构造求和表达式是否足以完整地弥补$[2p_1,2p_k]$中因剔除两个素数之间所包裹的 x 个奇合数而遗漏表达的偶数。

(12) 要证明扩大素数范围构造求和表达式足以完整弥补$[2p_1,2p_k]$中因剔除两个素数之间所包裹的 x 个奇合数所遗漏表达的偶数,首先必须证明:两个素数之间所包裹的奇合数个数 x 是有限的。

我们已经知道,素数的个数是无限的。“素数个数是无限的”这个论断包含了“两个素数之间所包裹的奇合数个数是有限的”这个论断。因为如果两个素数之间所包裹的奇合数个数是无限的,那么就必然存在最大的素数(包裹无限个奇合数的两个素数中低端素数就是最大的素数,高端素数是否存在不可知);而如果存在最大的素数,则素数个数就是有限的。因此逻辑上讲,承认“素数个数是无限的”,就必须承认“两个素数之间所包裹的奇合数个数是有限的”。因此,逻辑上讲,存在足够多的素数可以满足扩大素数范围构造求和表达式,可以完整弥补因剔除两个素数之间所包裹的奇合数所遗漏的集合$[2p_1,2p_k]$中的偶数。

(13) 要证明扩大素数范围构造求和表达式足以完整弥补$[2p_1,2p_k]$中因剔除两个素数之间所包裹的奇合数而遗漏表达的偶数,首先必须证明:以$[p_1,p_{k+a}]$中素数互求和及自求和表达集合$[2p_1,2p_k]$中全部偶数,a 一定是有限值。

设 p_k 为任意大素数,则 $2p_k$ 为任意大偶数;无论如何,p_k 必取某一具体数值(否则不能判定其素性),$2p_k$ 也必取某一具体数值。如果以$[p_1,p_{k+a}]$中素数互求和及自求和表达集合$[2p_1,2p_k]$中全部偶数,则意味着 a 一定是有限值,否则不能判定 p_{k+a}的素性。

(14) 综上所述,当素数序号 k 为任意值时,集合$[p_1,p_k]$中的素数求和不能完整地表达集合$[2p_1,2p_k]$中的偶数;集合 $[p_1,p_{k+a}]$中的素数求和可以完整表达闭区间$[6,2p_k]$中的全部偶数,其中 a 取有限值。命题 1 成立。证毕。

第 2 篇中所列“$[p_1,p_k]$区间素数求和表达$[2p_1,2p_k]$区间偶数冗余表达式数量表”给出了 $1\leqslant k\leqslant 1437$(对应闭区间[3,11987]的素数 k 选 2 求和及 k 次自求和表达闭区间[6,23974]偶数之冗余表达式数量 m_k,供读者查阅。

第 2 篇中所列“从$[p_1,p_{k-1}]$向$[p_1,p_k]$过渡形成的素数求和表达式覆盖$[2p_{k-1},2p_k]$偶数分析表”给出了 $3\leqslant n\leqslant 501$ 时所对应的 x 值(p_{k-1}与 p_k 之间的奇合数个数)及 y 值($[2p_{k-1},2p_k]$中未被求和表达式覆盖的偶数个数)对照表,供读者查阅。

§1.2 关于基于 3 的胚数表达≥7 的素数

胚数数列指由全部奇素数与部分奇合数混合构成的数列。

引理 2 在自然数中,≥7 的奇数数列只有一个,该奇数数列可由以下三个数列$PS_{3-}=(3^2-2)+2\times3\times m_{3-}$,$PS_3=3^2+2\times3\times m_3$ 以及 $PS_{3+}=(3^2+2)+2\times3\times m_{3+}$联合表达,其中,$m_{3-}$、$m_3$ 以及 m_{3+}皆取包含 0 在内的正整数。

证明:当 $m_{3-}=m_3=m_{3+}=0$ 时,3 个数列的首项分别为 $ps_{3-}=7$,$ps_3=9$,$ps_{3+}=11$;作为项差皆为 6 且首项值递差为 2 的等差数列,3 个等差数列的元素合并形成一个新的等差数列,该数列的首项为 7,数列之等差值为 2,即有 $PS_{3-}\oplus PS_3\oplus PS_{3+}=2k_{3\oplus}+1$,$k_{3\oplus}\geqslant3$。其中,⊕表示 3 个数列并列且 3 个数列值按升序规则依次排列。证毕。

引理 3 数列 $PS_3=3^2+2\times3\times m_3$ 为合数数列。

证明:因为 $PS_3=3^2+2\times3\times m_3=3(3+2m_3)$,所以无论$(3+2m_3)$中的 m_3 为何整数,PS_3 皆包含素因子 3,因此 PS_3 为合数数列。证毕。

为便于研究,以下将包含素因子 3 的胚数数列记为 HS_3,读作基于素数 3 的合数数列。

推论 2 数列 $PS_p=p^2+2\times p\times m_p$ 为基于素数 p 的合数数列。

命题 2 数列 PS_{3-}与 PS_{3+}包含了≥7 的全部素数。

证明:≥7 的素数必为奇数,由引理 2 及引理 3 知,PS_{3-}与 PS_{3+}包含了除基于 3 的合数之外的≥7 全部奇数,因此数列 PS_{3-}与 PS_{3+}包含了≥7 的全部素数。证毕。

定义 $PS_{3-}\oplus PS_{3+}=PS$,称 PS 为胚数数列。

推论 3 任何素数都是胚数数列 PS 的元素。

命题 3 属于胚数数列 PS 元素的奇数不一定是素数。

证明:假设属于胚数数列 PS 元素的奇数一定是素数。由于当 $m_{3-}=3$ 以及 $m_{3+}=4$ 时即存在反例,说明假设不成立,命题 3 成立。证毕。

命题 4 胚数数列 PS 中包含的合数皆可由合数数列 $HS_P=p^2+2\times p\times m_p$ 表达,其中 $p\geqslant5$,$m_p\geqslant0$。

证明:由于胚数数列 PS 不包含基于 3 的合数数列 HS_3,且由于 HS_p 在 $p\geqslant5$,$m_p=0$ 时值为 p^2,这表明胚数数列 PS 的取值在 p^2 以下不包含基于 p 的合数数列 HS_p 的项,而在 p^2 以上,基于 p 的合数数列 HS_p 覆盖了值为 p^2 的为首项、等差值为 $2p$、基于 $p\geqslant5$ 且不含素因子 3 的全部奇合数。

由于素数的约束条件是 $p\geqslant5$,所以当 p 取下一个任意大素数时这种关系仍然存在,

故命题得证。证毕。

推论 4 素数数列是胚数数列 PS 诸值剔除全部基于 $p\geqslant 5$ 的合数数列 HS_p 并列诸值之后形成的数列。

称自然数列元素为自然数集合 N，胚数数列 PS 元素为胚数集合 W，胚数集合 W 是自然数集合 N 的子集，$W\subset N$，$P\subset W$；基于 $p\geqslant 5$ 的诸合数数列 HS_p 元素集合 V 与素数集合 P 同为胚数集合的子集，$V\subset W$，且素数集合 P 是基于 $p\geqslant 5$ 的诸合数数列 HS_p 元素集合 V 对于胚数集合 W 的余集，$V\oplus P=W$。

§1.3 关于素性判定、合数分解与素数生成

§1.3.1 素数的无限性

定义 1 若自然数只能被 1 及自身整除，且不能整除大于自身的全部自然数，则称其为素数。

定义 2 可以分解为 2 个及 2 个以上素数相乘形式的自然数称为合数。

虽然 1 不能被大于 1 的任何自然数整除，但 1 能整除全部自然数，因此 1 不是素数。

虽然 1 可以分解为两个及两个以上因子 1 相乘形式，但相乘的因子 1 不是素数，因此 1 不是合数。

自然数 1 既不是素数，也不是合数，它是一个兼具素数与合数部分性质的特殊自然数。

公理 3 一个自然数不能被大于这个自然数的其他自然数整除。

自然数 2 只能被 1 及自身整除，且不能整除大于 2 的全部自然数（不能整除任何奇数），所以 2 是素数。

自然数 3 只能被 1 及自身整除，且不能整除大于 3 的全部自然数（不能整除任何偶数），所以 3 是素数。

自然数 4 能被 1、2 及自身整除，所以 4 不是素数。

自然数 5 只能被 1 及自身整除，且不能整除大于 5 的全部自然数（不能整除任何最低位不含数字“5”及“0”的数），所以 5 是素数。

自然数 6 能被 1、2、3 及自身整除，所以 6 不是素数。

自然数 7 只能被 1 及自身整除，且不能整除大于 7 全部自然数（例如不能整除 8），所以 7 是素数。

自然数 8 能被 1、2、4 及自身整除，所以 8 不是素数。

自然数 9 能被 1、3 及自身整除，所以 9 不是素数。

由于最低位含有数字“0”的数皆为偶数，凡偶数皆可被 2 整除，所以最低位含有数字“0”的数皆不为素数，故自然数 10 不是素数。

自然数 11 只能被 1 及自身整除，且不能整除大于 11 的全部自然数（例如不能整除 12），所以 11 是素数。

余类推。其中，素数第一性质区别于合数，素数第二个性质区别于特殊自然数1。

自然数列既包含了所有的素数，也包含了所有的合数，还包含了既具有素数的部分性质（只能被1和自身整除），也具有合数的部分性质（可以分解为两个及两个以上自然数相乘形式）的特殊自然数“1”。

自然数列的通项表达式为 psn=1+1n，n=0,1,2,…。

偶数数列可以视为从自然数列中排除了全部奇数的数列。特定情况下，数字0可以作为偶数数列的首项（尽管0并不被普遍认为是自然数）。偶数数列仅包含一个素数，这个素数就是唯一的偶素数2。

偶数数列的通项表达式为 pse=0+2n，n=0,1,2,…。

奇数数列可以视为从自然数列中排除了全部偶数的数列。奇数数列包含了所有的奇素数，但不包含唯一的偶素数2。

奇数数列的通项表达式为 pso=1+2n，n=0,1,2,…。

实际上，存在若干这样的数列，它们组合在一起之后，可以排除一部分（低端）素数，但是包含剩余的全部（高端）素数。

例如，psd0=1+6n，psd1=5+6n，n=0,1,2,…。

数列组合 psd=psd0 ⊕ psd1 是一种奇数数列，同 pso 一样，它不含2这个唯一的偶素数，同时它还排除了排序第一的奇素数3以及包含素因子3的全部奇合数。

相似地，还有

pst0=1+30n，pst1=7+30n，pst2=11+30n，

pst3=13+30n，pst4=17+30n，pst5=19+30n，

pst6=23+30n，pst7=29+30n

n=0,1,2,…。

数列 pst=pst0 ⊕ pst1 ⊕ pst2 ⊕ pst3 ⊕ pst4 ⊕ pst5 ⊕ pst6 ⊕ pst7 是一种奇数数列，同 pso 一样，它不含2这个唯一的偶素数，同时它还排除了排序处于低端的2个奇素数{3,5}以及包含素因子3和5的全部奇合数。

总结一下上述概念：自然数列 psn 包含全部素数，项差值为1，在整个数列中项差均匀分布；偶数数列 pse 包含1个素数2，项差值为2，在整个数列中项差均匀分布；奇数数列 pso 不包含素数2，但包含其余素数，项差值为2，在整个数列中项差均匀分布；由于 pse 与 pso 首项值差为1，且各自的项差值均为2，当 n=0,1,2,…时，这两个等差数列可以合并，合并的结果得到自然数数列，即 pse ⊕ pso=psn。

这给了我们一个启发：首项值不同、等差值相同的数列，在 n=0,1,2,…条件下，适当个数的数列可以合并为另一个具有全新意义的数列。

例如，psd0 ⊕ psd1=psd。psd 是这样一种数列，它是奇数数列，数列的项差值为4+2分布（即任意两个数项组合的差值为6，其中单数序号项与双数序号项之间差值为4，双数序号项与单数序号项之间差值为2）。

相似地，有 pst0 ⊕ pst1 ⊕ pst2 ⊕ pst3 ⊕ pst4 ⊕ pst5 ⊕ pst6 ⊕ pst7=pst，pst 的项