

Logical number theory



逻辑数论

姜月乾 著

Jiang Yue-qian

知识产权出版社

责任编辑: 罗家光
封面设计: 陈 弘

开拓数论的新理论

ISBN 7-80011-513-5



ISBN7-80011-513-5/O·001

定价: 16 元

逻辑数论

姜月乾 著

1999年3月6日

图书在版编目 (CIP) 数据

逻辑数论 / 姜月乾编著. — 北京: 知识产权出版社, 2000.12

ISBN 7-80011-513-5

I. 逻… II. 姜… III. 布尔代数—代数数论
IV. 0153.2

中国版本图书馆 CIP 数据核字(2000)第 81707 号

书名: 逻辑数论

著作责任者: 姜月乾

责任编辑: 罗家光

书号: ISBN 7-80011-513-5 / O · 001

出版发行: 知识产权出版社

地址: 北京海淀区西土城路 6 号 邮编 100088

印刷: 知识产权出版社制印中心

规格: 850×1168 毫米 大 32 开本 7 印张 130 千字

印数: 1—1000 册 2000 年 12 月第一版 2000 年 12 月第一次印刷

定价: 16 元

目 录

内容简介

序

前言

符号表

一、基本概念和引理…………… (17)

1. 基本概念

2. 基本引理 1 - 15

二、素数列的逻辑数串表示…………… (40)

1. 定义

2. 素数列的逻辑数串表示

3. 素数筛法的逻辑数串表示

三、素数定理的证明…………… (43)

四、“1 + 1”问题的证明…………… (46)

五、双素数问题的证明…………… (49)

1. 移位定义

2. 移位运算的性质

3. 定理、双素数有无穷个

六、“ $i + k$ ”问题	(52)
1. 定义 1.2.3	
2. 引理 16.17.18.19.20.21	
3. 合数的逻辑数串	
4. “ $1 + 2$ ”定理证明	
七、等差级数的素数问题	(60)
1. 引理 22	
2. 定理证明	
八、Mersenne 数问题	(63)
1. P 的幂数列的逻辑数串表示	
2. 定理证明	
九、Fermat 数问题	(66)
1. 2^{2^i} 数的逻辑数串表示	
2. 定理证明	
十、Fermat 大定理	(71)
1. 合数幂数列的逻辑数串表示	
2. 数的 k 次方幂的逻辑数串表示	
3. 三项式幂指不定方程的一般表示	
4. 定理证明	
十一、黎曼猜想	(80)
十二、素数分布相似定理	(88)

十三、数的素性检查和分解	(91)
十四、余新河猜想的证明	(99)
十五、信息的保密传输	(110)
附录 1:海明距离和素数分布(摘要)	(111)
附录 2:当 $0 \leq n \leq t$ 时, g_{up}, g_{low} 解的全部公式	(147)
参考资料	

内容简介

本文以逻辑代数为基础,建立了一个新的数学理论方法;它以巧妙的方式,对数论中的传统的、被认为是难以证明的,或者证明也是异常繁杂的论题,能给出明晰的表示和简洁的证明。如素数定理、哥德巴赫猜想、黎曼猜想等。

素数分布问题是数论研究的课题,逻辑代数仅用“1, 0”研究逻辑式的“真,伪”问题。将二者统一起来,正是本文的巧妙之处。

本文第一部分内容,论述了独立的数学方法体系,建立了由“0,1”组成的 n 位逻辑数串、周期逻辑数串、及相应的逻辑运算理论,创立并证明了 15(其它各部分是 11 个)个基本引理,它们构成了崭新的、完整的理论方法体系。

本文的第二部分内容,是论述如何将求素数的筛法,转变成逻辑数串表示的逻辑筛法,于是便产生了素数的逻辑数串,哥德巴赫逻辑数串等等;它们完全可用第一部分的理论来研究。逻辑数串可以描述素数分布,又是逻辑运算的对象,它就是巧妙地统一点。

这个特点,使本理论方法,用于表示那些素数分布的传统、古老论题(如素数定理、哥德巴赫猜想等)时,明快、简练。

本文第三部分是本理论用于研究素数定理的实例。

本文第四至第十一部分分别探讨证明“ $1+1$ ”、“ $1-1$ ”、“双素数”、“ $i+k$ ”、“等差级数中的素数”、“Mersenne 数”、“Fermat 数”、“Fermat 大定理”、“黎曼猜想”等问题。

序

本书作者姜月乾先生 1964 年毕业于中国科学技术大学,所学专业是理论核物理。曾在国防科研单位工作多年,后转而从事计算机软件工作,并长期担任计算机软件企业的领导。

作者作为一位电脑软件专家,并非专业的数学家,然而由于他对数学问题的爱好,使他在探讨海明距离时,发现它和数论中诸多顶尖难题的联系,于是形成了“逻辑数论”的思考。特别是已故数学家潘承洞先生在他的一本科普读物“素数分布与哥德巴赫猜想”中写道:“不仅现有的方法不适用来解决‘ $1+1$ ’,而且到目前为止,还看不到沿着什么途径、利用什么方法来解决它。”这更激发起他探索这个思路的信念。本书是作者几乎用去他 20 多年的业余时间辛勤耕耘的结果。

“逻辑数论”是一个崭新的概念,以往也没有人利用类似方法来研究顶尖的数论难题。

“逻辑数论”是对“逻辑代数”和“数论”的融合,为什么这样说?因为:

1 “逻辑数论”是对“逻辑代数”的扩展,它吸取了若干计算机科学中的概念和算符,并加以发展,诸如:逻辑数串、单位逻辑数串等概念以及对于数串的运算符,诸如倒置、移

位等。也就是说在“逻辑数论”中将算符 CPU 化了。

2 作者为了使“逻辑数论”方法既可作逻辑运算又可作数字运算,发展了 15 个引理,从而使“0,1”数串的运算,既可表现出数串运算结果的特性和性质,也可表示出在数串中“0,1”的分布规律,并且反映出与自然数的对应关系,使“0,1”数串不仅是一个逻辑标识符,而且具有了数的意义。特别是建立了周期逻辑数字串的概念后,它就隐含了数论中同余式的概念。从而确立起“逻辑数论”中“逻辑数串”与“数论”中自然数列、同余式的等价关系。于是对“数论”中的一些问题、转而可用“逻辑数论”的方法去研究。这也是本书起名【逻辑数论】的一个原因。

3 作者借鉴传统数论中的“素数筛法”,把它逻辑化,而且把筛法的思想推广到幂数列中,建立了幂数列的“逻辑筛法”。从而将“数论”中的许多著名的问题,如“Mersenne 数”,“Fermat 数”,“Fermat 大定理”等等都纳入了“逻辑数论”的理论中,这是作者认为“逻辑数论”是对“数论”的融合的地方。

4 两个周期逻辑数串的周期 t_1, t_2 互素,则逻辑乘或逻辑加后的新逻辑数串仍为周期数串,且周期为 $t_1 t_2$ 。这正是充分表明了一个数学公理:同一个起点,每两米站一个人,每三米站一个人,在六米处要站两个人了。正是这个公理,“逻辑数论”中,可以用数串的逻辑运算进行演绎,获得定性的结果,又可以通过计算数串中的“0,1”的数目,求出定量的结果,运用极限理论定出阈值,从而解决要证明的问题。或许这正是“逻辑数论”的整个理论和对具体问题的分析都很简洁的原因。没有太艰深繁难的方程和计算。而且作者发现,诸如:素数定理、 $1+1$ 、 $i+k$ 、双

素数、Mersenne 数、Fermat 数、Fermat 大定理、哥德巴赫猜想、黎曼猜想等等，在数论中的顶尖难题，竟是“一棵树上的果子”，都可用逻辑数论予以表示和证明。

数论中的难题几乎被所有“趣味数学”的书作为题材，其原因是这些难题叙述上都很简洁，提出来很引人兴趣，但因证明极为繁难，所以既吊人胃口，又高山仰止，这更吸引了一代又一代的各类业余爱好者，乐此不疲地参与。作者本属专家中的业余爱好者，仅献此书以飨读者，希望数学的业余爱好者也能看懂。共享这本不厚的书中居然令人难以置信地证明了如此众多的数论尖端难题。或许是“他山之石，可以攻玉”的奇效吧！这种事例科学史上并不少见。我相信本书的出版将引起国内外强烈反响，业余数学爱好者将饶有兴趣地读完此书，而不是对顶尖数论难题望而却步，并从中获得鼓舞和启发。国内外数论专家必将仔细审查，任何建议均欢迎。由於本书对基本数学问题提出了新的想法和作一种新的尝试，错误和不妥的观点在所难免，批评和建议请直言相告。如果本书可以起到抛砖引玉的作用，我相信本书作者会非常高兴。

孙亲仁

1999.8.20

前 言

“逻辑数论”就是要用逻辑代数方法,对数论中的问题进行表示和证明。这些问题是“素数定理”,“ $1+1$ ”,“ $i+k$ ”,“ $1-1$ ”“双素数”、“等差级数中的素数”、“Mersenne 数”、“Fermat 数”及“Fermat 大定理”、“黎曼猜想”等。

作者在二十年前,曾探讨过“海明校验”,由此建立起来的“海明距离”的分析方法,恰与以上各问题有密切的关系,并以“海明距离和素数分布”(上、下)为题,发表在“北京计算机”80年,81年第一期上。文章中对核心“引理 10”的证明方法别具一格,其摘要收在本书附录中。这次重新整理后,本书的核心引理 13 的证明使用了新的技巧,常系数的求取是独立取得的,也就能把素数定理的证明也包括在本书中了。

书中理论基础是第一部分,由 15 个基本引理构成,回答了在什么情况下,逻辑数字串中的“1”的个数是可求得,这样一个基本问题。这个问题表面上与数论没有什么关系,但实质上却有着深刻的内在联系。这种内在联系是由书中第二部分揭示的,其中心是完成了素数筛法的逻辑数字化,那么数论中的诸多问题就可以用这里的理论来一一描述,表示和证明。这就是第三,四,五……部分的内容,当然在以后的各部分中,根据问题的本身特点,前后又增加了 11 个引理,但它们不完全属于逻辑数字

串运算规律的。

这个理论方法能表示这一系列的问题,至少说明它们的难度都属于一个水平,或者说其难度的根源是一个。这就是传统的数论方法,用公式表示这些问题是不方便的。数论的问题都有这样一个特点,就是说用文字或语言就可以说清楚,甚至有点算术知识的人都会明白,可证明起来,已经消耗了不知多少天才的智慧而无结果,这也是它们魅力和兴趣所在吧。

本书讲述的方法简明,逻辑上是简洁的,没有复杂的公式推导,不是高深莫测的,有点布尔代数知识的人,都可以看懂。在本质上它是初等的,为方便读者,对每个问题,简述了历史源由。同时为读者方便查阅本书使用的数学符号的含义,附一个符号表于次。

在本书成稿过程中,孙亲仁教授、张锡珍教授、赵维勤教授等许多朋友都给予了热情的支持和帮助。孙教授并为本书作了序言,简要介绍了书的内容,孙立军先生还专门编程计算了一些问题的系数,借此之机向他们表示作者的衷心感谢。也深深感谢国家知识产权出版社的李林先生、董建华先生和程兰女士的热情相助,本书才得以出版。

作者

1999年8月18日

符号表

$A, B, \dots$	大写字母表示逻辑数字串。
$a, b, \dots$	小写字母表示通常的代数数。
F	周期逻辑数字串。
t	周期逻辑数字串的周期。
D	单位周期逻辑数字串。
$\vee$	逻辑加。
$\wedge$	逻辑乘。
$\forall$	按位加。
$\overline{A}$	A 的求反。
A'	A 的逆转
g	$F = F_1 \wedge F_2$ 中的“1”的个数。
ω_i^j	F_i 中一周期内第 j 个“0”的位置。
$g(n, t_i, l_i), g(n, a, t)$	n 是 t 的整倍数时, g 的参数表示。
$g(n, t_i, l_i, \omega_i^j)$	n 不是 t 的整倍数时, g 的参数表示。
$g_{\max}(n, t_i, l_i)$	ω_i^j 各种变化后, $g(n, t_i, l_i, \omega_i^j)$ 的最大值。
$g_{\min}(n, t_i, l_i)$	ω_i^j 各种变化后, $g(n, t_i, l_i, \omega_i^j)$ 的最小值。
$\triangle(n, t_i, l_i)$	$g_{\max}(n, t_i, l_i)$ 与 $g_{\min}(n, t_i, l_i)$

$$t = \prod_{i=1}^m t_i$$

$$a = \prod_{i=1}^m (t_i - l_i)$$

$$\triangle_{up}(n, a, t)$$

$$g_{up}(n, a, t)$$

$$g_{low}(n, a, t)$$

$$F(m) = F_1 \wedge F_2 \wedge \cdots \wedge F_m$$

$$g_{\max}(n, t_i, l_i, m - r)$$

$$g_{\min}(n, t_i, l_i, m - r)$$

$$a(m - r)$$

$$t(m - r)$$

$$J$$

$$S_i$$

$$S$$

$$S \wedge S'$$

$$\stackrel{\leftarrow K}{S} \wedge S$$

$$S_{Ep}$$

之差。

各 F_i 周期 t_i 的积。

各 F_i 周期内“1”的个数的积, l_i 为 F_i 一周期内“0”的个数。

$\triangle(n, t_i, l_i)$ 的上界。

$g_{\max}(n, t_i, l_i)$ 的上界。

$g_{\min}(n, t_i, l_i)$ 的下界。

m 个 F_1 的逻辑乘。

$F(m-r)$ 的 n 位内“1”的个数的最大值。

$F(m-r)$ 的 n 位内“1”的个数的最小值。

为 $(t_1 - l_c)(t_2 - l_c) \cdots (t_{m-r} - l_c)$ 。

为 $t_1 t_2 \cdots t_{m-r}$ 。

奇数列。

奇素数 $(2i + 1)$ 的筛法的逻辑数字串。

奇素数的逻辑数字串。

“1 + 1”问题的逻辑数字串。

“1 - 1”问题的逻辑数字串。

素数 p 的方幂的逻辑数字串。