指数和的估计
及其在数论中的应用

华 罗 庚

科 学 出 版 社

內 容 簡 介

本书主要討論了指数和的各种估計方法及其应用，特别討論了这些方法对 Waring 問題及 Гольдбах 問題的应用．除此而外，也談到了解析数論的其他一些問題与方法．本书不仅綜合了这几方面的結果与文献，更重要的是对其中絕大部分重要的結果都給出了較完备的提綱性的証明．本书对于想了解这方面数学成果及从事这方面研究工作的数学工作者，将会有所帮助．

指数和的估計
及其在数論中的应用

华 罗 庚 著

*

科学出版社出版（北京朝阳門大街 117 号）

北京市书刊出版业营业許可証出字第 061 号

中国科学院印刷厂印刷　新华书店总經售

*

1963 年 8 月第一版	书号：2767
1963 年 8 月第一次印刷	字数：153,000
（京）精：1—2,700	开本：787×1092 1/18
平：1—2,900	印张：7 7/9　插頁：3

定价：精裝本 1.90 元
平裝本 1.20 元

序

2K611/22

“指数和的估計及其在数論中的应用”一书是应“德国数学百科全书”編委会之請而写，作为这套书的一个分册于 1959 年在德国以德文出版.

本书的目的在于系統地总結指数和方法. 近代解析数論、几何数論与堆垒数論所以有如此重大的发展，都是由于指数和方法的引入与改进. 尤其是著名的素数分布問題，Waring 問題，Гольдбах 問題，Tarry 問題以及圓內、球內整点問題等，更加如此.

作为百科全书的一部分，本书力求較全面地介紹这一分支的工作. 不仅如此，本书的写作方法，还不只是結果与文献的罗列，而是尽力注意到这一分支的系統性、关联性与完整性. 我試图把主要結果貫穿起来，并且尽可能地扼要地涉及到这些結果的証明. 希望有一定数学修养的讀者，可以直接看懂本书的主要部分，而不必另翻原作. 以上是作者平素对总結性与綜合性文章的撰写要求，虽然由于篇幅有限以及作者知識水平的局限，未能完全如愿，但作者还是尽力为之的.

本书由 1952 年开始撰写，至 1956 年完稿，自始至終是在中国科学院数学研究所党組織的支持与鼓励下进行工作的. 飲水思源，衷心感謝. 在写作过程中，很多同志帮我查閱了可能得到的文献，并且編制了附有摘要的文献卡片. 而本书就是在掌握这些材料之后，經整理、消化、取舍与綜合，而后写成的. 作者謹向这些同志致以謝意.

五年来，这一分支又有了进一步的发展. 王元、吳方两同志在翻譯本书的同时，又写了五个附录，把最近发展的結果补充了进去.

最后，作者衷心地希望讀者多提意見与批評.

华罗庚

1963 年 1 月

目　　录

导　　引

堆垒数論的历史是从两个著名的問题,即 Гольдбах 問题与 Waring 問题开始的.

Гольдбах 問题是在 1742[1] 年, Гольдбах 写信給 Euler 时提出的. 在信中, Гольдбах 提出了关于将整数表为素数和的两个猜想. 这两个猜想可用略为修改了的語言叙述为: (A)每一个 $\geqslant 6$ 的偶数都是两个奇素数之和; (B)每一个 $\geqslant 9$ 的奇数都可以表成三个奇素数之和. 显然,由命題(A)可以推出命題(B).

从 Гольдбах 写信起到今天,已經积累了不少宝貴的数值資料[2]. 这些資料指出了这两个猜想是正确的,但迄今还不能証明它們的眞伪.

大約在四十年前[3], 即使是証明如下的命題: 存在一个整数 c, 使每一个 $\geqslant 2$ 的整数都可表为不超过 c 个素数之和,也被認为是現代数学家力所不能及的事.

在 1770 年, Waring 提出了下面的猜想[4]:每一个自然数都是四个平方之和,九个立方之和,十九个四方之和,等等. 他的言論表明了他相信:对于每一个給定的整数 $k \geqslant 2$, 恆存在一仅依賴于 k 的整数 $s = s(k)$, 使每一正整数都可表为不超过 s 个非負整数的 k 次方之和.

Hilbert[5] 在 1909 年 (Waring 提出猜想后的 139 年) 首先証明了 $s(k)$ 的存在性. 以后, Шнирельман[6] 又在 1930 年 (Гольдбах 提出猜想后的 188 年) 証明了 c 的存在性. Hilbert 的方法虽然是很奇妙的,但它在堆垒素数論的近代发展中,并未显示出其功效. 但另一方面, Шнирельман 方法是广有用途的. 我們可以用这一方法同时处理这两个問题. 更須指出,在 Шнирельман 的論文中,他引入了关于自然数集合的非常重要的概念——"正密率".

Hardy 与 Littlewood 在这一世紀的二十年代,作出了极为重要的貢献. 用他們強有力的方法,不仅能够得到关于存在性的結果,而且可以得到明确的上界. 在总标題为"'partitio numerorum' 的若干問题"[7]的一系列論文中,他們系統地开創与发展了堆垒数論中的一个嶄新的解析方法. 这个方法就是人所共知的 Hardy 与 Littlewood 的圓法[8]. 命 $G(k)$ 表示最小的整数 s,使每一充分大的整数都能表成 s 个非負整数的 k 次方之和. 圓法可以得出 $G(k)$ 的一个明确的上界. 同时他們在广义 Riemann 猜想之下,証明了每一充分大的奇数都可以表为三个素数之和. Landau[9] 把这些結果都很好地整理在他的专著之中了.

为了取消在証明 Гольдбах 問題时所用到的未經証明的猜想，并改进 Waring 問題中的上界 $G(k)$，我們需要估計某种类型的指数和（Виноградов 称它們为三角和）．因此，获得指数和的精确估計就成了近代堆垒数論的解析方法发展中的最主要环节了．在近三十年来，Виноградов 創造了一系列估計指数和的天才方法．因此，他对 Hardy-Littlewood 方法作了巨大的改进．

对于 Гольдбах 問題，Виноградов 成功地对某种以素数为变数的指数和給出了非无聊的估計，他証明[10]了命題(B)对于充分大的奇数是正确的．Бороздкий[11] 經过計算証明了，每一奇数 $n \geqslant e^{e^{16.038}}$ 都能表成三个奇素数之和．

后来，Линник[12] 沿用 Hardy-Littlewood 原来的方法，并借助于 Dirichlet L-函数的零点的知識，亦証明了同样的結果．

另外一个研究 Гольдбах 問題的方法就是"篩法"．这一方法是 Erathostenes[13] 首創的．Brun[14] 与 Selberg[15] 分别对这一方法作出了重要的改进．由这一方法所得到的最好的、已經发表的結果是[16]：每一充分大的偶数都是两个素因子个数各不超过 3 的整数之和．但是无論如何，Selberg[17] 曾經宣布过，用他的方法可能証明每一充分大的偶数都可表为一个不超过 2 个素数的乘积及一个不多于 3 个素数的乘积之和．此外，应用 Линник[18] 的大篩法，Renyi[19] 証明了：每一充分大的偶数都是一个素数及一个素因子个数不超过某一給定常数的整数之和．

我們称在 Waring 問題的研究中所遇到的指数和为 Weyl 和．Weyl[20] 在关于一致分布的开創性工作中，最先使用了这种和．因此，他也是首先給出这种和以非无聊估值的人．他的估計成了 Hardy-Littlewood 关于 Waring 問題的研究方法中的一个最主要环节．Виноградов 与 van der Corput 作出了关于估計这种和的重要貢献．

Виноградов[21] 在 1935 年发表了一系列关于 Weyl 和的論文，他不断地改进着自己的結果．他的方法的最后形式被收集在他的选集[22]之中．在华罗庚[23]的专著中也有着 Виноградов 方法的略为改进了的形式．Виноградов 方法的价値不仅在于它能成功地用于 Waring 問題，而且它还有效地应用于素数分布論，Riemann ζ-函数論及 Dirichlet L-函数論，一致分布及 Diophantine 逼近論，高維橢球中的格子点估計及 Prouhet 問題等等．例如，用 Виноградов 的結果可以証明，不超过 x 的素数个数等于

$$\operatorname{li} x + O(xe^{-c(\log x)^{3/5}})\text{[24]}.$$

我們称下面的問題为 Prouhet 問題[25]（有时也称为 Tarry 問題或 Tarry-Escott 問題），即寻求最小的整数 s，使不定方程組

$$x_1^h + \cdots + x_s^h = y_1^h + \cdots + y_s^h, \quad 1 \leqslant h \leqslant k$$

有非无聊解，也就是說，$x_1, \cdots, x_s$ 不是 $y_1, \cdots, y_s$ 的重新排列．华罗庚[26]指出：估

計 Prouhet 問題的解数是 Виноградов 方法的主要环节；另一方面，这一方法也能用于 Prouhet 問題.

改进 $G(k)$ 上界的另一重要环节是寻求方程

$$x_1^k + \cdots + x_l^k = y_1^k + \cdots + y_l^k$$

的解数的上界,此处 x 与 y 都是适合某些条件的整数.

Виноградов[27] 証明了 $G(k) \leqslant 3k \log k + 11k$，而 Davenport[28] 則对較小的 k 作出了重要的貢献. $k = 3$ 时，較好的估計 $G(3) \leqslant 7$ 則是属于 Линник[29] 的. 运用 Виноградов 強有力的方法，Dickson[30]，Pillai[31] 与 Niven[32] 証明了：当 $k \neq 4$ 与 5，$k > 3$ 及 $\left(\frac{3}{2}\right)^k - \left[\left(\frac{3}{2}\right)^k\right] \leqslant 1 - \left(\frac{1}{2}\right)^k \left\{\left(\frac{3}{2}\right)^k + 3\right\}$ 时,每一整数都能表成 $g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$ 个非負整数的 k 次方之和. Siegel[33] 則将 Hardy-Littlewood 的圓法推广到代数数域上去.

Van der Corput[34] 給出了估計 Weyl 和的另一方法. 这一方法对圓內整点問題、除数問題与几何数論的其他問題,以及 Riemann ζ-函数論中的 Lindelöf 猜想,都有着重要的应用. 以后,他本人，Titchmarsh 与 Виноградов 又推广与改进了这个方法.

关于 L-函数及模函数論，請讀者参看百科全书中另一些专著"特殊的 Dirichlet 級数及其应用"与"解析数論中的模函数論". 同样,本书亦不包括超越数論及 Diophantine 逼近論. 关于这些主題,可以参看熟知的 Siegel，Гельфонд 与 Koksma 的书 (見后面的参考书籍).

Erdős 教授，Линник 教授与 Turán 教授都对本书提供了宝貴的意見，作者仅向他們致以衷心地感謝. 在准备这本书的手稿时,又得到了越民义先生与王元先生的帮助,作者也借此机会向他們致以謝意.

第一章　初等方法

1. 密　率

命 $\mathfrak{A}$ 表一由一些互不相同的非負整数 a 所成的集合. 命 $A(n)$ 表 $\mathfrak{A}$ 中不大于 n 之正整数的个数,即 $A(n)=\sum\limits_{1\leqslant a\leqslant n}1$, 在此需要注意 0 并不計算在內. 若 $\alpha>0$ 为使 $A(n)\geqslant\alpha n$ 对于一切 $n\geqslant 1$ 都成立的最大正数,则称 $\mathfrak{A}$ 具有正密率 α. 显然 $\alpha\leqslant$ $\leqslant 1$. 若 $\alpha=1$,则 $\mathfrak{A}$ 包有全体自然数. 引入記号 $\mathfrak{B}$, b, $B(n)$, β 及 $\mathfrak{C}$, c, $C(n)$, γ, 其間之关系一如 $\mathfrak{A}$, a, $A(n)$, α.

所有形如 $a+b$ $(a\in\mathfrak{A},\ b\in\mathfrak{B})$ 的整数所成之集合 $\mathfrak{C}$, 称为 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的"和集", 記为 $\mathfrak{C}=\mathfrak{A}+\mathfrak{B}$. 关于 $\mathfrak{A}$ 与 $\mathfrak{B}$ 的和集 $\mathfrak{C}$, Шнирельман[6] 很簡单地証明了下面两个重要定理:

(A) 若 $0\in\mathfrak{A}$,则 $\gamma\geqslant\alpha+\beta-\alpha\beta$;

(B) 若 $0\in\mathfrak{A}$ 及 $\alpha+\beta\geqslant 1$,则 $\gamma=1$, 即集合 $\mathfrak{C}$ 包有全体自然数.

命 $2\mathfrak{A}=\mathfrak{C}=\mathfrak{A}+\mathfrak{A}$, 并用归納法定义 $s\mathfrak{A}=\mathfrak{A}+(s-1)\mathfrak{A}$, 則由(A)可知, $s\mathfrak{A}$ 的密率 $\geqslant 1-(1-\alpha)^s$. 命 $s_0=\left[\dfrac{\log 2}{\log\dfrac{1}{1-\alpha}}\right]+1$, 則 $s_0\mathfrak{A}$ 的密率 $\geqslant\dfrac{1}{2}$. 又由(B)可知,集合 $2s_0\mathfrak{A}$ 包有全体自然数,故得:

(C) 若 $\mathfrak{A}$ 包有 0,則每一正整数都可表成 $\mathfrak{A}$ 中 $2s_0$ 个元素之和.

Шнирельман 給出了集合具有正密率的判別法:

(D) 命 $\mathfrak{A}^*$ 表一非負整数之集合,其中的元素允許重复, 命 $\mathfrak{A}$ 为 $\mathfrak{A}^*$ 中不同元素所成之最大集合. 命 $r(a)$ 表示 a 在 $\mathfrak{A}^*$ 中出現之次数. 若有 $\alpha'>0$,使对諸 $n\geqslant 1$ 都有

$$\frac{1}{n}\Big(\sum_{1\leqslant a\leqslant n}r(a)\Big)^2\geqslant\alpha'\Big(\sum_{1\leqslant a\leqslant n}r^2(a)\Big),$$

則 $\mathfrak{A}$ 有正密率 $\alpha\geqslant\alpha'$.

事实上,由 Буняковский-Schwarz 不等式可知

$$\Big(\sum_{1\leqslant a\leqslant n}r(a)\Big)^2\leqslant\sum_{1\leqslant a\leqslant n}r^2(a)\sum_{1\leqslant a\leqslant n}1=A(n)\sum_{1\leqslant a\leqslant n}r^2(a).$$

以上就是 Шнирельман 关于正整数集合的貢献的主要部分.

命 $\mathfrak{A}_1, \mathfrak{A}_2, \cdots, \mathfrak{A}_s$ 为密率都是 α 的 s 个集合. Хинчин[35] 証明了:集合 $\mathfrak{A}_1+\mathfrak{A}_2+ +\cdots+\mathfrak{A}_s$ 的密率 $\geqslant \min(1, s\alpha)$.

Mann[35] 在 1942 年証明了重要的猜想: $\gamma \geqslant \min(1, \alpha+\beta)$. 以后, Artin 与 Scherk[37] 又簡化了 Mann 的証明. 請讀者参考 Ostmann[38] 的书,在那里詳細地闡述了密率的理論及其应用.

2. Hilbert-Waring 定理

在講 Линник[39] 关于 Hilbert-Waring 定理的初等証明之前(在此稍有簡化与改进[40]),先証明下面两个引理.

引 1. 命 $X, Y \geqslant 0$. 又命 $q(n)$ 为不定方程

$$x_1y_1+x_2y_2=n, \quad |x_m| \leqslant X, |y_m| \leqslant Y, \quad m=1,2, \tag{1}$$

的整数解数,则

$$q(n) \ll \begin{cases} (XY)^{\frac{3}{2}}, & \text{若 } n=0; \\ (XY)\sum\limits_{d|n}\dfrac{1}{d}, & \text{若 } n \neq 0. \end{cases} \tag{2}$$

当 $n=0$ 时, 引理显然成立. 当 $n \neq 0$ 时, 只要証明在条件 $(x_1, x_2)=1$ 及 $|x_2| \leqslant |x_1| \leqslant X$ 下,(1)的解数 $q'(n) \ll XY$ 即可. 不失一般性,可以假定 $X \leqslant Y$. 命 y_1', y_2' 是(1)的一組解答, 則其他解 y_1, y_2 可以表成 $y_1=y_1'+tx_2$, $y_2=y_2'-tx_1$. 因此 $|t|=\dfrac{|y_2'-y_2|}{|x_1|} \leqslant \dfrac{2Y}{|x_1|}$. 所以

$$q'(n) \leqslant \sum_{1\leqslant|x_1|\leqslant X}\ \sum_{|x_2|\leqslant|x_1|}\frac{5Y}{|x_1|} \ll XY.$$

由引理立刻推出

$$\sum_{|a|\leqslant 2XY} q^2(a) \ll (XY)^3. \tag{3}$$

引 2. 命 $k \geqslant 2$ 及

$$f(x)=a_kx^k+a_{k-1}x^{k-1}+\cdots+a_1x, \quad a_k \ll 1, \quad a_{k-1} \ll P, \quad \cdots, \quad a_1 \ll P^{k-1}$$

为一整系数多項式,則

$$\int_0^1\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha \ll P^{8^{k-1}-k}, \tag{4}$$

此处与記号 $\ll$ 有关的常数仅依赖于 k.

仅仅是为了方便,我們才在这里使用了积分. 我們可以毫无困难地把全部証明

都用初等数論的語言写出来.

当 $k=2$ 时,(4)之左端乃方程

$$f(x_1)+f(x_2)-f(y_1)-f(y_2)=f(x_3)+f(x_4)-f(y_3)-f(y_4),$$
$$x_m \ll P; \quad y_m \ll P; \quad m=1,2,3,4$$

的整数解数. 显然它不超过方程

$$z_1w_1+z_2w_2=z_3w_3+z_4w_4, \quad z_m \ll P; \quad w_m \ll P, \quad m=1,2,3,4$$

的整数解数. 因此,由(3)可知,引理当 $k=2$ 时是正确的. 現在用归納法来証明引理. 由于

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^2=\sum_{x=0}^{P} e^{-2\pi i f(x)\alpha}\sum_{-x\leqslant h\leqslant P-x} e^{2\pi i f(x+h)\alpha}=$$
$$=\sum_{|h|\leqslant P}{}' \sum_{x=1}^{P}{}' e^{2\pi i h\varphi(x,h)\alpha},$$

此处 $\sum'$ 表示經过所示区間內整数的某一部分集合,而

$$\varphi(x,h)=\begin{cases}\dfrac{1}{h}(f(x+h)-f(x)), & 若\ h\neq 0;\\ 0, & 若\ h=0,\end{cases}$$

故由 Hölder 不等式可知

$$\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{2\cdot 8^{k-2}} \ll P^{8^{k-2}-1}\sum_{|h|\leqslant P}{}'\left|\sum_{x=1}^{P}{}' e^{2\pi i h\varphi(x,h)\alpha}\right|^{8^{k-2}}=$$
$$=P^{8^{k-2}-1}\sum_{|h|\leqslant P}{}'\sum_{n} r(n)e^{2\pi i h n\alpha}, \tag{5}$$

此处

$$r(n)=\int_0^1\left|\sum_{x=0}^{P}{}' e^{2\pi i\varphi(x,h)\beta}\right|^{8^{k-2}} e^{-2\pi i n\beta}d\beta. \tag{6}$$

由归納法假定可知 $r(n)\ll P^{8^{k-2}-(k-1)}$. 所以由(3),再将(5)式四方,并从 0 至 1 求积分,便得

$$\int_0^1\left|\sum_{x=0}^{P} e^{2\pi i f(x)\alpha}\right|^{8^{k-1}} d\alpha \ll$$
$$\ll P^{4(8^{k-2}-1)}\int_0^1\left|\sum_{|h|\leqslant P}{}'\sum_{n} r(n)e^{2\pi i h n\alpha}\right|^4 d\alpha \ll$$
$$\ll P^{4(8^{k-2}-1)}\sum_{hn+h'n'=h''n''+h'''n'''} r(n)r(n')r(n'')r(n''') \ll$$
$$\ll P^{4(8^{k-2}-1)+4(8^{k-2}-(k-1))+3(k-1+1)}=$$
$$=P^{8^{k-1}-k}.$$

取 $\mathfrak{A}_t^*$ 为整数

$$x_1^k + \cdots + x_t^k$$

所成之集合，此处 x_m 各自經过全体非負整数．定义 $\mathfrak{A}_t$ 为 $\mathfrak{A}_t^*$ 中的不同元素所成之最大子集．命 $c_1 = \frac{1}{2} 8^{k-1}$ 及 $r(a)$ 为不定方程

$$x_1^k + \cdots + x_{c_1}^k = a, \quad x_m \geqslant 0$$

的解数，則显然

$$\sum_{1 \leqslant a \leqslant n} r(a) \gg \left(\frac{n}{c_1}\right)^{\frac{c_1}{k}} \gg n^{\frac{c_1}{k}}.$$

又由(4)可知

$$\sum_{1 \leqslant a \leqslant n} r^2(a) \ll n^{\frac{2c_1}{k}-1},$$

故由定理(D)可知，当 $k \geqslant 2$ 时，集合 $\mathfrak{A}_{c_1}$ 有正密率．因此我們証明了

Hilbert-Waring 定理． 对于任意整数 $k \geqslant 2$，恆存在一仅依賴于 k 的整数 $s = s(k)$，使每一正整数都是不超过 s 个正整数的 k 次方之和．

3. 篩法及 Шнирельман-Гольдбах定理

Möbius 函数 $\mu(n)$ 是正整数 n 的函数，其定义如下：$\mu(1) = 1$；若 n 能被一素数的平方所整除，則 $\mu(n) = 0$；又若 n 为 r 个不同素数之乘积，則 $\mu(n) = (-1)^r$．

古典的 Eratosthenes 篩法可以用下面的方式陈述出来：命 P 为 $\leqslant \xi$ 的全体素数的乘积，則

$$\sum_{d|(P,n)} \mu(d) = \begin{cases} 1, & \text{若 } n \text{ 无} \leqslant \xi \text{ 的素因子；} \\ 0, & \text{其他情形．} \end{cases} \tag{7}$$

命 $\mathfrak{B}$ 为由 M 个相同或相异的整数 b 所成之集合，N_ξ 为 $\mathfrak{B}$中不能被 $\leqslant \xi$ 的素数整除的元素 b 的个数，則得

$$N_\xi = \sum_b \Big(\sum_{d|(P,b)} \mu(d) \Big). \tag{8}$$

交换(8)中的求和次序，便得

$$N_\xi = \sum_{d|P} \mu(d) \sum_{d|b} 1 = \sum_{P|P} \mu(d) N(d), \tag{9}$$

此处 $N_d = \sum_{d|b} 1$ 为 $\mathfrak{B}$ 中能被 d 整除的元素 b 的个数．

用 Eratosthenes 原来的形式，可以将(9)式叙述为：先减掉集合 $\mathfrak{B}$ 中为 2, 3, 5, ···(素数貫)倍数的元素的个数．假如一个数为两个素数的乘积所整除，因为它被

計算了两次,所以需要添上 $\mathfrak{B}$ 中为 $2\cdot 3,\ 2\cdot 5,\ 3\cdot 5,\ \cdots$(两个素数乘积的貫)的倍数的元素的个数. 又因为被三个素数的乘积整除的元素,共計算了 $\binom{3}{1}-\binom{3}{2}=0$ 次,所以又需减掉 $\mathfrak{B}$ 中为 $2\cdot 3\cdot 5,\ \cdots$(三个素数乘积的貫)整除的元素的个数. 如此等等.

若 $N(d)$ 有漸近表达式

$$N(d)=g(d)\frac{N}{d}+R_d, \tag{10}$$

此处 $g(d)$ 为无平方因子数的积性函数. 則由(9)得

$$\begin{aligned} N_\xi &= \sum_{d\mid P}\frac{\mu(d)}{d}g(d)N+O\Big(\sum_{d\mid P}|R_d|\Big)= \\ &= N\prod_{p\mid P}\Big(1-\frac{g(p)}{p}\Big)+O\Big(\sum_{d\mid P}|R_d|\Big). \end{aligned} \tag{11}$$

除了一些很显然的情况外,(11)的余項常常比主項更大,因此(11)几乎是无用的.

Brun[14] 对篩法作了重大的改进. 命

$$2=p_1<p_2<\cdots<p_{k_0}\leqslant\xi$$

为 $\leqslant\xi$ 的全体素数,又

$$k_0\geqslant k_1\geqslant\cdots\geqslant k_{t-1}\geqslant 1$$

为一整数集合. 命 Q 为具有如下形式的整数的集合:

$$d=1;\quad d=p_{r_1}p_{r_2}\cdots p_{r_s},\quad s\leqslant 2t, \tag{12}$$

其中 $r_1>r_2>\cdots>r_s,\ r_j\leqslant k_{\left[\frac{j-1}{2}\right]},\ 1\leqslant j\leqslant s$. 則得

$$\sum_{\substack{d\mid n\\ d\in Q}}\mu(d)\begin{cases}=1, & \text{若 } n \text{ 无} \leqslant\xi \text{ 的素因子;}\\ \geqslant 0, & \text{其他情形.}\end{cases} \tag{13}$$

事实上,若 n 无 $\leqslant\xi$ 的素因子,則(13)式显然成立. 若 n 有 $\leqslant\xi$ 的素因子,則以 p_0 表示 n 的最小素因子. 当 $d\in Q,\ d\mid n$ 及 d 的素因子个数为奇数时,我們就定义 d_1 如下:若 $p_0\mid d$,則 $d_1=\dfrac{d}{p_0}$; 若 $p_0\nmid d$,則 $d_1=dp_0$. 因此 $d_1\mid n,\ d_1\in Q$ 且 d_1 的素因子个数为偶数. 由于每一个 d 都唯一地对应到一个 d_1,故得(13).

由(13)可知

$$\begin{aligned} N_\xi &\leqslant \sum_b\sum_{\substack{d\in Q\\ d\mid(b,P)}}\mu(d)=\sum_{d\in Q}\mu(d)\sum_{d\mid b}1= \\ &= N\sum_{d\in Q}\mu(d)\frac{g(d)}{d}+O\Big(\sum_{d\in Q}|R_d|\Big). \end{aligned} \tag{14}$$

对于各种間題,我們选取适当的 $k_0, \cdots, k_{t-1}$,就能得到 N_ξ 的上界.

其次,我們用另一集合 Q' 来代替集合 Q. 命 $k_0 \geqslant k_1 \geqslant \cdots \geqslant k_t \geqslant 1$, Q' 为适合下面条件的整数集合:

$$d' = 1, \quad d' = p_{r_1} p_{r_2} \cdots p_{r_s}, \quad s \leqslant 2t + 1,$$

其中 $r_1 > r_2 > \cdots > r_s$ 及 $r_j \leqslant k_{[\frac{1}{2}j]}$. 对应于(13),有

$$\sum_{\substack{d' | n \\ d' \in Q'}} \mu(d') \begin{cases} = 1, & \text{若 } n \text{ 无} \leqslant \xi \text{ 的素因子;} \\ \leqslant 0, & \text{其他情形.} \end{cases}$$

类似地,我們得到 N_ξ 的下界如下:

$$N_\xi \geqslant N \sum_{d' \in Q'} \frac{\mu(d') g(d')}{d'} + O\left(\sum_{d' \in Q'} |R_{d'}| \right). \tag{15}$$

取 $\mathfrak{B}$ 为整数

$$x(a-x), \quad 1 \leqslant x \leqslant a$$

的集合. 再适当地选取(14)中的 $k_i (1 \leqslant i \leqslant t-1)$. Шнирельман 証明了下面的結果:命 $r(a)$ 为方程 $a = p_1 + p_2$ 的解数,此处 p_1, p_2 为素数,则

$$r(a) \ll \frac{a}{\log^2 a} \sum_{k|a} \frac{\mu^2(k)}{k}. \tag{16}$$

与 §1 相同的記号. 取 $\mathfrak{A}^*$ 为由整数 1 及諸整数 $a = p_1 + p_2 (1 < p_1, p_2 \leqslant a)$ 所成的集合,则显然有

$$\sum_{1 \leqslant a \leqslant n} r(a) = 1 + \sum_{p_1 + p_2 \leqslant n} 1 \geqslant \left(\sum_{p_1 \leqslant \frac{n}{2}} 1 \right)^2 \gg \left(\frac{n}{\log n} \right)^2.$$

又因 d 与 d' 的最小公倍数 $\{d_1, d_2\} \geqslant (dd')^{\frac{1}{2}}$,故由(16)得到

$$\begin{aligned} \sum_{1 \leqslant a \leqslant n} r^2(a) &\ll \sum_{4 \leqslant a \leqslant n} \frac{a^2}{\log^4 a} \sum_{d | a} \frac{1}{d} \sum_{d' | a} \frac{1}{d'} \ll \\ &\ll \frac{n^2}{\log^4 n} \sum_{d, d' \leqslant n} \frac{1}{dd'} \sum_{\substack{1 \leqslant a \leqslant n \\ d|a, \ d'|a}} 1 \ll \\ &\ll \frac{n^3}{\log^4 n} \left(\sum_{1 \leqslant d \leqslant n} \frac{1}{d^{3/2}} \right)^2 \ll \frac{n^3}{\log^4 n}. \end{aligned}$$

于是由 §1, 定理(D)可知, 由 1 及可以表为两个素数之和的諸整数所成的集合具有正密率. 因此由定理(C),我們得到下面的享有盛名的定理.

Шнирельман-Гольдбах 定理. 存在整数 c, 使每一整数都是不超过 c 个素数之和.

命 s 表示最小的整数, 使每一充分大的整数都能表成不多于 s 个素数之和.

Шнирельман的方法不仅証明了 s 的存在性，而且可以得到 s 的明确上界。他的方法給出 $s \leqslant 800{,}000$。Романов[41] 又在以后証明了 $s \leqslant 2208$。沿着这一方向，还有如下更进一步的改进：Heilbronn，Landau 与 Scherk[42] 得到 $s \leqslant 71$，而估計 $s \leqslant 67$ 則是屬于 Ricci[43] 的。

在(15)中选取适当的 $k_0, k_1, \cdots$，Brun 首先証明了；每一充分大的偶数都是两个各不超过 9 个素数的乘积之和。Rademacher[44] 将 9 改进为 7，而 Estermann[45] 又将 7 減至 6。

Бухштаб[46] 成功地以 4 代替了 6，他改进这一結果的主要想法如下：命

$$3 = p_1 < p_2 < \cdots < p_k$$

为不超过 y 的全体素数。又命

$$(w) \qquad a;\ a_1,\ b_1;\ a_2,\ b_2;\ \cdots;\ a_k,\ b_k$$

为适合下面条件的整数集合：

$$a = 0 \text{ 或 } 1,\ a_i \neq b_i,\ 0 \leqslant a_i,\ b_i < p_i,\ 1 \leqslant i \leqslant k;$$

而命 $F_w(x, y)$ 为适合下面条件的整数 n 的个数：

$$1 \leqslant n \leqslant x;\ n \equiv a (\operatorname{mod} 2),\ n \not\equiv a_i (\operatorname{mod} p_i),\ n \not\equiv b_i (\operatorname{mod} p_i),$$
$$(1 \leqslant i \leqslant k)$$

則得

$$F_w(x; p_s) = F_w(x; p_{s-1}) - F_{w'_s}\left(\frac{x}{p_s};\ p_{s-1}\right) - F_{w''_s}\left(\frac{x}{p_s};\ p_{s-1}\right) + 2\theta,$$
$$0 \leqslant |\theta| \leqslant 1. \qquad (17)$$

命 $v > u \geqslant 2$。将 $x^{\frac{1}{v}}$ 与 $x^{\frac{1}{u}}$ 之間的素数依次排列为 $p_t \leqslant x^{\frac{1}{v}} < p_{t+1} < \cdots < p_k \leqslant$ $\leqslant x^{\frac{1}{u}} < p_{k+1}$，則連續运用(17)便得

$$F_w(x; x^{\frac{1}{u}}) = F_w(x; x^{\frac{1}{v}}) - \sum_{i=t+1}^{k} F_{w'_i}\left(\frac{x}{p_i};\ p_{i-1}\right) -$$
$$- \sum_{i=t+1}^{k} F_{w''_i}\left(\frac{x}{p_i};\ p_{i-1}\right) + 2k\theta. \qquad (18)$$

Бухштаб 用 Brun 方法証明了：存在两个非負的阶梯函数 $\lambda(u)$ 及 $\Lambda(u)$，使当 x 充分大时，下式对于 w 一致地成立：

$$\lambda(u)\frac{cx}{\log^2 x} \leqslant F_w(x;\ x^{\frac{1}{u}}) \leqslant \Lambda(u)\frac{cx}{\log^2 x}, \quad 15 \geqslant u \geqslant 2. \qquad (19)$$

由(18)，我們可以构造两个阶梯函数

$$\lambda_1(u) \leqslant \lambda(v) - 2\int_{u-1}^{v-1} \Lambda(z)\frac{z+1}{z^2}dz$$

及

$$\Lambda_1(u) \geqslant \Lambda(v) - 2\int_{u-1}^{v-1} \lambda(z)\frac{z+1}{z^2}dz.$$

它們分别具有与 $\lambda(u)$ 及 $\Lambda(u)$ 相同的性質. 进而言之,我們有

$$\lambda(u) \leqslant \lambda_1(u) \leqslant g(u) \leqslant \Lambda_1(u) \leqslant \Lambda(u).$$

不断运用这个原則,并經过一些复杂的計算,就能得到 Бухштаб 的結果.

4. 續

Selberg[15) 17) 47)] 对篩法作出了另一重要的改进.

命 $\lambda_1, \lambda_2, \cdots$ 为一实数貫,它滿足 $\lambda_1 = 1$, 且当 $d > \sqrt{z}$ 时, $\lambda_d = 0$. 則显然有

$$\left(\sum_{d|(n,P)} \lambda_d\right)^2 \begin{cases} = 1, & \text{若 } n \text{ 无} \leqslant \xi \text{ 的素因子;} \\ \geqslant 0, & \text{其他情形,} \end{cases}$$

此处 $P = \prod_{p \leqslant \xi} p$. 因此

$$\begin{aligned} N_\xi &= \sum_b \left(\sum_{d|(b,P)} \mu(d)\right) \leqslant \sum_b \left(\sum_{d|(b,P)} \lambda_d\right)^2 = \\ &= \sum_{\substack{d\leqslant\sqrt{z} \\ d|P}} \sum_{\substack{d'\leqslant\sqrt{z} \\ d'|P}} \lambda_d\lambda_{d'} \sum_{\substack{b \\ \{d,d'\}|b}} 1 = \\ &= N \sum_{\substack{d\leqslant\sqrt{z} \\ d|P}} \sum_{\substack{d'\leqslant\sqrt{z} \\ d'|P}} \lambda_d\lambda_{d'} \frac{g(\{d,d'\})}{\{d,d'\}} + \sum_{\substack{d\leqslant\sqrt{z} \\ d|P}} \sum_{\substack{d'\leqslant\sqrt{z} \\ d'|P}} \lambda_d\lambda_{d'} R_{\{d,d'\}}, \end{aligned}$$

此处 $\{d, d'\}$ 表示 d 与 d' 的最小公倍. Selberg 定出了使二次型

$$\sum_{\substack{d\leqslant\sqrt{z} \\ d|P}} \sum_{\substack{d'\leqslant\sqrt{z} \\ d'|P}} \lambda_d\lambda_{d'} \frac{g(\{d,d'\})}{\{d,d'\}}$$

取极小値的諸 λ,从而得到了 N_ξ 的上界.

为了估計 N_ξ 的下界,我們假定 $\lambda_1 = 1$. 若 $p \leqslant \xi$,則 $\lambda_p = 1$; 若 $d > \sqrt{\frac{z}{p}}$, 則 $\lambda_{d\cdot p} = 0$. 易知

$$1 - \sum_{p|(n,P)} \left\{\sum_{\substack{d|(n,P) \\ p'|d \Rightarrow p'<p}} \lambda_{d\cdot p}\right\}^2 \begin{cases} = 1, & \text{若 } n \text{ 无} \leqslant \xi \text{ 的素因子;} \\ \leqslant 0, & \text{其他情形.} \end{cases}$$

故得