数论的方法

（上　册）

闵嗣鹤

科学出版社

数论的方法

（上册）

闵嗣鹤

科学出版社

1983

内 容 简 介

本册分两篇．第一篇介绍数论中几种重要的初等方法．包括 Шнирельман 的密率论及由此发展而成的渐近密率与本性分量的理论，Brun 的筛法与更精密的 Selberg 筛法，素数定理的初等证明与弱型 Goldbach 问题的初等解法等．第二篇介绍解析数论的一些基本理论与方法．包括关于黎曼 ζ 函数与狄氏 L 函数的一些基本理论及应用这些理论来研究自然数串中或一般算术级数中的素数分布的方法等等．

本书这次重印时，由戚鸣皋同志对原书进行了校正．

数 论 的 方 法

（上 册）

闵 嗣 鹤

责任编辑 张鸿林 杜小杨

科学出版社出版

北京朝阳门内大街 137 号

中国科学院印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

*

1958 年 7 月第 一 版 开本：850×1168 1/32

1983 年 8 月第四次印刷 印张：5 7/8

印数：8,571—15,870 字数：153,000

统一书号：13031·1560

本社书号：2140·13—1

定价：1.10 元

序

在 1955—1957 年我曾两度于北大数学力学系讲授数论专门化的课程，这本书的内容就是根据当时的讲义加以补充整理而写成的. 本来讲义包含三部分，即初等的方法、解析的方法与三角和的方法三篇. 由于第三部分还需要更彻底的改写与补充，一时还没能够整理到比较令人满意的地步，所以先把前两部分整理出来，合写成这一本书.

这本书的目的与作用和原来的讲义是一样的，那就是使得仅仅具有数论初步知识的读者（例如读过裘光明所译 Виноградов 的《数论基础》）借着本书逐渐提高水平，使在不长的时间内能够阅读近代数论在若干方面的文献，以至独立地或在适当辅导下进行科学研究. 因此，本书的性质仍然是一种阶梯或导引，并不能也不想对数论的各个分支都作深入与全面的讨论. 至于材料的选择当然一方面不免受到个人研究范围的影响，另一方面也考虑到不要与已有写的很好的书有不必要的重复.

在写这本书时，参考了不少的数论名著（华罗庚先生著的《数论导引》附有很好的一个参考书目）. 通过了实际教学，已经把不少的材料融化成为自己的形式. 但由于时间关系，即在本书中，仍有不少的材料未能如意予以改写. 在我讲课与改写的时候，两届数论专门化的学生曾给我很大的帮助. 其中尹文霖同志参加编写 Шнирельман 的密率论及渐近密率与本性分量二章，这里面也包括他的毕业论文中的一个结果. 潘承洞同志参加编写 Selberg 的筛法及算术级数中的素数分布二章，他在讨论班上的报告也供给我以写稿的便利. 他们在写稿时都曾参考科学院数学研究所的一份讲义，特在此致谢. 此外，还有不少同志对于旧讲义或作过文辞

的润色或给以式子的更正或改正印刷的错误. 这一切都给我很大的便利，衷心在此致谢.

闵嗣鹤

1957 年 10 月

符 号 说 明

本书中除用到一般初等数论所常用的符号以外，还时常用到集论中的符号．如 $a \in A$ 表 a 属于 A，$a \notin A$ 表 a 不属于 A，$A \subset B$ 表 A 是 B 的部分集合（可以是 B 本身），$A \cup B$ 表 A 与 B 的联合，$A \cap B$ 表 A 与 B 的交界等．其他比较特殊的符号，都在用到时，给以定义．

目　　录

第一篇　初等的方法

第二篇　解析的方法

第一篇　初等的方法

第　一　章

Шнирельман 的密率论

§1. 堆垒数论的问题

Waring 问题与 Goldbach 问题是堆垒数论中有代表性的两个著名问题，Waring 问题所要讨论的是：是不是能找到一个只与 n 有关的常数 C_n，使当 $k > C_n$ 时，每一个正整数都可以表成 k 个非负整数的 n 次方幂之和. Goldbach 问题所要讨论的是：(1) 是不是每一个大于 4 的偶数都能表成两个奇素数之和，(2) 是不是每一个大于 7 的奇数都能表成三个奇素数之和. 由于 Goldbach 问题的解决是非常难的，我们退一步讨论一个比较容易的问题(弱型 Goldbach 问题)：是不是每一个自然数都可以表成不超过一定个数的素数之和. Waring 问题和弱型 Goldbach 问题都包含在下列更带一般性的问题之中.

设有 k 个递增的整数序列所组成的集合：

$$\begin{aligned}
&(A^{(1)}) \quad 0 = a_0^{(1)}, a_1^{(1)}, \cdots, a_n^{(1)}, \cdots \\
&(A^{(2)}) \quad 0 = a_0^{(2)}, a_1^{(2)}, \cdots, a_n^{(2)}, \cdots \\
&\qquad\qquad \cdots\cdots\cdots\cdots\cdots\cdots \qquad (a_\nu^{(k)} < a_{\nu+1}^{(k)}) \qquad (1.1) \\
&(A^{(k)}) \quad 0 = a_0^{(k)}, a_1^{(k)}, \cdots, a_n^{(k)}, \cdots
\end{aligned}$$

我们要问是不是每一个非负整数 n 都可以表成下列形式：

$$n = a_{n_1}^{(1)} + a_{n_2}^{(2)} + \cdots + a_{n_k}^{(k)}. \qquad (1.2)$$

在这里，我们最好引进集合 $A^{(1)}, A^{(2)}, \cdots, A^{(k)}$ 的和的概念. 我们把所有能表成 (1.2) 的形式的非负整数所组成的集合称为 $A^{(1)}, \cdots, A^{(k)}$ 的 Шнирельман 和，或简称它们的和，记作

$$A = A^{(1)} + \cdots + A^{(k)} = \sum_{i=1}^{k} A^{(i)}. \tag{1.3}$$

有了以上的定义[1)]，我们的一般性问题就可以叙述为：是不是 k 个集合 (1.1) 的和 (1.3) 包含全体自然数. 在本书里面，以后所谓集合都指非负整数的集合.

§2. 密率的引进

为了研究上述一般性的问题，Л. Г. Шнирельман 首先引进了密率的概念. 考虑任何一个集合：

(A) $0 = a_0, a_1, a_2, \cdots, a_n, \cdots (a_n < a_{n+1}, a_n$ **是整数)**.

用 $A(n)$ 代表 A 中不超过 $n(n \geqslant 1)$ 的正整数的个数（注意 0 不计算在内），即

$$A(n) = \sum_{\substack{1 \leqslant \nu \leqslant n \\ \nu \in A}} 1,$$

则 $0 \leqslant A(n) \leqslant n$ 而

$$0 \leqslant \frac{A(n)}{n} \leqslant 1.$$

我们定义 $\frac{A(n)}{n}$ $(n = 1,2,\cdots)$ 的下确界为 A 的密率，记作 $d(A)$，即

$$d(A) = \inf_{n \geqslant 1} \frac{A(n)}{n}. \tag{2.1}$$

从这个定义立刻可以推出以下的一些简单结果：

1. 当 $a_1 > 1$ (即 A 不包含 1) 时，$d(A) = 0$，

2. 当 $a_n = 1 + r(n-1)$ [即 A 从 a_1 起是以 1 为首项，r 为公差的等差级数] 时，

$$d(A) = \frac{1}{r}.$$

---

1) 对于不包含 0 的整数集合，应该先把 0 加进去然后求和，所得的和仍称为原来各集合的 Шнирельман 和.

3. 每一个等比级数所成集合的密率是 0.

4. 所有完全平方所组成集合的密率是 0.

5. 若 $d(A)=0$，而 A 包含 1 则任给 $\varepsilon>0$ 一定可找到 $N\geqslant 1$ 使得

$$A(N)<\varepsilon N.$$

6. 集合 A 包含自然数全体的充要条件是 $d(A)=1$.

从以上最后一条性质看来，我们就知道上节最后所提出的问题，就是要问 k 个集合之和 A 的密率 $d(A)$ 是不是1. 因此，下面的定理有着重要的意义：

定理 2.1 (Шнирельман). 设 A，B 是两个集合，则

$$d(A+B)\geqslant d(A)+d(B)-d(A)d(B). \tag{2.2}$$

证 设 $A+B=C$ 而

$$A(n)=\sum_{\substack{1\leqslant\nu\leqslant n\\ \nu\in A}}1,\quad B(n)=\sum_{\substack{1\leqslant\nu\leqslant n\\ \nu\in B}}1,\quad C(n)=\sum_{\substack{1\leqslant\nu\leqslant n\\ \nu\in C}}1$$

及

$$d(A)=\alpha,\quad d(B)=\beta,\quad d(C)=\gamma.$$

在自然数的一段 $(1,n)$ 中含有 A 内的 $A(n)$ 个整数. 设用 a_k 及 a_{k+1} 表其中依次相邻的两个数，则在这两数之间有 $a_{k+1}-a_k-1=l$ 个数不属于 A，它们是

$$a_k+1,\ a_k+2,\ \cdots,\ a_k+l=a_{k+1}-1.$$

以上各数中间凡可以写成 a_k+b $(b\in B)$ 这种形式的数都是属于 C 的，它们的个数等于 B 在 $(1,l)$ 一段中所包含整数的个数，这当然就是 $B(l)$.

因此，在 A 的每相邻两数之间，如果所包含的一段自然数的长度(即个数)是 l，就至少有 $B(l)$ 个数属于 C. 因此在自然数的一段 $(1,n)$ 中，C 所包含整数的个数 $C(n)$ 至少是

$$A(n)+\sum B(l),$$

上式中$\sum$的各项通过 $(1,n)$ 中不含 A 内整数的一段一段的自然数. 但根据密率的定义，$B(l)\geqslant\beta l$，故

$$C(n)\geqslant A(n)+\beta\sum l=A(n)+\beta\{n-A(n)\}.$$

上面最后一个等式的成立是由于$\sum l$等于$(1, n)$中不落在A内的整数的个数，当然它等于$n - A(n)$. 又$A(n) \geqslant \alpha n$，故

$$C(n) \geqslant A(n)(1-\beta) + \beta n \geqslant \alpha n(1-\beta) + \beta n.$$

由此立刻得到

$$\frac{C(n)}{n} \geqslant \alpha + \beta - \alpha\beta.$$

上式对于所有正整数n都成立，故

$$\gamma = d(C) \geqslant \alpha + \beta - \alpha\beta. \qquad \text{[证完]}$$

上面的不等式又可以写成

$$1 - d(A+B) \leqslant \{1 - d(A)\}\{1 - d(B)\}.$$

用归纳法即可推广成

$$1 - d(A_1 + \cdots + A_k) \leqslant \prod_{i=1}^{k} \{1 - d(A_i)\}.$$

故得下面的

推论

$$d(A_1 + \cdots + A_k) \geqslant 1 - \prod_{i=1}^{k} \{1 - d(A_i)\}.$$

从 Шнирельман 的不等式，可以推出一系列值得称道的结果，其中居首要地位的是下面的定理 2.2. 在叙述这个定理之前，我们先引进一个定义并证明一个引理.

定义 如果一个集合A本身与本身相加至一定次数k时就包含自然数全体，则称A是自然数的一个基.

引理 2.1 若$A(n) + B(n) > n - 1$则$n \in A + B$.

证 若n在A或B中，引理显然成立. 今设n既不在A又不在B中，于是

$$A(n) = A(n-1), \quad B(n) = B(n-1),$$

而

$$A(n-1) + B(n-1) > n - 1.$$

设在$(1, n-1)$一段内，A与B所包含的数分别为

$$a_1, a_2, \cdots, a_r,$$

$$b_1, b_2, \cdots, b_s.$$

则 $r = A(n-1)$, $s = B(n-1)$ 而

$$a_1,\ a_2,\ \cdots,\ a_r$$
$$n - b_1,\ n - b_2,\ \cdots,\ n - b_s$$

都在 $(1, n-1)$ 一段中，它们的总个数是 $r + s = A(n-1) + B(n-1) > n - 1$ 所以其中至少有两个相等，设为 $a_i = n - b_k$，则 $n = a_i + b_k$ 故 n 在 $A + B$ 中.

从上面的引理很容易推出下面的

推理 若 $C = A + B$ 而 $d(A) + d(B) \geqslant 1$，则 $d(C) = 1$.

定理 2.2 (Шнирельман). 每一个密率是正的集合都是自然数的基.

证 设 $d(A) = \alpha > 0$ 而

$$A_k = A + A + \cdots + A \ (\text{共 } k \text{ 项}),$$

则由定理 2.1 的推论，

$$d(A_k) \geqslant 1 - (1-\alpha)^k.$$

显然当 k 充分大时

$$d(A_k) > \frac{1}{2},$$

故

$$A_k(n) > \frac{1}{2} n > \frac{1}{2}(n-1).$$

即

$$A_k(n) + A_k(n) > n - 1.$$

由引理 2.1，$n \in A_k + A_k = A_{2k}$. 但 n 是任意自然数，故定理成立.

从这个简单的定理出发 Шнирельман 得出了一系列有趣的定理. 例如，他证明了由 0，1 及一切素数组成的序列 P 是自然数的一个基(看第二章 § 7). 其实这个序列 P 的密率是 0，但他却证明了 $P + P$ 的密率是正的，因而推出了：存在一个充分大的 k 使得每一个大于 1 的自然数都可以表成不超过 k 个素数之和.

§3. Landau-Шнирельман 的假说及其证明

所谓 Landau-Шнирельман 假说就是：在显然必要的条件

$$d(A)+d(B)\leqslant 1$$

之下，可以用不等式

$$d(A+B)\geqslant d(A)+d(B) \tag{3.1}$$

代替前证的

$$d(A+B)\geqslant d(A)+d(B)-d(A)d(B).$$

从 (3.1)，在 $\sum_{i=1}^{k} d(A_i)\leqslant 1$ 的条件下，容易推出

$$d\left(\sum_{i=1}^{k} A_i\right)\geqslant \sum_{i=1}^{k} d(A_i). \tag{3.2}$$

上面的假说最初是通过具体的例子，在1931年由 Шнирельман 和 Landau 推想出来的，看起来这个假说很简单其实很难证明. Хинчин 在 $d(A_1)=\cdots=d(A_k)$ 的条件之下，首先证明了这个假说的成立. 接着有不少的数学家企图证实这个假说，但是都只得到部分的结果. 直到 1942 年才由 Mann 完全地证明了这个假说的成立. 在 1943 年 Artin 与 Scherk 给出了比较简单的证明. 1954 年 Kemperman 与 Scherk 给了新的更简单的证明，并有所推广，本章的陈述即以他们的论文为根据. 但为简单明确起见，只涉及整数.

令 n 为任一固定整数，I_n 为小于或等于 n 的非负整数的集合，A，B，C 是 I_n 的子集. 定义

$$A\oplus B=(A+B)\cap I_n. \tag{3.3}$$

特别当 A(或 B) 只包含一个元素 d 时，我们常把 $A\oplus B$ 写作 $d\oplus B$ (或 $A\oplus d$). 依照 Hadiwiger，我们又定义 $C\ominus A$ 为满足次述条件的元素 d 的集合，即 $d\in I_n$ 且 $A\oplus d\subset C$. 这样，$C\ominus A$ 就是满足 $A+D\subset C$ 的 I_n 的最大子集 D. 显然有 (我们用 $\longleftrightarrow$ 表示可以彼此互推)

$$A\oplus B\subset C\longleftrightarrow B\subset C\ominus A, \tag{3.4}$$

现在叙述我们的基本引理如下：

基本引理 设 $A \oplus B \subset C$，$0 \in A$，$0 \in B$，$n \notin C$，则一定有 $m \in I_n$ 存在，具有下列性质

$$C(n) - C(n-m) \geqslant A(m) + B(m), \tag{3.5}$$

$$m = n \text{ 或 } 0 < 2m < n, \tag{3.6}$$

$$n - m \in C \ominus A \quad n - m \in C \ominus B. \tag{3.7}$$

摆在我们面前的有两件事，第一是证明这个基本引理，第二是从基本引理导出不等式 (3.1). 比较起来，第二件容易得多，因此我们先作第二件.

显然，如果基本引理已建立，则立即推得下面的命题：

对任意自然数 n，存在一数 $m(1 \leqslant m \leqslant n)$ 使得

$$C(n) - C(n-m) \geqslant (\alpha + \beta)m.$$

式中 α, β 分别表 A，B 的密率 $d(A)$ 及 $d(B)$. 换句话说，从数列 $(1, n)$ 中可以截下一段 $(n-m+1, n)$ [我们用 (a, b) 表数列 $a, a+1, \cdots b$]. 使得在这一段中 C 的平均密度

$$\frac{C(n) - C(n-m)}{m}$$

至少是 $\alpha + \beta$.

上述命题成立是因为当 $n \in C$ 时

$$C(n) - C(n-1) = 1 \geqslant (\alpha + \beta) \cdot 1,$$

而当 $n \notin C$ 时，由基本引理，有 m 存在满足

$$C(n) - C(n-m) \geqslant A(m) + B(m) \geqslant (\alpha + \beta) \cdot m.$$

利用上述命题，我们可以从 $(1, n)$ 中截取一段 $(n-m+1, n)$ 使得在这段里面 C 的平均密度至少是 $\alpha + \beta$，又同样的可以截下一段 $(n-m-m'+1, n-m)$ 使其中 C 的平均密度至少是 $\alpha + \beta$. 如此反覆进行，经有限步骤分 $(1, n)$ 成有限段，每段平均密度至少是 $\alpha + \beta$，故对数列 $(1, n)$ 而言 C 的平均密度至少是

$$\frac{m(\alpha+\beta) + m'(\alpha+\beta) + \cdots}{m + m' + \cdots} = \alpha + \beta.$$

又因 n 是任意的，故

$$d(C) \geqslant \alpha + \beta. \qquad \text{[证完]}$$

剩下只有证明基本引理这一件事，但这是很复杂的一件工作，所以另立一节来讨论.

§4. 基本引理的证明

由于 $B \subset C \ominus A$，只需在较强条件

$$B = C \ominus A \tag{4.1}$$

的情况下证明基本引理.

设

$$A_0 = A, \quad B_0 = B. \tag{4.2}$$

又设 $e_1 \in A_0$ 是能使下列方程有解的最小元素，

$$e_1 + b_1 + b_1' = \bar{c}\begin{cases} \leqslant n, \\ \notin C, \end{cases} \tag{4.3}$$

其中 b_1，b_1' 均须属于 B_0（若无此类元素存在则在下面的 (4.8) 式中取 h 为 0），取定 e_1 以后，b_1 与 b_1' 一般不是唯一的. 设 B_1^* 表全部解 b_1，b_1' 的集合而 $A_1^* = e_1 \oplus B_1^*$. 于是 $B_1^* \subset B_0$. $A_0 \cap A_1^* = 0$，这因为若 $a_1 \in A_1^*$ 则有 $a_1 = e_1 + b_1$，由集合的构成知必有 b_1' 存在，使得 $e_1 + b_1 + b_1' = \bar{c}$，即 $a_1 + b_1'$ 不属于 C. 由此推出 $a_1 \notin A_0$（否则 $a_1 + b_1'$ 属于 C）.

设 B_1 是 B_1^* 在 B_0 中的余集（即属于 B_0 而不属于 B_1^* 的元素的集合）. 又设 $A_1 = A_0 \cup A_1^*$. 由(4.3)有

$$0 \notin B_1^*, \tag{4.4}$$

$$0 \in A_1, \quad 0 \in B_1. \tag{4.5}$$

引理 4.1

$$B_1 = C \ominus A_1.$$

证　由(4.1)及 A_1 与 B_1 的定义有

$$C \ominus A_1 \subset C \ominus A_0 = B_0, \tag{4.6}$$

$$B_1 \subset B_0. \tag{4.7}$$

若 $b_1 \in B_1^*$ 则有 b_1' 满足 (4.3)，即 $e_1 + b_1 + b_1' = \bar{c}$ 而 $e_1 + b_1' \in A_1^* \subset A_1$. 故 $b_1 \notin C \ominus A_1$. 由此推知 $C \ominus A_1$ 包含于 B_1^* 的余集 B_1 中，即 $C \ominus A_1 \subset B_1$.

反之，设 $b_1 \in B_0$，且 $b_1 \notin C \ominus A_1$，则有 $a_1 \in A_1$ 使 $a_1 + b_1 = \bar{c}$. 由于 $A_0 \oplus b_1 \subset C$，故 $a_1 \in A_1^*$ 即 $a_1 = e_1 + b_1'$，$b_1' \in B_1^*$. 由 $a_1 + b_1 = e_1 + b_1' + b_1 = \bar{c}$ 推知 $b_1 \in B_1^*$，故 $b_1 \notin B_1$. 由此

$$B_1 \subset C \ominus A_1. \qquad \text{[证完]}$$

用 A_1，B_1 代替前面的 A_0，B_0，我们可以仿前定义 e_2，B_2^*，A_2^*，B_2，A_2，重复运用这种步骤，我们可以定义 e_3，B_3^*，A_3^*，B_3，$A_3 \cdots$. 容易看出 B_ν 较 $B_{\nu-1}$ 中确实减少了若干元素，由于 B_ν 中元素的有限性，这一系列的步骤进行至有限次后必将停止，设次数为 $h \geqslant 0$. 此时有

$$A_h \oplus B_h \oplus B_h \subset C. \tag{4.8}$$

此外按归纳法易证

$$B_\nu = C \ominus A_\nu, \tag{4.9}$$

$$0 \notin B_\nu^* \quad 0 \in B_\nu \ (\nu = 1, 2, \cdots, h). \tag{4.10}$$

故

$$B_h \subset B_h \oplus B_h \subset C \ominus A_h = B_h.$$

由此有

$$B_h \oplus B_h = B_h. \tag{4.11}$$

引理 4.2

$$e_1 < e_2 < \cdots < e_h. \tag{4.12}$$

证　只需证 $e_1 < e_2$. 由定义 $e_2 \in A_1 = A_0 \cup A_1^*$. 若 $e_2 \in A_0$，则由 e_1 的极小性及 B_1^* 的定义即得 $e_1 < e_2$. 若 $e_2 \in A_1^*$ 则

$$e_2 = e_1 + b_1,\ b_1 \in B_1^*. \text{ 又 } 0 \notin B_1^* \text{ 故 } e_1 < e_2. \qquad \text{[证完]}$$

据 (4.10)，B_h 非空集. 设 $n - m$ 是它的最大元素，我们将证 m 具有 (3.5)—(3.7) 所要求的性质.

由 (4.11) 及 $n - m$ 的定义，我们有

$$2(n - m) = n - m \text{ 或 } 2(n - m) > n. \tag{4.13}$$

但 $B_h \subset B = 0 \oplus B \subset A \oplus B \subset C$. 故由 $n \notin C$ 推知 $n \notin B_h$ 故

有

$$n - m \neq n \tag{4.14}$$

结合(4.13)导出(3.6). 显然 $n - m \in B_h \subset B = C \ominus A$. 即(3.7)的前一部分成立. 又由 $n - m \in B_h$ 推知

$$n - m \notin B_1^*. \tag{4.15}$$

再由 c_1 的极小性,我们可以推出没有 $b_1' \in B_0$ 能满足

$$0 + (n - m) + b_1' \begin{cases} \in I_n, \\ \notin C, \end{cases}$$

这因为否则将得出 $n - m \in B_1^*$. 这又验证了(3.7)的后一部分: $n - m \in C \ominus B$.

下面我们用几个引理来证明(3.5)这个唯一待验证的性质.

引理 4.3

$$B(m) = \sum_{\nu=1}^{h} B_\nu^*(m).$$

证 $B = B_h \cup B_1^* \cup \cdots \cup B_h^*$. 又 B_ν^* 不相交,故只需证

$$B_h(m) = 0.$$

设 $b \in B_h$ 及 $b > 0$. 由(4.11), $b + (n - m) \in B_h$ 或大于 n. 由 $n - m$ 的极大性,第一个可能性不存在. 故 $b > m$ 即

$$B_h(m) = 0. \qquad \text{[证完]}$$

引理 4.4

$$C(n) - C(n - m) \geqslant A(m) + \sum_{\nu=1}^{h} A_\nu^*(m).$$

证 $A_h \oplus (n - m) \subset A_h \oplus B_h \subset C$. 故若 $0 < a \leqslant m$, $a \in A_h$ 则可推出

$$n - m < a + (n - m) \leqslant n, \quad a + (n - m) \in C.$$

由此

$$C(n) - C(n - m) \geqslant A_h(m) = A(m) + \sum_{\nu=1}^{h} A_\nu^*(m).$$

这因为 $A_h = A \cup A_1^* \cup \cdots \cup A_h^*$ 且 $A, A_1^*, \cdots, A_h^*$ 彼此不相交.

[证完]