

基原素数论

何宝起 著

大连出版社

基 原 素 数 论

何宝起 著

大 连 出 版 社 出 版

(大连市西岗区长白街12号 邮政编码 116011)

大连理工大学印刷厂激光照排排版

大连海事大学印刷厂印刷

新华书店发行

开本:787×1092 1/32 字数:75千字 印张:3.5

印数:1—2000册

1998年2月第1版

1998年2月第1次印刷

责任编辑:胡孝纯

责任校对:张积召

封面设计:范一峰

版式设计:张积召

ISBN 7-80612-490-x/0·2

定价:17.00元

序 言

素数在自然数中的分布情形非常有趣,神奇莫测,奥妙无穷。但是,在初等数学中有关素数的概念甚少,而这个小子可供广大的中学生做课外读物。在撰写中,出于让高中生能看懂的要求,应用了看来是最原始、最初级的数学方法,但却是前书所未曾有过的,系本书首次给出的新方法。即以“矩阵筛划法”和“筛线坐标法”,描绘和揭示了素数的某些性质和特征,使读者能够形象、直观地目睹素数分布的规律性,可取得从现有有关数论书上难以得到的直观性认识。诸如“复合数连排的最大区间”、“两个相邻素数的最大之差”、“ K^2 与 $(K+1)^2$ 之间有无素数”、“任一不小于 6 的偶数是否都可表为两个奇素数之和”、“任一不小于 9 的奇数是否都可表为三个奇素数之和”、“相差为 2 的‘素数对’是否分布无穷”等数论问题之迷已均被揭开,将给读者以详尽解答。这个小册子取名的涵义,即以最基础的数学方法来解释素数的性质和固有的规律性。

在撰写过程中,学者那吉生先生和彭肇藩教授、蔡海涛教授、欧阳维城教授等都曾给予有益的帮助,在此深表谢意。

在出版过程中,感谢孙宏安^①教授审阅了原稿,并提出了很好的意见;感谢出版社的同志给予了大力协助。

由于水平和条件所限,错误之处在所难免,恳请读者批评指正。

何宝起

一九九七年五月

^① 数学教授,曾任辽宁师范大学数学系主任,现任大连教育学院副院长。

符 号 说 明

1. $a, b, m, n, N, i, j, h, t, l, \tau$ 表示整数;
2. P, P_m, P_k 表示一般素数;
3. $P_0, P_1, P_2, \dots, P_r (P_r \leq \sqrt{n})$ 表示筛素数, P_i 表示其中任一筛素数; P_r^* (为 $\sqrt{2n}$ 中最大素数) 表示“回折双筛法”的最大筛素数;
4. F, F_i 表示奇复合数;
5. $\sum$ 表示求和;
6. $\prod_{i=1}^r P_i$ 表示乘积 $P_1 P_2 \dots P_r$;
7. $\{n\}$ 或 $\{N\}$ 表示数列 $1, 2, \dots, n$, 或 $1, 3, \dots, N$;
8. $\left[\frac{n}{P_i} \right]$ 表示 $\frac{n}{P_i}$ 的整数部分;
9. $\left\{ \frac{n}{P_i} \right\}$ 表示 $\frac{n}{P_i}$ 的小数部分;
10. $\|A\|, \|B\|, \|C\|$ 分别表示筛线坐标系数位线中 A、B、C 区的符号;
11. $\|N\|$ 即筛素数行矩阵体系符号;
12. NP_i 表示筛素数 P_i 行矩阵;
13. μP_i 即筛素数 P_i 的筛线符号;
14. $\pi(n, r)$ 表示未划数个数;
15. $E(n, r) = n \prod_{i=0}^r \left(1 - \frac{1}{P_i} \right)$ 表示未划数个数的比份式或素

素数个数的表达式；

16. $\mu(n, r)$ 即筛线坐标系符号；

17. $w_a(n, r)$ 表示展开式中小于 1 的项造成的误差；

18. $w_b(n, r)$ 表示展开式中大于 1 的项的小数部分造成的误差；

19. $w(n, r)$ 即未划数比份式(或素数个数表达式)的误差符号(为前两项 $w_a(n, r), w_b(n, r)$ 之和)；

20. $\overline{w(n, r)}$ 表示正差的误差波；

21. $\underline{w(n, r)}$ 表示负差的误差波；

22. $\mu_a(\overline{P_i}), \mu_b(\overline{P_i}), \mu_c(\overline{P_i})$, 分别表示筛线坐标系 $\|A\|, \|B\|, \|C\|$ 中 P_i 或 P_i+1 个连续奇数位上筛线峰掩盖数位密度符号；

23. $\mu_k(n, r)$ 表示复合数连排的最大区间；

24. $D(\frac{n}{P_i})$ 表示 $\frac{n}{P_i} \geq 1$ ；

25. $w(\frac{n}{P_i})$ 表示 $\frac{n}{P_i} < 1$ ；

26. $\pi(n)$ 表示 n 内的素数个数；

27. $\pi_i(n)$ 表示 n 的“双筛素数”个数；

28. $\pi_s(n)$ 表示 n 时“素对子”的个数；

29. $\pi_b(n)$ 表示 n 内“差为 2 的素数对”的个数；

30. 符号 $\sim$ 表示相似； $\simeq$ 或 $\approx$ 表示“约等”。

目 录

第一章 概论	1
§ 1 名词概念	1
§ 2 判定素数的最基本法则	3
§ 3 素数分布简况	5
第二章 筛素数行矩阵筛划法	10
§ 1 筛素数行矩阵的布构	10
§ 2 筛素数行矩阵的性质	11
§ 3 筛素数行矩阵筛划法	14
§ 4 未划数个数比份式的分析	15
第三章 筛线坐标法	22
§ 1 筛线坐标系的布构	22
§ 2 未划数个数的比份式	23
§ 3 筛线坐标系的性质	26
§ 4 未划数不等式定理	44
§ 5 素数个数的表达式	54
第四章 双筛素数	58
§ 1 双筛素数比份式的分析	58
§ 2 回折双筛法	65
§ 3 并列双筛法	86
第五章 若干其他定理	91

§ 1	复合数的分解	91
§ 2	素数个数无穷	92
§ 3	逐步淘汰法则	92
§ 4	Чебышев 定理	94
§ 5	Bertrand 假设	98

第一章 概 论

§ 1 名词概念

整数

整数有正负之分。 $1, 2, 3, \dots, n$ 即正整数,也叫自然数;
 $-1, -2, -3, \dots, -n$ 即负整数。显然,整数之间进行加减乘
运算仍为整数。

整数有奇偶之分。 $1, 3, 5, 7, 9, \dots$ 为奇数; $2, 4, 6, 8, 10, \dots$
称偶数。

倍数和因数

若第一个数可被第二个数整除,则称第一个数为第二个
数的倍数,第二个数为第一个数的因数;当第二个数既不为
1,又不同于第一个数,即称第二个数为第一个数的真因数。如
有两个整数 a 和 b ,若 $a=mb$ (m 为整数),当 $m=1$ 时,即 $a=b$,
说明 a 只有 1 和自身为因数;当 $|m|>1$ 时,则说明 a 不仅
有 1 和自身为因数,而且还有 b 与 m 为真因数。

素数及复合数

将自然数分为三类:

1. 1——只可被自身所整除,即只有自身一个数为其因
数;

2. 素数——(亦叫质数)只可被 1 和自身所整除,即只有

1 和自身两个数为其因数。如 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37... 等都是不被除 1 和自身外的任何数所整除。;

3. 复合数——(亦称合数)既可被 1 和自身所整除, 还可被其它整数所整除, 即不仅有 1 和自身两个数为其因数, 而且又有两个或两个以上的整数为其真因数。如 15 不仅有 1 和自身 15 两个因数, 而且还有 3 和 5 两个真因数。4, 6, 8, 10, ... 除 2 以外的偶数皆为复合数; 9, 15, 21, 25, ... 等为奇复合数。

筛素数

在判定和计算 n 内的素数及其个数时, 我们以 $\sqrt{n}$ 之内的素数为根据, 称其为“筛素数”, 以符号 $P_0=2, P_1=3, P_2=5, \dots, P_r \leq \sqrt{n} < P_{r+1}$ 表示。

回筛素数

在判定和计算 n 时的“素对子”及其个数时, 把 $\sqrt{2n}$ 内的素数称为回筛素数, 以符号 $P_0=2, P_1=3, P_2=5, \dots, P_r^* \leq \sqrt{2n} < P_{r+1}^*$ 表示(定义见第四章第二节)。

双筛素数

我们把“素数”看作是倍数行(列)单一筛划后的剩留数, 而把两行(列)双重筛划后的剩留数称为“双筛素数”(定义见第四章第一节)。

素对子

两个平均值为 n 的奇素数称为“素对子”(定义见第四章第二节)。

素数对

一般指“差为 2 的两素数”, 有的也称为“双生素数对”或“孪生素数对”。如 3, 5; 5, 7; 11, 13; 17, 19; 29, 31; 41, 43; ...

(定义见第四章第三节)。

自然数列

公差为 1 的自然数列 $1, 2, 3, 4, \dots, n$ 。

奇数列

公差为 2 的奇数列 $1, 3, 5, 7, 9, \dots, n$ 。

偶数列

公差为 2 的偶数列 $2, 4, 6, 8, 10, \dots, n$ 。

等差数列

公差为 d 的 (d 为整数) 数列

$$a_1, a_2, a_3, a_4, \dots$$

(其中 $a_2 = a_1 + d, a_3 = a_2 + d, \dots; a_1$ 为整数; $d \geq 1$)

§ 2 判定素数的最基本法则

定理 对 n 内 (1 除外) 的自然数, 划去所有不大于 $\sqrt{n}$ 的各素数的一切倍数 (各素数本身除外) 后所剩留之数即为不大于 n 的全部素数。

证明 设自然数列为

$$2, 3, 4, 5, \dots, n (n \geq 4);$$

$$P_0 = 2, P_1 = 3, \dots, P_r \leq \sqrt{n} < P_{r+1}$$

将数列中依次划去

$$\left. \begin{array}{l} 2P_0, 3P_0, 4P_0, \dots; \\ 2P_1, 3P_1, 4P_1, \dots; \\ 2P_2, 3P_2, 4P_2, \dots; \\ \dots\dots\dots \\ 2P_r, 3P_r, 4P_r, \dots \end{array} \right\} \quad (1.1)$$

之后所剩之数,都不能被 $P_0, P_1, \dots, P_r$ 各素数所整除(称为同其“互素”)。假设所剩之数中有某复合数为

$$F = aP_m \quad (1.2)$$

其中 F 为 n 内的数; P_m 为异于 $P_0, P_1, P_2, \dots, P_r$ 的素数; a 为整数,即

$$\begin{aligned} F &= aP_m \leq n \\ P_m &> \sqrt{n} \geq P_r \end{aligned}$$

则有

$$a < \sqrt{n} < P_{r+1}$$

所以,不论 a 是前 $r+1$ 个中某一素数或是一复合数,其 F 必为前 $r+1$ 个中某素数所整除,即 F 在(1.1)式中必被划除,因而 F 为复合数的假设不能成立,故 n 内所剩之数皆为素数。

显然,其倍数

$$\begin{aligned} &2P_{r+1}, 3P_{r+1}, 4P_{r+1}, \dots, (P_{r+1}-1)P_{r+1} \text{ 的系数} \\ &2, 3, 4, \dots, (P_{r+1}-1) \end{aligned} \quad (1.3)$$

中的任一项均有 $< P_{r+1}$, 则(1.3)式中各项,或为前 $r+1$ 个素数中某素数或被其中某素数所整除,即于(1.1)式中被划除,故令

$$r=1, 2, \dots$$

时,(1.1)式则可简化为

$$\left. \begin{aligned} &P_0^2, 3P_0, 4P_0, 5P_0, \dots \\ &P_1^2, 5P_1, 7P_1, 9P_1, \dots \\ &P_2^2, 7P_2, 11P_2, 13P_2, \dots \\ &\dots\dots\dots \end{aligned} \right\} \quad (1.4)$$

定理得证。

基于以上定理,我们把 $\sqrt{n}$ 之内的前 $r+1$ 个素数称为判定 n 内素数的“筛素数”,以符号 $P_0, P_1, P_2, \dots, P_r$ 表之。

例 设自然数列为

$$2, 3, 4, 5, \dots, 100;$$

其筛素数为 $P_0=2, P_1=3, P_2=5, P_3=7$ 为 $\sqrt{100}$ 内最大素数。判定 $n=100$ 内的素数有哪些?

解 应用以上定理和法则,由(1.4)式,将100内复合数逐次除去:

$$4, 6, 8, 10, \dots, 98, 100;$$

$$9, 15, 21, 27, \dots, 93, 99;$$

$$25, 35, 55, 65, 85, 95;$$

$$49, 77, 91。$$

所剩数有

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59,$$

$$61, 67, 71, 73, 79, 83, 89, 97$$

25个数为100之内的全部素数。

§ 3 素数分布简况

了解不大的 n 内的素数分布情况可察看“素数表”。现有较完善的“素数表”是查基尔作出的,他把50 000 000内的素数全部列出来了。现将100 000 000内素数的分布情况列出(1.1)表如下。表中 n 表自然数, $\pi(n)$ 表 n 内的素数个数。

表(1.1)

n	$\pi(n)$	$\frac{\pi(n)}{n}$	$\frac{\pi(n)}{n - \pi(n)}$	$\frac{n}{\log n}$	$\frac{\pi(n)}{\frac{n}{\log n}}$
1 000	168	0.1680	0.2019	145	1.1586
10 000	1 229	0.1229	0.1401	1 086	1.1317
100 000	9 592	0.0959	0.1061	8 686	1.1043
1 000 000	78 498	0.0785	0.0852	72 382	1.0845
10 000 000	664 579	0.0665	0.0712	620 417	1.0712
100 000 000	5 761 455	0.0576	0.0611	5 428 613	1.0613

此表提示我们：

1. 素数个数有无限多个。通过借助于电子计算机和特殊方法现在已知的最大素数为 $2^{1398267} - 1$ ；

2. n 中素数个数在 n 中的比例，随 n 的不断增大而逐渐减少。通过素数个数 $\pi(n)$ 与 n 的比值来看：

n 为 1 000 时的比值为 0.1680，

n 为 10 000 时的比值为 0.1229，

n 为 100 000 时的比值为 0.0959，

n 为 1 000 000 时的比值为 0.0785，

n 为 10 000 000 时的比值为 0.0665，

n 为 100 000 000 时的比值为 0.0576，

.....

比值随 n 的增大而减小，随 n 的不断增大而越来越接近于 0；

3. n 中素数个数在其复合数中的比例，也随 n 的不断增大而逐渐减小。通过素数个数 $\pi(n)$ 与复合数个数 $n - \pi(n)$ 的比值来看：

n 为 1 000 时的比值为 0.2019,
 n 为 10 000 时的比值为 0.1401,
 n 为 100 000 时的比值为 0.1061,
 n 为 1 000 000 时的比值为 0.0852,
 n 为 10 000 000 时的比值为 0.0712,
 n 为 100 000 000 时的比值为 0.0611,

比值随 n 的继续增大而逐步接近于 0;

4. n 内的素数个数与 $\frac{n}{\log n}$ 的值相当。通过素数个数 $\pi(n)$ 与 $\frac{n}{\log n}$ 的比值来看:

n 为 1 000 时的比值为 1.1586,
 n 为 10 000 时的比值为 1.1317,
 n 为 100 000 时的比值为 1.1043,
 n 为 1 000 000 时的比值为 1.0845,
 n 为 10 000 000 时的比值为 1.0712,
 n 为 100 000 000 时的比值为 1.0613,

比值随 n 的增大而越来越接近于 1。这就是“素数定理”:

$$\pi(n) \sim \frac{n}{\log n} \quad (1.5)$$

(阿达马和德·拉·瓦莱·普森于 1896 年各自独立地证明了该定理)。这样,欲知 n (任意正整数) 内有多少个素数时,即可极易求出 $\frac{n}{\log n}$ 的值,也就知道了素数的大约个数。这里附上 5000 内的素数表(1.2)。

5000 内的素数表

表(1.2)

2	3	5	7	11	13	17	19	23	29	31
37	41	43	47	53	59	61	67	71	73	79
83	89	97	101	103	107	109	113	127	131	137
139	149	151	157	163	167	173	179	181	191	193
197	199	211	223	227	229	233	239	241	251	257
263	269	271	277	281	283	293	307	311	313	317
331	337	347	349	353	359	367	373	379	383	389
397	401	409	419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503	509	521	523
541	547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659	661
673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823
827	829	839	853	857	859	863	877	881	883	887
907	911	919	929	937	941	947	953	967	971	977
983	991	997	1009	1013	1019	1021	1031	1033	1039	1049
1051	1061	1063	1069	1087	1091	1093	1097	1103	1109	1117
1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213
1217	1223	1229	1231	1237	1249	1259	1277	1279	1283	1289
1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453
1459	1471	1481	1483	1487	1489	1493	1499	1511	1523	1531
1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607
1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693
1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777
1783	1787	1789	1801	1811	1823	1831	1847	1861	1867	1871
1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951
1973	1979	1987	1993	1997	1999	2003	2011	2017	2027	2029
2039	2053	2063	2069	2081	2083	2087	2089	2099	2111	2113
2129	2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287	2293
2297	2309	2311	2333	2339	2341	2347	2351	2357	2371	2377

续表(1.2)

2381	2383	2389	2393	2399	2411	2417	2423	2437	2441	2447
2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551
2557	2579	2591	2593	2609	2617	2621	2633	2647	2657	2659
2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713
2719	2729	2731	2741	2749	2753	2767	2777	2789	2791	2797
2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887
2897	2903	2909	2917	2927	2939	2953	2957	2963	2969	2971
2999	3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181	3187
3191	3203	3209	3217	3221	3229	3251	3253	3257	3259	3271
3299	3301	3307	3313	3319	3323	3329	3331	3343	3347	3359
3361	3371	3373	3389	3391	3407	3413	3433	3449	3457	3461
3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539
3541	3547	3557	3559	3571	3581	3583	3593	3607	3613	3617
3623	3631	3637	3643	3659	3671	3673	3677	3691	3697	3701
3709	3719	3727	3733	3739	3761	3767	3769	3779	3793	3797
3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889
3907	3911	3917	3919	3923	3929	3931	3943	3947	3967	3989
4001	4003	4007	4013	4019	4021	4027	4049	4051	4057	4073
4079	4091	4093	4099	4111	4127	4129	4133	4139	4153	4157
4159	4177	4201	4211	4217	4219	4229	4231	4241	4243	4253
4259	4261	4271	4273	4283	4289	4297	4327	4337	4339	4349
4357	4363	4373	4391	4397	4409	4421	4423	4441	4447	4451
4457	4463	4481	4483	4493	4507	4513	4517	4519	4523	4547
4549	4561	4567	4583	4591	4597	4603	4621	4637	4639	4643
4649	4651	4657	4663	4673	4679	4691	4703	4721	4723	4729
4733	4751	4759	4783	4787	4789	4793	4799	4801	4813	4817
4831	4861	4871	4877	4889	4903	4909	4919	4931	4933	4937
4943	4951	4957	4967	4969	4973	4987	4993	4999		