DISQUISITIONES ARITHMETICAE

算术探索

[德] 高斯 著

潘承彪 张明尧 译

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

DISQUISITIONES ARITHMETICAE

算术探索

[德] 高斯 著

潘承彪 张明尧 译

由黑龙江省精品图书出版工程专项资金资助出版

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

图书在版编目(CIP)数据

算术探索/(德)高斯著;潘承彪,张明尧译. —哈尔滨:哈尔滨工业大学出版社,2011.8
ISBN 978-7-5603-3409-7

Ⅰ.①算… Ⅱ.①高…②潘…③张… Ⅲ.①算术-研究 Ⅳ.①O121

中国版本图书馆 CIP 数据核字(2011)第 222809 号

策划编辑 刘培杰 张永芹
责任编辑 王勇钢
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 黑龙江省教育厅印刷厂
开 本 787mm×1092mm 1/16 印张 31 字数 740 千字
版 次 2011 年 12 月第 1 版 2011 年 12 月第 1 次印刷
书 号 ISBN 978-7-5603-3409-7
定 价 158.00 元

内容简介

《算术研究》是被誉为“数学王子”的德国大数学家高斯的第一部杰作，该书写于1797年，1801年正式出版. 这是一部用拉丁文写成的巨著，是数论的最经典及最具权威性的著作. 在随后的200年时间中被翻译成多国文字，如德文、英文、俄文等.

这部著作在数学中的重要地位不亚于《圣经》在基督教中的地位，只有欧几里得的《几何原本》堪与之相比. 因为高斯有一句名言：“数学是科学的女皇，数论是数学的女皇.”这部著作共七篇.

第一篇讨论一般的数的同余. 并首次引进了同余记号，这是现代数学中无处不在的等价和分类概念出现在代数中的最早的意义重大的例子.

第二篇讨论一次同余方程. 其中严格证明了算术基本定理.

第三篇讨论幂的同余式. 此篇详细讨论了高次同余式.

第四篇“二次同余方程”意义非同寻常. 因为其中给出了二次互反律的证明，有人统计到21世纪初，二次互反律的证明已经超过200种，其中柯西、雅可比、迪利克雷、艾森斯坦、刘维尔、库默尔、克罗内克、戴德金、瓦莱-布桑、希尔伯特、弗罗贝尼乌斯、斯蒂尔切斯、M·里斯、韦伊都给出了新证法，可见问题之重要.

第五篇是“二次型与二次不定方程”在这一篇中关于二次型的特征的研究，标志着群特征标理论的肇始，使高斯成为群论的先驱者之一.

第六篇把前面的理论应用到各种特殊情形，并引入了超越函数.

第七篇是“分圆方程”，不少人认为此篇是《算术研究》的顶峰.

《算术研究》当时对于数学家也很难读，它曾被称为“七印封严之书”（这是西方人对难解之书喜用的词，近于中国人所谓的“天书”，典出《圣经·启示录》第五章第一节：“我看见坐宝座的右手中有书卷，里外都写着书，用七印封严了”）后来迪利克雷作了详细注释. 此书简洁完美的风格多少减慢了它的传播速度，而最终当富有才华的年轻人开始深入研读它时，由于出版商的破产，又买不到它了，甚至高斯最喜欢的学生艾森斯坦从未能拥有一本，有些学生不得不从头到尾抄录全书.

序

本书所探索的内容是属于数学中研究整数的那一部分，在大多数情形将不讨论分数，而且从不涉及无理数（俄、德为“虚数”以后再加译注）. 通常所谓的不定分析或 Diophantus 分析，是讨论从满足一个不定方程的无穷多个解中去选出那些是整数或至少是有理数（通常还要求是正的）解的学问，它并不是彻底研究这一学科，而仅是这学科的十分特殊的一部分，它和这整个学科的关系差不多如同方程变形与解方程的学问（代数学）与整个分析学的关系一样. 这就是说，如同所有涉及数量及它们之间的关系的一般性质的研究属于分析的领域一样，整数（及分数——在它们由整数确定的意义下）是算术研究的真正对象. 然而，因为通常所说的算术很难超出记数与计算的技巧（即以确定的形式来表示数，例如十进位表示，以及对其进行算术运算），同时它还常常包含这样一些问题，它们或者与算术毫无关系（如对数理论），或者不仅对整数而且对任意的数量也有意义，所以这样来区分这两部份算术看来是适当的：把刚刚说到的这些称为初等算术，而把所有关于整数间内在联系的一般研究归入高等算术. 本书将只讨论高等算术.

Euclid 在其《几何原本》的第七及其后几卷中，以古人所固有的优美而又严格讨论的论题就是属于高等算术，不过这些内容仅可看做是这学科的一个导引. 全部用于讨论不定分析问题的 Diphantus 的名著包含了许多研究，由于它们的难度及他所用的精妙方法，特别是，考虑到只有很少的辅助工具可供他应用，这些研究激起了人们对作者的才智和洞察力的高度关注. 然而，因为对这些问题要求创新性和灵巧性甚于需要深刻的原理. 此外，这些问题过于特殊以及很难导致更为普遍性的结论，所以，把这本书看做是开创了一个数学迅速发展的时代，是由于它本身记录了代数学所特有的巧妙技巧的最早踪迹，而不是由于它以新的发现丰富了高等

算术. 主要的是由于近期的研究,虽然确实不多,但赢得了永恒的声誉,它们是属于 P. de Fermat, L. Euler, L. Lagrange 及 A. M. Legendre(以及另外少数几位),我们应当感谢他们开启了通向这一神圣科学宝藏的入口,并揭示了它所蕴含的宝藏是何等丰富. 但是,我不再在这里列举这些学者的一个又一个发现,因为它们可在 Lagrange 为 Euler 的《代数学》所加的附录的前言中,及 Legendre 最近的著作(我将立刻提到它)中找到;此外,这些发现中的许多也将在本书的相应之处加以引述.

本书的目的是介绍我在高等算术领域所做的探索与研究,早在五年前我就允诺要出版这本书,现在它包括了我在早前及在这一段时间所做的两部份工作. 为了避免有人感到奇怪,为什么本书的内容要追溯到许多最简单的原理,而且还要重新讨论许多已被其他人卓有成效地研究过的结果,我在此必须向读者说明:当我在 1795 年初开始转向这种探索时,我并不知道这一领域中近期的这些最新发现,同时用于得到我自己的结果的方法技巧都是我自己想出来的. 事情是这样的,在从事其它工作时我偶然发现了一个极不寻常的正确的算术命题(如果我没有记错的话,这就是本书第 108 目所说的那个定理),因为我认为不仅它本身是这样的漂亮,而且感觉到它还会与其他著名的重要结论有联系,所以我把自己的全部精力集中于去搞清楚它所依赖的原理并给出严格的证明. 当我在这方面最后取得成功后,我就被这些问题所深深地吸引而一发不可收拾了. 这样一来,在我接触到其他学者的类似研究工作之前,我就已经得到了一个又一个结论,从而完成了本书前四篇所介绍的绝大多数内容. 最后,当我有可能拜读这些天才人物的著作后,我才认识到我所深入思考的大部分内容都是早已知道的东西. 但是,这只是更增加了我的兴趣,并努力尝试沿着他们的足迹进一步去发展算术. 这就产生了不同的研究,其中的部分结果已被安排在第五、第六和第七篇中. 稍后,我开始考虑发表我努力所得的这些成果,并说服自己不要删去任何早期研究所得的成果,这是因为,首先,在那时还没有一本书把其他学者的工作收集在一起,而这些工作只是散见于一些学术研究机构的会报纪事中;其次,这些研究中的多数结果是全新的,且其中大多数结果还是用新方法讨论的;最后,所有的结果之间有着如此密切的联系,以致于如果不从一开始就重提前面的某些工作,后面的新成果就难以充分阐述清楚.

就在这时,出现了当时已经在高等算术领域做出了巨大贡献的 Legendre 的杰出著作《数论(Essai d´une théorie des nombres, Paris, a. VI)》,书中他不仅把到当时所发现的所有结果都收集在一起并加以系统整理,而且添加了许多他本人的新结果. 因为我过晚才见到这本书,当看到它时本书的大部分书稿已经完成并交给了出版商,所以当讨论类似的问题时,我就没有机会处处提到它了. 只是对该书的我认为是必要的若干部分在补记中给出某些注记,我期望这位通情达理的学者不会不注意到这些并以他的宽容和真诚对此给予善意的理解. (按法文本))

本书的出版在超过四年的时间里遇到了许多阻碍. 在这一段时间里,我不仅进一步继续过去已经开始进行的研究(当时为了避免本书篇幅过大,决定分离出这些研究,准备在另外的地方发表),而且也从事许多新的研究. 此外,有许多我过去只是稍有触

及而当时觉得似乎不必详细讨论的问题(例如,第37目,第82目及其后各目和其他的若干目)也得到了进一步发展,并导致一些看来是值得发表的更一般的结论(参见补记中关于第306目的注记).最后,主要由于第五篇的内容使本书的篇幅变得大大超出我原来的预期,使我只得削减了最初打算写的不少内容,特别是删去了整个第八篇(在本书的若干处已经提到了该篇,它包含了任意次代数同余方程的一般讨论(俄)).在条件允许时,我将尽早地发表所有这些研究成果,它们容易构成与本书篇幅相当的一本书.

在多处困难的讨论中,我采用了综合性证明,且隐匿了导致这样的证明的分析,这样做主要是由于简洁性的要求,而这是我尽可能地力求做到的.

第七篇讨论的是分圆理论或正多边形理论,它本身不属于算术,但所涉及的那些原理无疑是唯一地依属于高等算术的.或许这会出乎数学家们的意料,但我希望他们对从这样的讨论导出的这些新结论会同样地感到高兴.

以上就是我要请读者注意的一些事情.至于此书本身的价值,不是我应加以判断的.我最大的愿望是,它会使得那些关心科学发展的人士感到高兴,不论是由于本书所提出的解法正是他们所一直寻求的,还是由于它开创了通向新探索的途径.

目　录

第一篇　数的同余[1]　第 1 ~ 12 目

§1. 同余的数，模，剩余及非剩余　第 1 ~ 3 目

1.

若数 a 是数 b 和 c 的差的除数，则称 b 和 c 对于 a **同余**；在相反的情形，则称 b 和 c 对于 a **不同余**. 我们把数 a 称为**模**. 在第一种情形，数 b 和 c 中的每一个称为是它们中的另一个的**剩余**，而在第二种情形，则称为是它们中的另一个的**非剩余**.

这些概念和符号可用于所有整数间的关系，无论是正的或负的整数①[2]，但一定不能推广到分数. 例如，-9 和 $+16$ 对模 5 同余；-7 对模 11 是 $+15$ 的剩余，但对模 3 是 $+15$ 的非剩余. 因为 0 被任意数整除，所以对任意的模每个数都和它自己同余.

2.

给定的数 a 对模 m 的所有剩余由公式 $a + km$ 给出，其中 k 是任意整数. 由此可立即推出我们在下面要给出的定理中的大多数，当然一看就知道它们也能容易地直接证明.

此后，我们将用符号“≡”来表示数的同余关系，当必需要指出模时，在其后用括号写出模，例如，$-7 \equiv 15 \pmod{11}$，$-16 \equiv 9 \pmod{5}$②[3].

3.

定理　**设给定 m 个相邻整数 $a, a+1, a+2, \cdots, a+m-1$，及某个整数 A. 那么，在这 m 个整数中有且仅有一个数对模 m 同余于 A.**

若 $\frac{a-A}{m}$ 是整数，则 $a \equiv A$；若它是分数，则设 k 是最接近它且大于它的整数（若这分数是负的，则是最接近它，且按绝对值来说是小于它的整数），这时，$A + km$ 将位于 a 和 $a + m$ 之间，因此这就是所要的数. 显见，所有的比 $\frac{a-A}{m}, \frac{a+1-A}{m}, \frac{a+2-A}{m}, \cdots$ 均位于

---

① 显见，模总是应取其绝对值，即不计正负号.

② 我采用这一符号是因为在同余和相等之间有很大相似之处. 基于同样的理由，Legendre 在他的著作（以后我们将经常引用）中，对同余就简单地采用了与相等一样的符号. 为了避免混淆，我没有仿效他，而作了区分.

$k-1$ 和 $k+1$ 之间，所以它们中不能有一个以上的整数.

§2 最小剩余 第4目

4.

这样一来，每个数在数组 $0,1,2,\cdots,m-1$ 及数组 $0,-1,-2,\cdots,-(m-1)$ 中对模 m 都恰有一个剩余，我们将称它们是**最小剩余**. 显然，如果 0 不是剩余，那么最小剩余总是有两个，一个为**正**一个为**负**. 如果它们的绝对值不相等，那么必有一个的绝对值小于 $\frac{m}{2}$；不然，它们的绝对值都等于 $\frac{m}{2}$. 因而，每个数总有一个剩余其绝对值不超过模的一半. 这个剩余称为**绝对最小剩余**[4].

例如，对于模 5，-13 的最小正剩余为 2（它也是绝对最小剩余），而 -3 是它的最小负剩余. 对于模 7，$+5$ 是它自身的最小正剩余，而 -2 是它的最小负剩余，也是**绝对最小剩余**.

§3 关于同余的若干基本定理 第5 ~ 11目

5.

引入这些概念后，我们来列出关于同余的一些十分显然的性质.

对合数模同余的两个数，一定对这个模的每一个除数也同余.

如果对同一个模，若干个数都同余于同样的数，那么，对这个模它们彼此都同余.

在下面这些定理中，我们总假定模是相同的.

同余的数有同样的最小剩余，不同余的数有不同的最小剩余.

6.

如果给定有限个数 $A,B,C,\cdots$，及另外同样多个数 $a,b,c,\cdots$，它们相应地都对某个模同余，即

$$A\equiv a,B\equiv b,C\equiv c,\cdots,$$

那么

$$A+B+C+\cdots\equiv a+b+c+\cdots.$$

若 $A\equiv a,B\equiv b$，则 $A-B\equiv a-b$.

7.

若 $A\equiv a$，则 $kA\equiv ka$.

如果 k 是正的，那么这只是上一目中的定理的一个简单特例，即取 $A=B=C=\cdots$，及 $a=b=c=\cdots$. 如果 k 是负的，那么 $-k$ 是正的，因而有 $-kA\equiv -ka$，由此推出 $kA\equiv ka$.

若 $A\equiv a,B\equiv b$，则有 $AB\equiv ab$.

因为,$AB \equiv Ab \equiv ab$.

8.

如果给定有限个数$A,B,C,\cdots$,及另外同样多个数$a,b,c,\cdots$,它们相应地都对某个模同余,即$A \equiv a, B \equiv b, C \equiv c, \cdots$,那么,这两组数的乘积也同余,即$ABC\cdots \equiv abc\cdots$.

从上一目可知,$AB \equiv ab$,同理推出$ABC \equiv abc$,以及任意有限多个都可以这样相乘.

如果所有的数$A,B,C,\cdots$均相等,以及相应的数$a,b,c,\cdots$亦均相等,那么可得下面**定理:**

若$A \equiv a$,及k是正整数,则有$A^k \equiv a^k$.

9.

设X是变数x的形如

$$Ax^a + Bx^b + Cx^c + \cdots$$

的代数函数,其中$A,B,C,\cdots$是任意整数,而$a,b,c,\cdots$是非负整数. 那么,若变数x所取的各个值都对某个模同余,则相应的函数X所取的各个值也都对这个模同余.

设f,g是x所取的同余的数. 那么,从上一目知$f^a \equiv g^a$及$Af^a \equiv Ag^a$,同理可得$Bf^b \equiv Bg^b$等. 因而有

$$Af^a + Bf^b + Cf^c + \cdots \equiv Ag^a + Bg^b + Cg^c + \cdots$$

证毕.

容易看出,应如何把这定理推广至多变数函数的情形.

10.

这样一来,如果变数x依次用全部整数代入,并把函数X的对应的值划归为它的最小剩余,那么,这些值将构成一个序列,这序列中在由相邻的m(m是模)项组成的一组值之后,将循环地重复出现同样的这些项,也就是说,这序列是以m项为周期,无穷多次重复所构成的. 例如,设$X = x^3 - 8x + 6$及$m = 5$,那么,对$x = 0,1,2,3,4,\cdots$,由X的值所得到的最小剩余是:1,4,3,4,3,1,4,…,其中开头的5个数1,4,3,4,3总是无穷多次重复;而如果这序列按反方向依次取值,即使x取负值,那么,将有同样的周期但这些项的次序相反. 由此显见,在整个序列中不会出现与这周期中的值不同的项.

11.

由于在上面这个例子中,$X \equiv 0$及$\equiv 2 \pmod 5$都不能成立,所以它更不能等于0或2. 因此,方程$x^3 - 8x + 6 = 0$和$x^3 - 8x + 4 = 0$都没有整数解,进而可知,它们都没有有理数解[5]. 更一般地,如果变数x的函数X有如下的形式

$$x^n + Ax^{n-1} + Bx^{n-2} + \cdots + N$$

其中$A,B,C,\cdots$是整数,n是正整数,那么,只要同余式$X \equiv 0$对某个模不能成立,方程$X = 0$(我们知道,所有的代数方程都能化为这样的形式)就没有有理根[5]. 这个十分显然

的判别法将在第八篇[6] 作更充分的讨论. 不过,从这个例子我们已经可以对这种讨论的用处得到一点自己的想法和理解.

§4 若干应用 第12目

12.

在算术研究中常用的许多结论都是基于本篇所讨论的定理,例如,判断给定的数能否被9,11,或其他整数**整除的法则. 对模9** 所有10的方幂都同余于1. 所以,如果给定的数是形如 $a + 10b + 100c + \cdots$,那么,对模9它与数 $a + b + c + \cdots$ 有相同的最小剩余. 由此可知,若把一个数的十进表示中的各位数字相加,则这个和一定与所给的数有相同的最小剩余,因而,若前者能被9整除则后者也能被9整除,且反过来也对. 以上的讨论及法则对除数3同样成立. 此外,因为**对模** 11,$100 \equiv 1$,所以总有,$10^{2k} \equiv 1$,而 $10^{2k+1} \equiv 10 \equiv -1$,因此,形如 $a + 10b + 100c + \cdots$ 的数与数 $a - b + c - \cdots$ 对模11有相同的最小剩余. 由此就立即推出熟知的法则. 同理我们可容易地推得所有类似法则.

利用以上同样的论证,我们也能发现这样的基本原理,它常被推荐来作为**算术运算的检验法则**. 这就是,如果有一个数是由给定的若干个数通过加,减,乘,或乘幂等运算所得到的,那么,对于某个适当的模(通常是用9或11,因为,正如已经看到的,在十进制中容易求得其剩余),把给定的这些数分别用它们的最小剩余代替后再作同样的运算,这样所得到的数一定同余于原来所得到的数. 如果不是这样,则运算一定有错.

由于这些及其他类似的结论是熟知的,这里来细说它们将是多余的.

第二篇　一次同余方程　第 13 ~ 44 目

§5　关于素数、因数等的若干预备定理　第 13 ~ 25 目

13.

定理　**两个小于给定素数的正数的乘积不能被这个素数整除.**

设 p 是素数,正数 $a < p$. 这时可以断言,不存在小于 p 的正数 b,使得 $ab \equiv 0 \pmod{p}$.

证明　若定理不成立,则有正数 $b,c,d,\cdots$ 都小于 p,使得 $ab \equiv 0, ac \equiv 0, ad \equiv 0, \cdots \pmod{p}$. 设 b 是这些正数中的最小的,这样,在小于 b 的正数中没有一个具有所说的性质. 显然有 $b > 1$,因为若 $b = 1$,则由假设知 $ab = a < p$,所以不能被 p 整除. 由于 p 是不能被 b 整除的素数,它一定位于 b 的两个相邻倍数之间,设为 mb 和 $(m+1)b$. 设 $p - mb = b'$,b' 是小于 b 的正数. 因为根据假设有 $ab \equiv 0 \pmod{p}$,所以也有(根据第 7 目)$mab \equiv 0$,将它与 $ap \equiv 0$ 相减得到 $a(p - mb) = ab' \equiv 0$,即 b' 一定是 $b,c,d,\cdots$ 中的一个,但 b' 小于它们中的最小的,矛盾. 证毕.

14.

若 a 和 b 都不能被素数 p 整除,则乘积 ab 也不能被 p 整除.

设 α,β 分别是 a,b 对模 p 的最小正剩余,由假设知它们都不等于 0. 若 $ab \equiv 0 \pmod{p}$,则有 $\alpha\beta \equiv 0$,因为 $ab \equiv \alpha\beta$. 这和上面的定理矛盾.

虽然,Euclid 在他的《*Elements*(原本)》(Ⅶ,32) 中早已证明了这一定理,但我们不想在这里忽略它. 这首先是因为,现在的许多作者要么是常常忽略了这定理的证明,要么是给出了不能令人信服的论证;其次是因为,通过这个最简单的情形能使我们更容易地理解这一证明方法的实质,而这方法在以后要被用来解决更为困难得多的问题.

15.

若 $a,b,c,d,\cdots$ 都不能被素数 p 整除,则乘积 $abcd\cdots$ 也不能被 p 整除.

由上一目知,ab 不能被 p 整除,所以 abc 也不能被 p 整除,类似地可以推出 $abcd$ 也不能被 p 整除,等等.