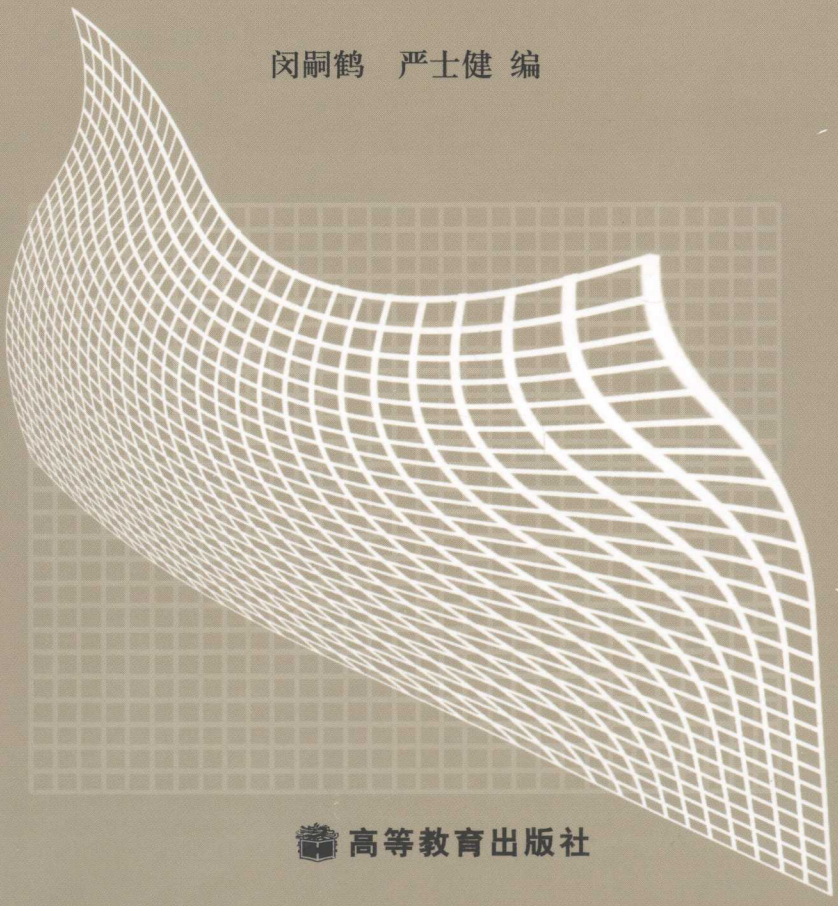
高等学校教材

初等数论

（第三版）

闵嗣鹤　严士健 编



高等教育出版社

高等学校教材

初等数论

（第三版）

闵嗣鹤
严士健 编

高等教育出版社

第三版内容简介

本书第一版系1957年出版，1982年再版。主要内容为整除，不定方程，同余，同余式，平方剩余，原根与指数，连分数，代数数与超越数，数论函数与质数分布。

这次第三版由严士健增补、修订而成，主要是增加了关于20世纪后期费马大定理的获证以及应用数论建立公开密钥体制的介绍，指出整数的初等性质与抽象代数之间的联系。希望帮助读者了解数论的进展，加强对数学统一性的理解。

本书可作为师范院校和综合大学数学系的教材或教学参考书，中学数学教师的参考用书。

图书在版编目(CIP)数据

初等数论/闵嗣鹤，严士健编．—3版．—北京：高等教育出版社，2003.12（2005重印）

ISBN 7-04-011874-2

Ⅰ.初… Ⅱ.①闵…②严… Ⅲ.初等数论-高等学校-教材 Ⅳ.0156.1

中国版本图书馆CIP数据核字(2003)第030699号

出版发行	高等教育出版社	购书热线	010-58581118
社　　址	北京市西城区德外大街4号	免费咨询	800-810-0598
邮政编码	100011	网　　址	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	北京蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	北京机工印刷厂		
		版　　次	1957年11月第1版
开　　本	850×1168　1/32		2003年7月第3版
印　　张	7.25	印　　次	2005年3月第7次印刷
字　　数	180 000	定　　价	11.30元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　11874-00

第三版序

从本书第二版发行以来，经历了21年。在此期间，印行了27次，印数累计达到27万余册。作为一本数论教科书，能够得到如此广泛的使用，作为作者之一，深深感谢广大老师和读者对本书的关爱和支持；同时也深深意识到作为本书作者的责任，如何让它能更好地为社会服务。

20世纪是数学的黄金时代，在数论中最值得向广大读者介绍的是世纪后期的两件大事：费马大定理获得证明和公开密钥体制的建立。

可能费马也未必能想到，它在书边写下的一个结论和他关于这个结论的附注“我对此命题有一个十分美妙的证明，这里的空白太小，写不下”竟成了一个困扰了人类智者358年的谜团——费马大定理，真正是“引无数英雄竞折腰”的难题。三百多年以来，人们百折不回，此路不通又另辟蹊径。终于在世纪末的1994年才由安德鲁·怀尔斯(Andrew Wiles)最后完成证明。费马大定理的证明，既是数学界的盛事，更是人类智慧的象征，是一件具有伟大意义的事件。它的证明过程提供了很多的重要启示。说明一个好的数学难题应该能够对数学——甚至是科学——的发展起推动作用。就像为研究欧几里得第五公设的独立性而发现非欧几何，为研究超过四次的代数方程的根式解而产生伽罗华理论、建立群论一样，费马大定理的证明的前期是发现理想子环——抽象代数的支柱之一的原动力；在20世纪末有力地促进了数论与代数几何结合而形成算术代数几何，证明了志村－谷山－韦依猜想(TSW猜想)而提供了朗兰兹纲领(Langlands programme)成立的一个重要例证。说明数学是统一的，既要搞清楚各个分支以至各个具体问题的结构，同

时要搞清楚各个分支之间的本质联系。说明数学甚至科学的重大成就常常是一种艰巨的接力运动，后人的伟大是“站在巨人的肩膀上”。说明人类的智慧是无限的，产生于艰苦的努力之中。这是我想在这本小书中和读者交流、讨论的认识之一，为此在这一版中增加了费马大定理证明过程的介绍。

数论，作为课程内容常常被认为是介绍一些基础知识，作为研究内容是一大批纯数学的难题，经常被认为与实际应用没有多大关系的学科。有些学者就是由于这个原因而在某个时期转而从事其他分支的教学与研究。但是出乎人们的预料，在20世纪后期，随着计算机技术和信息科学的发展，人类进入了信息时代，科学和技术进入了新的时代，提出了信息安全这样的重大问题。在这种背景下，数论在实际应用的前沿做出了重大的贡献，为解决信息安全问题提供了一种核心技术——公开密钥。这一事实再一次（因为这种情况不止一次地出现）告诉人们，对于基础科学的作用应该有一个正确的认识，它不但在基础方面对科学、技术乃至思维方面起着奠基的作用，而且在技术的发展方面有时能做出突破性贡献。同时也启示我们，学习一门学科虽然不能都要求全面掌握，但是应该对它有全面的了解，做到胸有成竹、能够抓住时机。这一事件对于从事数论学习、研究的人们也是一个巨大的鼓舞。为此我在这一版中介绍了公开密钥的原理、基本方法和资料。

另外，本书的目的是向读者介绍数论本身的基础知识，并增加了一些大纲以外的材料，这些外加材料都独立成节或在习题中出现，特别用星号 * 加以标志。但是读者如果能进一步理解它与数学的其他分支的联系不但能更好地掌握和运用数论的基础知识，而且对于理解其他分支乃至数学都是有益的。以往我们在这方面作过一些努力，如介绍数论函数、三角和的基本概念，这次趁再版的机会，在有关章节建议读者与抽象代数联系并加以考察。

我希望对本书的补充和修改能够保持原书的意图，因为那是闵嗣鹤老师和我共同的意愿。

再一次感谢所有关心、支持此书的教师和读者，感谢高等教育出版社积极推动此书的再版。由于时间和水平所限，不妥和错误之处在所难免，希望老师们和读者继续关心和支持，随时指正，不胜感激。

严士健

2003 年春节于北京师范大学

本次重印，承新疆师范大学数学系王迪吉老师提出一些修改意见，特此致谢。

严士健

2004 年 7 月 21 日

写在再版前面

作为《初等数论》的作者之一，能看到这本书由于社会需要而再版，非常高兴，但是本书的主要构造者，我尊敬的老师闵嗣鹤先生却没有机会看到这次再版，不能对本书亲自作一次中肯的修改，这对我及读者都不能不是一件憾事。

由于本书是闵先生和我合作的结果，而且对当前教学还基本合用，所以这次修订再版，我只改正了书中的一些错误。原来书中提到的一些有关的数论研究课题的发展情况，目的是扩大青年同学的眼界，也介绍一些(远不全面)我国学者的成就。本书出版后，我国学者继续在一些数论问题上取得进展，有关原始文献容易得到。因此我也只在有关地方改动一下提法以尽量减少变动。

根据我自己以及一些老师的教学实践，数学系(特别是师范院校)的本科生在可能情况下学习数论的一些基础内容是有益的。一方面通过这些内容加深对数的性质的了解，更深入地理解某些其他邻近学科；另一方面，也许更重要的是可以加强他们的数学训练，这些训练在很多方面都是有益的。但本书作为每周四学时一学期的课程的教材，内容可能稍多一点。如果真是这样，我认为根据上述要求，第五、七章的后几节及第六章可以全部不讲或者只介绍一些基本概念。

历史上遗留下来没有解决的大多数数论难题有一个共同的特点：问题本身很容易弄懂，容易引起人们的兴趣，要想推进却非常之难。从数论的迄今发展历史来看，数论难题的解决或实质性进展，都用到一些深刻的数学概念、方法和技巧。所以凡是有志于这些问题的青年都应该扎扎实实地学习近代数论的一些方法和技巧，并且十分注意推证和估计能力的训练。这样才有可能在这些

难题上作些贡献，否则会劳而无功。另外有意义的数学研究课题（包括现代数学发展中提出的一些数论问题）还是很多的，祖国“四化”事业需要各方面的人才，有志于数学研究的青年不一定都去攻这些经典的数论难题。当然无论进行哪个方向的研究，坚实的理论基础和良好的解决问题的能力都是绝对需要的。

本书出版以来，很多同志热心地指出其中一些错误并提出一些宝贵意见。这次再版之前，承蒙闵先生的夫人朱敬一先生及其长子闵乐泉同志仔细阅读全书，提出很多宝贵意见。潘承彪同志详细地审阅了全书，提出了很多中肯的修改意见。这一切都对提高书的质量有极大的帮助。借此机会致以深深的谢意，并热诚欢迎大家给本书提出批评指正。

严士健

1982 年 1 月于北京师范大学

第一版序

在师范大学与师范学院的数学系都有整数论这一门课，它的试行教学大纲也由教育部在1955年制订并颁布执行了。但是由于没有一本适当的教本或参考书，担任这一课程的教师在选择教材与指定参考书方面都一直感到一定的困难。我和严士健同志先后在师范大学讲授整数论这一门课。最初，大纲还未制订，我只好采用И.М.Виноградов著的（裘光明同志翻译）数论基础为主要参考书，同时根据苏联的教学大纲，作了必要的补充。由于没有适当的教本，我曾计划编写讲义，但受时间的限制，那时只写了一些补充材料，而大部还是依照数论基础这本书来讲授。严士健同志在接着担任这门课程的期间加以整理写成一本完整的讲义。最后经过教育部的督促由我们依照师范学院整数论试行教学大纲，再加以修改补充合写成这本书。

作为一个好的教本，我以为要具有三个条件。第一是教材要选择得恰当，安排得自然。第二是说理要严格而清楚，深入而浅出，也就是逻辑性与直观性都要强。第三是要引人入胜，使人有“欲穷千里目，更上一层楼”之感，换句话说，问题的来源与发展都要交代清楚，使读者能从少许见多许，增加他们目前学习与今后钻研的兴趣。如果执此以绳眼前的这本书，我想会发现很多缺点的。不过，严士健同志和我自己，结合几年来的教学经验，在写作中还是朝着这个方向而努力的。虽然我们做得很不够，也希望采用这本书的教师能结合自己的经验与特长，随时弥补。

这本书虽然主要是依照师范学院的整数论教学大纲而写成的，但同时也照顾到综合大学数论这一课程的需要，增加了一些大纲以外的材料。这些外加的材料都独立成节，特别用星号*加以

标志。在写作中,我们还参考了华罗庚先生的数论导引,特在此致谢。本书对于我国古代与当今数学家在数论方面的成就以及前苏联和其他国家的数学家的贡献也尽可能作了一定程度的介绍,不够全面之处,还希望读者原谅。最后,希望读者,尤其是全国各师范学院采用这本书的老师们能对本书多提意见,以便将来能够根据这些意见把它修改成更合乎理想,更合乎教学需要的一本书。

闵嗣鹤

1956 年 10 月于北京大学

目　录

第一章　整数的可除性

整除是数论中的基本概念，本章从这个概念出发，引进带余数除法及辗转相除法，然后利用这两个工具，建立最大公因数与最小公倍数的理论，进一步证明极具重要性的算术基本定理．这一切都是整个课程中最基本的部分，以后时常要用到．同时，它们也是整个数学的基础知识，大部分都是读者在小学甚至在幼儿园时就开始学习的．由于当时考虑到儿童的理解力，着重点是具体数字的计算和运用．因此对绝大多数读者来说，可能计算技能是熟练的，对计算方法和概念未必能从一般的角度来掌握，从而对它们的本质未必理解．因此在大学甚至高中阶段，重新学习和体会是大有裨益的．此外，本章还要介绍$[x]$，$\{x\}$这两个极有用的记号，并利用$[x]$来说明如何把$n!$表示成质数幂的乘积．

§1　整除的概念·带余数除法

我们知道两个整数的和、差、积仍然是整数，但是用一不等于零的整数去除另一个整数所得的商却不一定是整数，因此我们引进整除的概念：

定义　设a，b是任意两个整数，其中$b\neq 0$，如果存在一个整数q使得等式

$$a = bq \tag{1}$$

成立，我们就说b整除a或a被b**整除**，记作$b\mid a$，此时我们把b叫作a的**因数**，把a叫作b的**倍数**．

如果(1)里的整数q不存在，我们就说b**不能整除**a或a不被b整除，记作$b\nmid a$．

小练：① $b\mid 0$　[证明：$0=b\cdot 0$]
② $1\mid a$　$a=1\cdot a \Rightarrow a\mid a.\ (a\neq 0)!$
③ $b\mid a \Rightarrow b\mid |a|$.　[证明：$b\mid a \Rightarrow a=bq$　$b>0$ 时 $|a|=b|q|$]　← 自己证.

整除这个概念虽然简单，但却是数论中的基本概念，我们很容易从定义出发，证明下面那些关于可除性的基本定理.

定理 1(传递性) 若 a 是 b 的倍数，b 是 c 的倍数，则 a 是 c 的倍数，也就是①

$$b \mid a, c \mid b \Rightarrow c \mid a.$$

证 $b \mid a, c \mid b$ 就是说存在两个整数 a_1, b_1 使得

$$a = a_1 b, b = b_1 c$$

成立，因此

$$a = (a_1 b_1) c,$$

但 $a_1 b_1$ 是一个整数，故 $c \mid a$. **证完**

定理 2 若 a, b 都是 m 的倍数，则 $a \pm b$ 也是 m 的倍数.

证 a, b 是 m 的倍数的意义就是存在两个整数 a_1, b_1，使得

$$a = a_1 m, b = b_1 m.$$

因此

$$a \pm b = (a_1 \pm b_1) m,$$

但 $a_1 \pm b_1$ 是整数，故 $a \pm b$ 是 m 的倍数. **证完**

用同样的方法，可以证明

定理 3 若 $a_1, a_2, \cdots, a_n$ 都是 m 的倍数，$q_1, q_2, \cdots, q_n$ 是任意 n 个整数，则 $q_1 a_1 + q_2 a_2 + \cdots + q_n a_n$ 是 m 的倍数.(证明留给读者.)

上面我们仅就能够整除的情形初步地讨论了一下，至于在一般(即未必能整除的)情形下，我们有下面基本而重要的定理.

定理 4(带余数除法) 若 a, b 是两个整数，其中 $b > 0$，则存在着两个整数 q 及 r，使得

$$a = bq + r, 0 \leqslant r < b \tag{2}$$

成立，而且 q 及 r 是惟一的.

---

① 我们用 $A \Rightarrow B$ 表示由命题 A 可以推出命题 B.

证 作整数序列

$$\cdots,-3b,-2b,-b,0,b,2b,3b,\cdots$$

则 a 必在上述序列的某两项之间，即**存在**一个整数 q 使得

$$qb\leqslant a<(q+1)b$$

成立. 令 $a-qb=r$，则 $a=bq+r$，而 $0\leqslant r<b$.

下面我们证明 q,r 的惟一性：设 q_1,r_1 是满足(2)的两个整数，则

$$a=bq_1+r_1,0\leqslant r_1<b,$$

因而 $$bq_1+r_1=bq+r,$$

于是 $$b(q-q_1)=r_1-r,$$

故 $$b|q-q_1|=|r_1-r|.$$

由于 r 及 r_1 都是小于 b 的正数，所以上式右边是小于 b 的. 如果 $q\neq q_1$ 则上式左边$\geqslant b$. 这是不可能的. 因此 $q=q_1$ 而 $r=r_1$. **证完**

整数的很多基本性质，都可以从定理 4 引导出来. 我们可以说这一章最主要的部分是建立在定理 4 的基础上的.

定义 (2)中的 q 叫做 a 被 b 除所得的**不完全商**，r 叫作 a 被 b 除所得到的**余数**.

为了更好地了解这个定义，我们举例说明如下：

例 设 $b=15$，则当 $a=255$ 时

$$a=17b+0,r=0<15,\text{而 } q=17;$$

当 $a=417$ 时，

$$a=27b+12,0<r=12<15,\text{而 } q=27;$$

当 $a=-81$ 时，

$$a=-6b+9,0<r=9<15,\text{而 } q=-6.$$

习 题

1. 证明定理 3.

2. 证明 $3 \mid n(n+1)(2n+1)$，其中 n 是任何整数.

3. 若 ax_0+by_0 是形如 $ax+by$（x,y 是任意整数，a,b 是两个不全为零的整数）的数中的最小正数，则

$$(ax_0+by_0) \mid (ax+by),$$

其中 x,y 是任何整数.

4. 若 a,b 是任意二整数，且 $b \neq 0$，证明：存在两个整数 s,t 使得

$$a=bs+t, |t| \leqslant \frac{|b|}{2}$$

成立，并且当 b 是奇数时，s,t 是惟一存在的. 当 b 是偶数时结果如何？

§2 最大公因数与辗转相除法

有了带余数除法，我们就可以着手研究整数的最大公因数的存在问题及其实际求法，在研究过程中，我们要用到基本而重要的辗转相除法.

定义 设 $a_1,a_2,\cdots,a_n$ 是 $n(n \geqslant 2)$ 个整数. 若整数 d 是它们之中每一个的因数，那么 d 就叫作 $a_1,a_2,\cdots,a_n$ 的一个**公因数**.

整数 $a_1,a_2,\cdots,a_n$ 的公因数中最大的一个叫作**最大公因数**，记作 $(a_1,a_2,\cdots,a_n)$，若 $(a_1,a_2,\cdots,a_n)=1$，我们说 $a_1,a_2,\cdots,a_n$ **互质或互素**，若 $a_1,a_2,\cdots,a_n$ 中每两个整数互质，我们就说它们**两两互质**.

显然，若整数 $a_1,a_2,\cdots,a_n$ 两两互质，则 $(a_1,a_2,\cdots,a_n)=1$，反过来却不一定成立（很容易举出反例），且若 $a_1,a_2,\cdots,a_n$ 不全为零，则 $(a_1,a_2,\cdots,a_n)$ 是存在的.

为了讨论时免去区别正负整数的麻烦，我们先证明

定理 1 若 $a_1,a_2,\cdots,a_n$ 是任意 n 个不全为零的整数，则

(i) $a_1,a_2,\cdots,a_n$ 与 $|a_1|,|a_2|,\cdots,|a_n|$ 的公因数相同；

(ii) $(a_1,a_2,\cdots,a_n)=(|a_1|,|a_2|,\cdots,|a_n|)$.

证 设 d 是 $a_1,a_2,\cdots,a_n$ 的任一公因数. 由定义 $d \mid a_i, i=1,$

$2,\cdots,n$，因而 $d\mid|a_i|$，$i=1,2,\cdots,n$，故 d 是 $|a_1|,|a_2|,\cdots,|a_n|$ 的一个公因数，同法可证，$|a_1|,|a_2|,\cdots,|a_n|$ 的任一个公因数都是 $a_1,a_2,\cdots,a_n$ 的一个公因数．故 $a_1,a_2,\cdots,a_n$ 与 $|a_1|,|a_2|,\cdots,|a_n|$ 有相同的公因数，即(i)获证．由(i)立得(ii)． 证完

定理 1 的(ii)告诉我们，要讨论最大公因数不妨仅就非负整数去讨论，下面我们首先看两个非负整数的情形．

定理 2 若 b 是任一正整数，则(i)0 与 b 的公因数就是 b 的因数，反之，b 的因数也就是 0 与 b 的公因数．(ii)$(0,b)=b$．

证 显然 0 与 b 的公因数是 b 的因数．由于任何非零整数都是 0 的因数，故 b 的因数也就是 0，b 的公因数，于是(i)获证．其次，我们立刻知道 b 的最大因数是 b；而 0，b 的最大公因数是 b 的最大因数，故 $(0,b)=b$． 证完

由定理 1,2 立刻得到①

推论 2.1 若 b 是任一非零整数，则 $(0,b)=|b|$．

定理 3 设 a,b,c 是任意三个不全为 0 的整数，且

$$a=bq+c,$$

其中 q 是非零整数，则 a,b 与 b,c 有相同的公因数，因而 $(a,b)=(b,c)$．

证 设 d 是 a,b 的任一公因数，由定义，$d\mid a,d\mid b$．由 §1 定理 3，d 是 $c=a+(-q)b$ 的因数，因而 d 是 b,c 的一个公因数．同法可证，b,c 的任一公因数是 a,b 的一个公因数．于是定理的前一部分获证．第二部分显然随之成立． 证完

现在我们介绍一下辗转相除法．它有很多应用：可用以求出两个正整数的最大公因数；借此推出最大公因数的重要性质；还是解一次不定方程的基本工具．

设 a,b 是任意两个正整数，由带余数除法，我们有下面的系

① 我们用推论 2.1 表示定理 2 的推论 1.