高等学校教学参考书

初等数论

（第二版）

闵嗣鹤 严士健编

高等教育出版社

高等学校教学参考书

初等数论

（第二版）

闵嗣鹤
严士健 编

高等教育出版社

本书第一版是1957年出版的，这次再版由严士健同志作了一些小的修改，主要是订正错误。

本书主要内容为整除，不定方程，同余，同余式，平方剩余，原根与指标，连分数，代数数与超越数，数论函数与质数分布。

本书可作为师范院校数学系的教学用书，及综合大学数学系的参考书。

图书在版编目(CIP)数据

初等数论/闵嗣鹤，严士健编 .—2版 .—北京：高等教育出版社，1982.9(2003重印)

ISBN 7-04-001259-6

Ⅰ.初… Ⅱ.①闵… ②严… Ⅲ.初等数论 Ⅳ.0156.1

中国版本图书馆CIP数据核字(97)第27595号

初等数论(第二版)

闵嗣鹤 严士健 编

出版发行	高等教育出版社	**购书热线**	010－64054588
社　　址	北京市东城区沙滩后街55号	**免费咨询**	800－810－0598
邮政编码	100009	**网　　址**	http://www.hep.edu.cn
传　　真	010－64014048		http://www.hep.com.cn
经　　销	新华书店北京发行所		
印　　刷	中国青年出版社印刷厂		
		版　　次	1957年11月第1版
开　　本	850×1168　1/32		1982年9月第2版
印　　张	6.5	**印　　次**	2003年5月第29次印刷
字　　数	152 000	**定　　价**	8.60元

凡购买高等教育出版社图书，如有缺页、倒页、脱页等质量问题，请在所购图书销售部门联系调换 .

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.第一是教材要选择的恰当，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.虽然我们做的很不够，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. 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$b\nmid a$.

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　若a是b的倍数，b是c的倍数，则a是c的倍数，也就是①

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

$$b|a, c|b \Longrightarrow c|a.$$

证 $b|a, c|b$ 就是说存在两个整数 b_1, a_1 使得

$$a=a_1b, b=b_1c$$

成立，因此

$$a=(a_1b_1)c.$$

但 a_1b_1 是一个整数，故 $c|a$. **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

$$a=a_1m, b=b_1m.$$

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 $q_1a_1+q_2a_2+\cdots+q_na_n$ 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，至于在一般情形下，我们有下面很重要的

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 是唯一的.

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 $0\leqslant r<b$.

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，我们举例说明一下：

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 $3|n(n+1)(2n+1)$，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

$$(ax_0+by_0)|(ax+by),$$

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 是单数时，s,t 是唯一存在的. 当 b 是双数时结果如何？

*5. 证明 $1+\frac{1}{2}+\cdots+\frac{1}{n}(n>1)$ 及 $\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{2n+1}(n\geqslant 1)$ 都不是整数.

§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，我们要用到所谓辗转相除法.

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，那末 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，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 $d|a_i,i=1,2,\cdots,n$，因而 $d||a_i|,i=1,2,\cdots,n$，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：$d|a,d|b$，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，这个辗转相除法不仅可用以求出两个正整数的最大公因数，并且可借此推出最大公因数的重要性质.

设 a,b 是任意两个正整数，由带余数除法，我们有下列等式：

$$\begin{aligned}
&a=bq_1+r_1, \quad 0<r_1<b,\\
&b=r_1q_2+r_2, \quad 0<r_2<r_1,\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
&r_{n-2}=r_{n-1}q_n+r_n, \quad 0<r_n<r_{n-1},\\
&r_{n-1}=r_nq_{n+1}+r_{n+1}, \quad r_{n+1}=0.
\end{aligned} \tag{1}$$

因为每进行一次带余数除法，余数就至少减一，而 b 是有限的，所

① 我们用推论 2.1 表示定理 2 的推论 1.

以我们最多进行 b 次(事实上不到 b 次)带余数除法,总可以得到一个余数是零的等式,即 $r_{n+1}=0$. (1)式所指出的计算方法,叫作辗转相除法. 这计算法是我国古代数学家所创造的,这就是中国古代算学书中的求一术(以后还要作较详细的介绍),但在外文书籍里,常把它叫做欧基里得除法. 现在我们证明

定理 4 若 a,b 是任意两个整数,则 (a,b) 就是(1)中最后一个不等于零的余数,即 $(a,b)=r_n$.

证 由定理 2,3 即得

$$r_n=(0,r_n)=(r_{n+1},r_n)=(r_n,r_{n-1})=\cdots=(r_1,b)=(a,b).$$

证完

由定理 2,3 及(1)我们还可以得到

推论 4.1 a,b 的公因数与 (a,b) 的因数相同(证明留给读者).

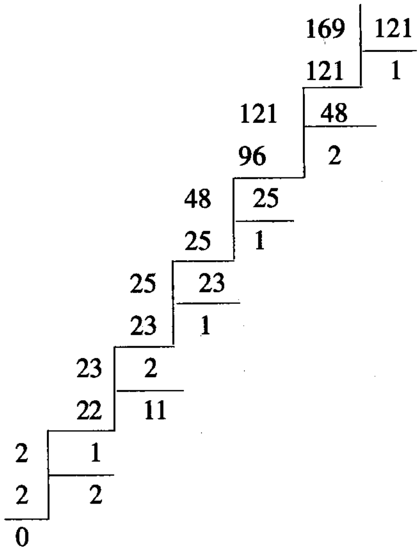
由以上的讨论,我们可以看到,若 a,b 两整数中有一为零,而另一数不为零时,则 (a,b) 为不等于零的数的绝对值,若 a,b 两数都不是零时,则 a,b 最大公因数可以由(1)实际地算出来.

我们看两个例子:

例 1 $a=-1859,b=1573$,由定理 1,$(-1859,1573)=(1859,1573)$.

$$\begin{array}{r|l|l|l}
|a| = 1859 & 1573 = b & 1 = q_1 & 1859 = 1\times 1573 + 286 \\
1573 & 286 = r_1 & 5 = q_2 & 1573 = 5\times 286 + 143 \\
1573 & 286 = r_1 & 2 = q_3 & 286 = 2\times 143 \\
1430 & 5 = q_2 & & \text{所以}(-1859,1573) = 143. \\
286 & 143 = r_2 & & \\
286 & 2 = q_3 & & \\
0 = r_3 & & &
\end{array}$$

例 2 $a=169,b=121$



$169 = 1 \times 121 + 48$

$121 = 2 \times 48 + 25$

$48 = 1 \times 25 + 23$

$25 = 1 \times 23 + 2$

$23 = 11 \times 2 + 1$

$2 = 2 \times 1$

所以$(169,121) = 1$.

我们再证明两个最大公因数的性质,即

定理 5 设a,b是任意两个不全为零的整数,(i)若m是任一正整数,则

$$(am,bm)=(a,b)m.$$

(ii)若δ是a,b的任一公因数,则$\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{|\delta|}$,因而$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$.

证 当a,b有一为零时,定理显然成立,今设a,b都不是零.

(i) 由定理 1,$(am,bm)=(|a|m,|b|m)$,$(a,b)m=(|a|,|b|)m$. 因此不妨假定a,b都是正数. 在(1)里,把各式两边同乘以m,即得

$$am=(bm)q_1+r_1m,0<r_1m<bm,$$

$$bm=(r_1m)q_2+r_2m,0<r_2m<r_1m,$$

$$\cdots\cdots$$

$$r_{n-1}m=(r_nm)q_{n+1}.$$

由定理 4 得$(am,bm)=r_nm=(a,b)m$，因而(i)获证.

(ii) 由(i)及定理 1，

$$\left(\frac{a}{\delta},\frac{b}{\delta}\right)|\delta|=\left(\frac{|a|}{|\delta|}|\delta|,\frac{|b|}{|\delta|}|\delta|\right)=(|a|,|b|)=(a,b),$$

故
$$\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{|\delta|}.$$

当$\delta=(a,b)$时，上式即为$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$. **证完**

现在来研究两个以上整数的最大公因数. 由定理 1 及 2 我们不妨假设$a_1,a_2,\cdots,a_n$是任意 n 个正整数. 令

$$(a_1a_2)=d_2,(d_2,d_3)=d_3,\cdots,(d_{n-1},a_n)=d_n. \tag{2}$$

于是我们有

定理 6 若$a_1,a_2,\cdots,a_n$是 n 个整数，则$(a_1,a_2,\cdots,a_n)=d_n$.

证 由(2)，$d_n\mid a_n$，$d_n\mid d_{n-1}$. 但 $d_{n-1}\mid a_{n-1}$，$d_{n-1}\mid d_{n-2}$，故$d_n\mid a_{n-1}$，$d_n\mid d_{n-2}$. 由此类推，最后得到$d_n\mid a_n$，$d_n\mid a_{n-1}$，$\cdots$，$d_n\mid a_1$，即d_n是$a_1,a_2,\cdots,a_n$的一个公因数. 又设 d 是$a_1,a_2,\cdots,a_n$的任一公因数，则$d\mid a_1$，$d\mid a_2$，由推论 4.1，$d\mid d_2$，同样由推论 4.1，$d\mid d_3$，由此类推，最后得 $d\mid d_n$. 因而$d\leqslant|d|\leqslant d_n$. 故$d_n$是$a_1,a_2,\cdots,a_n$的最大公因数. **证完**

习　题

1. 证明推论 4.1.

2. 应用 §1 习题 3 证明$(a,b)=ax_0+by_0$，其中ax_0+by_0是形如$ax+by$(x,y是任意整数)的整数里的最小正数，并将此结果推广到 n 个整数的情形.

3. 应用 §1 习题 4 证明任意两整数的最大公因数存在，并说明其求法. 试用你所说的求法及辗转相除法实际算出(76501,9719).

*4. 证明本节(1)式中的$n\leqslant\frac{2\log b}{\log 2}$.