教育部人才培养模式改革和开放教育试点教材
数学与应用数学专业系列教材

初等数论

主编 南基洙

中央广播电视大學出版社

教育部人才培养模式改革和开放教育试点教材
数学与应用数学专业系列教材

初等数论

主编　南基洙

图书在版编目（CIP）数据

初等数论/南基洙主编．－北京：中央广播电视大学出版社，2002.6

教育部人才培养模式改革和开放教育试点教材

数学与应用数学专业系列教材

ISBN 7－304－02246－9

Ⅰ.初… Ⅱ.南… Ⅲ.初等数论－高等学校－教材

Ⅳ.O158.1

中国版本图书馆 CIP 数据核字(2002)第 040150 号

教育部人才培养模式改革和开放教育试点教材

数学与应用数学专业系列教材

初等数论

主编　南基洙

出版·发行/中央广播电视大学出版社

经销/新华书店北京发行所

印刷/北京云浩印刷有限责任公司

开本/850×1168　1/32　**印张**/4.125　**字数**/98 千字

版本/2002 年 5 月第 1 版　2003 年 8 月第 2 次印刷

印数/2001～7000

社址/北京市复兴门内大街 160 号　**邮编**/100031

电话/66419791　68519502　**(本书如有缺页或倒装，本社负责退换)**

书号：ISBN 7－304－02246－9/O·118

定价：8.00 元

序　言

21世纪，中国全面进入了一个新的发展与竞争的年代.归根结底，竞争是人才和知识的竞争.团体竞争的优胜者将是那些具有一批高水平人才的团体；个体竞争的优胜者将是那些具有现代科学知识与超群工作能力的人.在这竞争的时代，青年人渴望学习到适应工作岗位需要的知识.正是在这种环境下，中央广播电视大学与东北师范大学为满足一大批中学数学教师的要求，联合开办了(师范类)本科数学与应用数学专业.

本专业的开办，为追求知识的中学青年教师开辟了一条前进的道路，而知识的获取，要靠学习者的辛勤劳动.可以说，学习是一项艰苦的劳动.这项劳动与其他劳动的一个显著区别是：学习不能由别人代替来完成，甚至也不能合作完成.特别是数学知识的学习，必须经过学习者一番夜不能寐的(有时甚至是痛苦的)冥思苦想，才能掌握数学的本质，才能体会到数学的真谛，才能达到由此及彼、由表及里的境界.

数学是众多学科中最为抽象的学科.它高度的抽象性，决定了它广泛的应用性，同时也造成了数学学习的困难.毋庸讳言，相对其他学科来说，学习数学需要花费更多的时间与精力.但是，数学并不是高不可攀的科学.数学的学习如同攀登高楼一样，只要一步一个台阶(而不是两个台阶，三个台阶…，更不是飞跃)地拾级而上，我们并不觉得太困难即可攀上高楼.同样，只要学习者扎扎实实地掌握这一步知识，再去学习下一步的内容，循序渐进，数学就

可以成为任你的思维纵横驰骋的自由王国.

作为教师,要充分地考虑到学生在自学过程中遇到的各种困难.我们在教材的编写中,尽最大可能地使教材通俗易懂,深入浅出.为了便于自学,我们适当地做出一些注释,引导学生深入理解知识.在每章的开始,给出本章学习目标和导学;每章的结尾,做出本章的总结,指出本章的重点及难点,并安排了学习辅导内容,介绍典型例题,同时配备了自测题目.

中央广播电视大学与东北师范大学联合开办本科数学与应用数学专业处于刚刚起步阶段.我们的教师首次编写这套教材,一切尚处于探索的过程中.因此,这套教材难免有这样或那样的不妥之处.我们热情地欢迎读者提出宝贵的批评意见和改进的建议,使我们的教师及时改进这套教材,以不断提高学生的学习效果.

史宁中

2002 年 4 月 25 日

前　言

初等数论也称整数论，主要研究整数的性质和方程的整数解，是数学基础理论的一个非常重要的分支．由于初等数论中的问题简明易懂，所以它比任何其它的数学分支更能引起人们的注意．近代数学中许多重要的思想、概念、方法和技巧都是从对整数性质的深入研究而不断丰富和发展起来的．

在数论问题的许多研究方面，我国都处于领先地位，如老一辈著名数学家华罗庚、柯召、闵嗣鹤等都取得过辉煌的成就，特别是华罗庚教授在解析数论方面的成果是举世公认的．20 世纪 60 年代后，著名数学家陈景润、王元、潘承洞等在哥德巴赫(Goldbach)猜想等问题上也取得了国际领先的成果．

本书取材我们遵循少而精的原则，力求叙述简明、说理详尽．全书共分 5 章，分别介绍了整除理论、不定方程、同余理论和连分数．每章配备了少量的习题，以供读者巩固学过的理论和熟练计算之用．这些内容都是初等数论中一些最基本的理论，是学习数论必需掌握的．书中加“＊”的章节供学有余力的学生阅读．

在此，我们感谢吉林大学的牛凤文教授、廖公夫教授，首都师范大学的石生明教授、卢才辉教授、周春荔教授，东北师范大学的王仁发教授对编写本书提出了建议．

本书的主要内容由南基洙同志编写．李林曙、马连荣、张旭红、潘焦萍等同志参加了学习指导和各章习题的选配工作．由于水平有限，书中难免存在不少缺点和错误，希望读者斧正．

目　录

第 1 章　整数的整除性理论

整除是初等数论中的基本概念，在此我们先引进剩余定理，然后以此为工具建立我们所需的其它概念、性质和方法. 如果没有特别的强调，在本章中涉及的整数均为非零的整数.

1.1　整除性、公因数、公倍数

我们知道，整数的和、差、积是整数，但是整数的商却不一定是整数，如 $1\div 2$. 而在初等数论中，我们要研究的是整数的性质，为此我们引进整除的概念.

定义　设 a,b 是两个整数，其中 $b\neq 0$，如果存在一个整数 q 使得

$$a=bq$$

则我们称 b 整除 a 或者 a 被 b 整除，记为 $b\mid a$，此时 b 叫做 a 的因数，a 叫做 b 的倍数. 如果满足等式的整数 q 不存在，则称 b 不能整除 a 或者 a 不被 b 整除，记为 $b\nmid a$.

由整除的定义及乘法的运算性质，容易得到整除关系的性质：

定理 1.1　设 a,b,c 是整数，则

(1)如果 a 是 b 的倍数，b 是 c 的倍数，则 a 是 c 的倍数，即 $b\mid a, c\mid b\Rightarrow c\mid a$；

(2)如果 a,b 是 c 的倍数，则 $a\pm b$ 是 c 的倍数；

(3)如果 $b\mid a, a\mid b$，则 $a=\pm b$；

(4)设 $m\neq0$, a 是 b 的倍数,则 am 是 bm 的倍数.

证明 (1)因为 $b|a$, $c|b$,所以

$$a=bm, b=cn,\text{其中 } m, n \text{ 是整数}.$$

因此,我们有 $a=c(nm)$,即 $c|a$;

(2)因为 a, b 是 c 的倍数,所以

$$a=cm, b=cn,\text{其中 } m, n \text{ 是整数}.$$

从而,有 $a\pm b=c(m\pm n)$,即 $a\pm b$ 是 c 的倍数;

(3)因为 $b|a$, $a|b$,所以

$$a=bm, b=an,\text{其中 } m, n \text{ 是整数}.$$

因此, $a=a(nm)$, $nm=1$.所以 $n=\pm1$, $m=\pm1$,即 $a=\pm b$.

(4)因为 a 是 b 的倍数,所以

$$a=bq,\text{其中 } q \text{ 是整数}.$$

因此, $am=(bm)q$,即 am 是 bm 的倍数.

例 1 设 a, b 是两个给定的整数,并且存在整数 x, y 使 $ax+by=1$,如果再有 $a|n$, $b|n$,则 $ab|n$.

证明 因为 $n=n\times1=n(ax+by)=(na)x+(nb)y$,又由于 $a|n$, $b|n$,得到 $ab|nb$, $ab|an$,所以 $ab|n$.

例 2 如果 $3|n$, $5|n$,则 $15|n$.

证明 因为 $3\times2+5\times(-1)=1$,所以由例 1 知道 $15|n$.

定理 1.2(剩余定理) 如果 a, b 是两个整数, $b>0$,则存在惟一的整数对 q, r,使得

$$a=bq+r, 0\leqslant r<b.$$

证明 首先证明惟一性.设 q', r',是满足条件的另外整数对,即

$$a=bq'+r', 0\leqslant r'<b.$$

所以 $bq'+r'=bq+r$,即 $b(q'-q)=r-r'$, $b|q'-q|=|r-r'|$.

又由于 $0\leqslant r<b$, $0\leqslant r'<b$,所以 $|r-r'|<b$.如果 $q\neq q'$,则等式

$b|q'-q|=|r-r'|$不可能成立.因此 $q=q',r=r'$.

其次证明存在性.我们考虑整数的有序列

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

则整数 a 应介于上面有序列的某两数之间,即存在一整数 q 使

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

我们设 $r=a-qb$,则有 $a=bq+r,0\leqslant r<b$.

剩余定理中的 q 称为 a 被 b 除所得的不完全商,r 称为 a 被 b 除所得到的余数.

有了剩余定理,我们就可以考虑整数的公因子(最大公因子)的存在性及其求法.

定义 设 a,b 是两个整数.如果存在整数 d,使得 $d|a,d|b$,那么称 d 为 a,b 的公因子(公因数).一般地,设 $a_i(1\leqslant i\leqslant k)$ 是 k 个整数.如果 $d|a_i(1\leqslant i\leqslant k)$,那么称 d 为 $a_i(1\leqslant i\leqslant k)$ 公因子(公因数).

例如设 $a=12,b=18$.它们的公因子是 $\pm1,\pm2,\pm3,\pm6$.它们的公因子的个数有限.为此我们引进

定义 设 $a_i(1\leqslant i\leqslant k)$ 是 k 个整数.我们称 $a_i(1\leqslant i\leqslant k)$ 的公因子中的最大数为最大公因子,记为 $(a_1,\cdots,a_k)$.特别地,如果 $(a_1,\cdots,a_k)=1$,我们就称 k 个整数 $a_i(1\leqslant i\leqslant k)$ 互素(互质).

例如 $(12,18)=6,(3,5)=1$.

显然,如果整数 $a_i(1\leqslant i\leqslant k)$ 两两互素,则 $(a_1,\cdots,a_k)=1$,反之不然.请读者自己举一反例.

我们为免去讨论正负数的麻烦,先证明以下定理:

定理 1.3 设 $a_i(1\leqslant i\leqslant k)$ 是 k 个整数,则 $a_i(1\leqslant i\leqslant k)$ 的公因子与 $|a_i|(1\leqslant i\leqslant k)$ 的公因子相同.特别地,$(a_1,\cdots,a_k)=(|a_1|,\cdots,|a_k|)$.

证明 设 d 是 $a_i(1\leqslant i\leqslant k)$ 的公因子.由定义 $d|a_i(1\leqslant i\leqslant k)$,所以 $d||a_i|(1\leqslant i\leqslant k)$,即 d 是 $|a_i|(1\leqslant i\leqslant k)$ 的公因子.反之

亦然.当然,由此有$(a_1,\cdots,a_k)=(|a_1|,\cdots,|a_k|)$.

定理 1.4 $(0,b)=|b|$.

定理 1.5 设 a,b,c 是三个非零整数,且

$$a=bq+c,$$

其中 q 整数,则 a,b 与 b,c 有相同的公因子.特别地,$(a,b)=(b,c)$.

证明 设 d 是 a,b 的公因子,则 $d|a,d|b$.所以 $d|a-bq$,即 $d|c$.因而 d 是 b,c 的公因子.反之亦然.于是 $(a,b)=(b,c)$ 随之成立.

至此,我们可以给出求最大公因子的辗转相除法.设 a,b 是两个整数,由剩余定理我们有下面的等式组

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

因为每运用一次剩余定理,余数就至少减少 1,而整数 b 是有限的,所以我们在有限步之内能够得到上面的等式组.也就是说,

$$\begin{aligned}
(a,b)&=(b,r_1)=(r_1,r_2)=\cdots=(r_{n-2},r_{n-1})\\
&=(r_{n-1},r_n)=(r_n,0)=r_n.
\end{aligned}$$

例 3 令 $a=-1\ 859,b=1\ 573$,求 $(a,b)=?$

解 因为我们有 $1\ 859=1\times1\ 573+286$

$$1\ 573=5\times286+143$$

$$286=2\times143$$

所以 $$(a,b)=(-1\ 859,1\ 573)=143.$$

例 4 求525与231的最大公因子.

解　因为我们有 $525=2\times231+63$

$$231=3\times63+42$$

$$63=1\times42+21$$

$$42=2\times21$$

所以　　$(525,231)=21$.

由辗转相除法，我们还得到关于最大公因子的一些基本性质.

定理 1.6　$(a,b)c=(ac,bc),c>0$.

事实上，用 c 乘以等式组(1)的各式即可.

例如 $(12,-18)=(2,-3)\times6=6$.

定理 1.7　设 $(a,b)=1$，那么 $(ac,b)=(c,b)$.

证明　因为 $(ac,b)\mid ac,(ac,b)\mid bc$，所以 $(ac,b)\mid(ac,bc)=(a,b)c=c$.

再因为 $(ac,b)\mid b$，所以 $(ac,b)\mid(c,b)$. 又 $(c,b)\mid ac,(c,b)\mid b$，所以 $(c,b)\mid(ac,b)$，于是 $(ac,b)=(c,b)$.

例如 $(300,-18)=(12\times25,-18)=(12,-18)=6$.

由上面的几个定理我们容易得到几个常用的结果：

当 $b\mid ac$ 时，如果 $(a,b)=1$，则有 $b\mid c$. 这是因为 $(ac,b)=b$，$(ac,b)=(c,b)$，所以 $(c,b)=b$，因此 $b\mid c$.

当 $a\mid c,b\mid c$ 时，如果 $(a,b)=1$，则有 $ab\mid c$. 这是因为从 $a\mid c$ 有 $c=ac_1$，所以 $b\mid c_1$，于是 $ab\mid ac_1$，即 $ab\mid c$.

当 $(a,c)=1,(b,c)=1$ 时，有 $(ab,c)=1$. 这是因为 $(ab,c)=(b,c)=1$.

再如果 $(a,b)=1$，那么 $(ab,a+b)=1$. 这是因为 $(a,a+b)=1,(b,a+b)=1$

定理 1.8　设 $c(>0)$ 是整数 a,b 的公因子，则

$$\left(\frac{a}{c},\frac{b}{c}\right)=\frac{(a,b)}{c}.$$

证明 $\left(\frac{a}{c},\frac{b}{c}\right)c=\left(\frac{a}{c}\cdot c,\frac{b}{c}\cdot c\right)=(a,b)$.

特别地,假如 $c=(a,b)=d$,那么 $\left(\frac{a}{d},\frac{b}{d}\right)=1$. 反之,如果 $\left(\frac{a}{c},\frac{b}{c}\right)=1$,那么 $c=(a,b)$. 即有

推论 1.9 假定 $c>0$,那么 $\left(\frac{a}{c},\frac{b}{c}\right)=1$ 的充分必要条件是 $c=(a,b)$.

如果我们反推辗转相除法(见式(1)),即如果 a,b 是两个正整数,则我们有

$$Q_k a-P_k b=(-1)^{k-1}r_k,\ k=1,2,\cdots,n, \quad . \tag{2}$$

其中 $P_0=1,P_1=q_1,P_k=q_kP_{k-1}+P_{k-2}$;

$Q_0=0,Q_1=1,Q_k=q_kQ_{k-1}+Q_{k-2},k=2,\cdots,n$.

所以,我们容易得到:

定理 1.10 设 $(a,b)=d$,则存在整数 x,y 使得 $ax+by=d$.

例 5 对525与231求满足定理1.10条件的 x,y.

解 因为 $21=63-1\times42=63-1\times(231-3\times63)$

$=4\times63-1\times231=4\times(525-2\times231)-1\times231$

$=4\times525-9\times231$,

即 $525\times4+231(-9)=21,x=4,y=-9$.

现在来考虑两个以上整数的最大公因子. 由定理 1.3,我们不妨假定 $a_i(1\leqslant i\leqslant k)$ 是 k 个正整数. 令

$$(a_1,a_2)=d_2,(d_2,a_3)=d_3,\cdots,(d_{k-1},a_k)=d_k \tag{3}$$

于是有:

定理 1.11 如果 $a_i(1\leqslant i\leqslant k)$ 是 k 个整数,则 $(a_1,\cdots,a_k)=d_k$.

证明 由式(3),$d_k\mid a_k,d_k\mid d_{k-1}$. 但 $d_{k-1}\mid a_{k-1},d_{k-1}\mid d_{k-2}$,所以 $d_k\mid a_{k-1},d_k\mid d_{k-2}$. 如此递推,可以得到 $d_k\mid a_k,d_k\mid a_{k-1},\cdots,$

$d_k \mid a_1$，即 d_k 是 $a_i(1 \leqslant i \leqslant k)$ 的公因子．又设 d 是 $a_i(1 \leqslant i \leqslant k)$ 的任意公因子，则 $d \mid a_1, d \mid a_2$，所以 $d \mid d_2$，继续递推，可以得到 $d \mid d_k$．所以 $d \leqslant |d| \leqslant d_k$．即 d_k 是 $a_i(1 \leqslant i \leqslant k)$ 的最大公因子．

例 6　求 $(136, 221, 391) = ?$

解　$(136, 221, 391) = (136, (221, 391))$

$$= (136, 17) = 17.$$

上面我们介绍了最大公因子，下面我们来讨论最小公倍数．

定义　设 $a_i(1 \leqslant i \leqslant k)$ 是 k 个整数．如果 d 是这 k 个整数的倍数，则 d 就叫做这 k 个整数的公倍数．又在 $a_i(1 \leqslant i \leqslant k)$ 的一切公倍数中的最小正数叫做最小公倍数，记作 $[a_1, \cdots, a_k]$．

最小公倍数与公倍数之间也有与最大公因子与公因子之间类似的关系．

定理 1.12　a, b 的公倍数是它们的最小公倍数 $[a, b]$ 的倍数．

证明　设 k 是 a, b 的倍数，用 $[a, b] = m$ 除 k 得到

$$k = qm + r, 0 \leqslant r < m.$$

因为 $a \mid k, a \mid m$，所以 $a \mid r$．同理 $b \mid r$．于是 r 是 a, b 的倍数，但 m 是 a, b 的最小公倍数，所以 $r = 0$．这样就有 $k = qm$，即 k 是 m 的倍数．

最大公因子与最小公倍数之间有下面的一个重要关系：

定理 1.13　如果 $ab > 0$，那么 $[a, b](a, b) = ab$．

证明　设 $[a, b] = m, (a, b) = d$．因为 $a \mid m, b \mid m$，所以 $ab \mid ma, ab \mid mb$，因此 $ab \mid (ma, mb)$，即 $ab \mid md$．

又因为 $a \mid \frac{ab}{d}, b \mid \frac{ab}{d}$，即 $\frac{ab}{d}$ 是 a, b 的公倍数，所以 $m \mid \frac{ab}{d}$，于是 $md \mid ab$，因此 $ab = md$，定理得证．

设 $a_i(1 \leqslant i \leqslant k)$ 是 k 个整数，令

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \cdots, [m_{k-1}, a_k] = m_k.$$

定理 1.14 如果 $a_i(1\leqslant i\leqslant k)$是 k 个整数,则$[a_1,\cdots,a_k]=m_k$.

例 7 求$[136,221,391]=?$

解 $[136,221,391]=[[136,221],391]$

$$=[\frac{136\times221}{17},391]=[1\ 768,391]$$

$$=\frac{1\ 768\times391}{17}=104\times391=40\ 664.$$

1.2 素数与算术基本定理

在正整数 1,2,3,…中,我们可以看到有些数只有两个正因数,有些有两个以上的正因数,只有 1 是例外,它只有一个正因数,即它只能用自身除尽.我们把这些数加以分类,有

定义 一个大于 1 的整数,如果它的正因数只有 1 及它自身,我们就称其为素数(质数).否则称其为合数.

1 既不是素数,也不是合数,它在正整数中的地位非常特殊.

我们容易知道 2,3,5,7,11…是素数,而 4,6,8,9,10,…是合数.偶数中只有 2 是素数,其余的都是合数.

任意一个大于 1 的整数 a 的最小因数 $q(>1)$是素数.事实上,如果 q 不是素数,则它就有因数 $p,1<p<q$.显然, p 又是 a 的因数,这与 q 是 a 的最小因数矛盾.

定理 2.1 设 a 是任意一个大于 1 的整数,则 a 的除 1 外的最小因数 q 是素数,并且当 a 是合数时,有 $q\leqslant\sqrt{a}$.

证明 当 a 是合数时,则 $a=bq,b>1$,否则 a 是素数.又由于 q 是 a 的最小因数,所以 $q<b,q^2\leqslant bq=a$,因此 $q\leqslant\sqrt{a}$.

定理 2.2 如果 p 是素数,a 是任意一个整数,则 a 能被 p 整除或 p 与 a 互素.

证明 因为$(p,a)\mid p,(p,a)>0$,及素数的定义,所以(p,a)

$=1$，或者$(p,a)=p$. 即$(p,a)=1$，或 $p\mid a$.

推论 2.3　设 $a_i(1\leqslant i\leqslant n)$是 n 个整数，p 是素数. 如果 $p\mid\prod_{i=1}^{n}a_i$，则存在某个 a_i 使 $p\mid a_i$.

证明　如果所有 $a_i(1\leqslant i\leqslant n)$都不能被 p 整除，则

$$(p,a_i)=1,\ i=1,2,\cdots,n.$$

因此，我们有$\left(p,\prod_{i=1}^{n}a_i\right)=1$，而这与 $p\mid\prod_{i=1}^{n}a_i$ 矛盾.

至此，我们可以证明任意一个大于 1 的整数，如果不考虑因数的次序，则能惟一地写成素数的乘积.

定理 2.4(算术基本定理)　任意大于 1 的整数 a 能写成素数的乘积，即

$$a=p_1p_2\cdots p_n,\ p_1\leqslant p_2\leqslant\cdots\leqslant p_n,$$

其中 $p_i(1\leqslant i\leqslant n)$是素数. 进一步，如果另外有

$$a=q_1q_2\cdots q_m,\ q_1\leqslant q_2\leqslant\cdots\leqslant q_m,$$

其中 $q_i(1\leqslant i\leqslant m)$是素数，则 $m=n$，$q_i=p_i$，$i=1,2,\cdots,n$.

证明　首先，我们证明分解式的存在性. 对 a 使用归纳法. 当 $a=2$ 时，分解式显然存在. 假设对小于 a 的整数素因子的分解式存在. 此时如果 a 是素数，则分解式已存在；如果 a 不是素数，则其必为合数，所以有两个正整数 b,c 满足

$$a=bc,1<b<a,1<c<a.$$

由假设及 $1<b<a,1<c<a$，我们知道 b,c 的素因子分解式存在. 于是由 $a=bc$ 能够知道 a 的素因子分解式存在. 由于 a 为有限数，所以我们只需调整素因子的次序，即能得到排序的素因子分解式.

其次，我们考虑素因子分解式的惟一性. 如果对于 a 有另外一个分解式