经全国中小学教材审定委员会2007年初审通过

数学

普通高中课程标准实验教科书

选修 4-6

初等数论初步

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

凤凰出版传媒集团

江苏教育出版社

JIANGSU EDUCATION PUBLISHING HOUSE

ISBN 978-7-5343-8244-4
9 787534 382444 >
定价：2.31元
审批号：苏费核（09秋）第21号　举报电话：12358

经全国中小学教材审定委员会2007年初审通过

普通高中课程标准实验教科书

数学

初等数论初步

chudeng shulun chubu

主　编：单　墫

副主编：李善良　陈永高　王巧林

选修 4-6

$$
\begin{cases}
x \equiv a_1 \pmod{m_1} \\
x \equiv a_2 \pmod{m_2} \\
\cdots \\
x \equiv a_k \pmod{m_k}
\end{cases}
$$

凤凰出版传媒集团

江蘇教育出版社

JIANGSU EDUCATION PUBLISHING HOUSE

凤凰国标教材

书　　名　普通高中课程标准实验教科书·数学
　　　　　初等数论初步（选修4–6）
责任编辑　胡晋宾
出版发行　凤凰出版传媒集团
　　　　　江苏教育出版社（南京市湖南路1号A楼　邮编210009）
网　　址　http://www.1088.com.cn
集团网址　凤凰出版传媒网http://www.ppm.cn
经　　销　江苏省新华发行集团有限公司
照　　排　南京理工出版信息技术有限公司
印　　刷　常州市大华印刷有限公司
厂　　址　常州市钟楼经济开发区星港路59号（邮编213023）
电　　话　0519-86697272
开　　本　1000×1400毫米　1/32
印　　张　1.875
版　　次　2007年8月第1版
　　　　　2010年1月第3次印刷
书　　号　ISBN 978-7-5343-8244-4
定　　价　2.31元
盗版举报　025-83658551

苏教版图书若有印装错误可向承印厂调换

提供盗版线索者给予重奖

主　　编　单　墫

副主编　李善良　陈永高　王巧林

编写人员　单　墫　宁连华

参与设计　葛　军　李善良　陈光立

责任编辑　胡晋宾

数论是历史最悠久的一个数学分支. 在过去的岁月里,“物不知数”、“费马大定理”、“哥德巴赫猜想”等问题,像一颗颗光辉灿烂的明珠,吸引了无数的数学爱好者,为之奋斗终身. 数论问题的研究,对现代数学的发展起了重要的推动作用,产生了一些重要的数学分支.

今天,数论不但保持着迷人的魅力,在促进数学发展方面继续起着重要的作用,而且在信息技术等应用领域中也发挥了重要的作用.

本专题将介绍初等数论的基础知识,包括整除知识、简单的一次不定方程的解法、同余方程等.

目　录

6.1 数的整除性

任意两个整数的和、差、积都是整数，但是一个非零整数去除另一个整数，所得的商却不一定是整数. 一个非零整数能否整除另一个整数，是本节研究的问题.

本节主要介绍整数的整除、因数和倍数的概念及其性质，并以带余除法和辗转相除法为工具，借助实例建立最大公约数和最小公倍数的理论，初步认识算术基本定理.

6.1.1 整数的整除

日常生活中，常遇到这样的问题：如何把 a 件物品平均分给 b 个人？这就涉及到整数 a 被整数 b 整除的问题.

1. 整除的概念及性质

我们知道，两个整数相除，所得结果不一定是整数，只有当被除数可以表示为除数和某个整数的乘积时，除数才能整除被除数，或者说被除数能被除数整除.

一般地，设 a, b 都是整数，且 $b \neq 0$. 若存在整数 q，使得 $a = bq$，则称 b 整除 a，或 a 能被 b 整除，记作 $b|a$.

此时，称 b 是 a 的因数(factor)或约数(divisor)，a 是 b 的倍数(multiple).

反之，若不存在这样的整数 q，则称 b 不整除 a，记作 $b \nmid a$.

例如，$2007 = 9 \times 223$, $2007 = 8 \times 250 + 7$，所以 $9 | 2\,007$, $8 \nmid 2\,007$.

整除有如下性质：

性质 1 如果整数 a, b, c 满足 $a|b$, $b|c$，那么 $a|c$.

性质 2 如果整数 a, b, c 满足 $a|b$, $a|c$，那么对任意整数 x, y，都有 $a \mid (bx + cy)$.

已知整数 a, b, c 满足 $a|c$, $b|c$,且存在整数 m, n,使得 $am+bn=1$, 证明:$ab|c$.

证　由 $am+bn=1$, 得

$$\begin{aligned} c &= c(am+bn) \\ &= cam+cbn. \end{aligned}$$

又因为

$$a|c,\ b|c,$$

所以

$$ab|cam,\ ab|cbn.$$

由性质 2 知,

$$ab \mid (cam+cbn),$$

即

$$ab \mid c.$$

一般地,由 $a|c$, $b|c$,并不能推出 $ab|c$,例如 $3|12$, $6|12$,但 $18\nmid 12$. 因此,例 1 中的条件 $am+bn=1$ 是重要的.

2. 带余除法

在一般的情形下,整数 a 被整数 b 除时,不一定总是整除的. 例如,$23\div 5$ 的商为 4,余数为 3,即 $23=4\times 5+3$, 其中余数小于除数. 我们把它叫做带余除法.

一般地,设 a, b 为整数,且 $b\neq 0$, 则存在惟一的一对整数 q 和 r,使得

$$a=bq+r,\ 0\leqslant r<|b|. \tag{*}$$

不妨先考虑 $b>0$ 的情形.

一方面需要说明 q, r 存在.

注意到

$$\cdots,\ -3b,\ -2b,\ -b,\ 0,\ b,\ 2b,\ 3b,\ \cdots \qquad ①$$

严格增加,其中必有相邻两项将 a"夹住",即有整数 q 使

$$qb\leqslant a<(q+1)b. \qquad ②$$

令

$$r = a - qb, \tag{③}$$

则(*)式成立.

另一方面需要说明 q, r 是惟一的. 如果 q, r 满足(*)式,那么 q 满足②式,因而 q 是惟一的;r 必然满足③式,也是惟一确定的. 实际上,q 是 $\frac{a}{b}$ 的整数部分,记作 $q = \left[\frac{a}{b}\right]$.

类似地,对于 $b < 0$ 的情形同样成立.

(*)式称为带余除法,其中 q, r 分别叫做 a 除以 b 所得的不完全商和余数(remainder),特别地,当 $r = 0$ 时,q 叫做 a 除以 b 所得的商(quotient),这时 $b \mid a$.

已知 2 008 除以一个整数 b,商为 87,余数为 r,求 b 和 r.

解　由题意得

$$2\,008 = 87b + r,\ 0 \leqslant r < b,$$

从而有

$$87b \leqslant 2\,008 < (87 + 1)b = 88b,$$

可得

$$87 \leqslant \frac{2\,008}{b} < 88,$$

所以

$$\frac{2\,008}{88} < b \leqslant \frac{2\,008}{87},$$

即

$$22\,\frac{9}{11} < b \leqslant 23\,\frac{7}{87},$$

因此

$$b = 23,$$

$$r = 2\,008 - 87 \times 23 = 7.$$

6.1.2 最大公约数与最小公倍数

1. 最大公约数

某中学召开代表大会，有教师代表 32 人，学生代表 40 人，职工代表 24 人，要编成人数相等的若干组进行讨论，且每一类代表在各组中的人数也相等. 问：最多能编成几组？

这一问题的实质就是求出一个最大的整数，它同时是 32，40，24 的约数，也就是求这 3 个数的最大公约数问题.

一般地，如果整数 b 是整数 a_i $(i=1, 2, \cdots, n)$ 的约数，那么 b 称为 $a_1, a_2, \cdots, a_n$ 的公约数. 公约数中最大的一个称为最大公约数，记为 $(a_1, a_2, \cdots, a_n)$.

例如，-6 和 -15 的公约数有 $1, -1, 3, -3$，最大公约数为 3，所以 $(-6, 15)=3$.

如果两个数的最大公约数是 1，那么这两个数称为互质或互素(coprime). 例如，$(8, 9)=1$，即 8 与 9 互质. 特别地，1 与任意一个正整数互质，即 $(a, 1)=1$.

易知，$a \pm b$ 与 b 的公约数一定是 a 与 b 的公约数. 反过来，a 与 b 的公约数也是 $a \pm b$ 与 b 的公约数，所以

$$(a \pm b, b)=(a, b).$$

如果 d 是 a 的约数，那么

$$(a, d)=d.$$

如何求两个或更多个整数的最大公约数呢？

本节开始的问题中，由于整数 32，40，24 都比较小，容易分别写出各自的约数，从而得到 $(32, 40, 24)=8$. 但对于比较大的整数，就不容易直接得到它们的最大公约数了.

一般地，求 a，b 两个整数的最大公约数可以按以下步骤进行：

不妨设 $a>b$，$b \neq 0$. 首先写出

$$a=qb+r, \ 0 \leqslant r<|b|,$$

由 $(a \pm b, b)=(a, b)$ 得

$$(a,\ b)=(a-b,\ b)=\cdots=(a-qb,\ b)=(b,\ r).$$

这样，问题转化为求$(b,\ r)$. 再由带余除法，写出

$$b=q_1r+r_1,\ 0\leqslant r_1<r.$$

同理得

$$(b,\ r)=(r,\ r_1).$$

于是，问题转化为求$(r,\ r_1)$. 如此继续下去，

$$r=q_2r_1+r_2,\ 0\leqslant r_2<r_1,$$

$$\cdots\cdots$$

$$r_{k-1}=q_{k+1}r_k+r_{k+1},\ 0\leqslant r_{k+1}<r_k,$$

$$\cdots\cdots$$

由于非负整数 $r_1>r_2>\cdots$，因此，经过若干步将有

$$r_{n+1}=0,$$

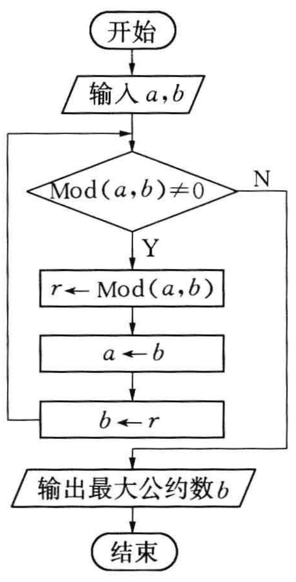
这时，

$$r_{n-1}=q_{n+1}r_n.$$

这表明 r_n 是 r_{n-1} 的约数，所以 $(r_{n-1},\ r_n)=r_n$. 于是，

$$(a,\ b)=(b,\ r)=(r,\ r_1)=(r_1,\ r_2)=\cdots=(r_{n-1},\ r_n)=r_n.$$

这就得到了求$(a,\ b)$的一个方法，通常称为辗转相除法. 其算法程序框图如下：



求(27，15).

解

$$27 = 1 \times 15 + 12,$$
$$15 = 1 \times 12 + 3,$$
$$12 = 4 \times 3.$$

所以

$$(27,\ 15) = 3.$$

以上步骤可以缩简为下面的算式，其中，每次的商 1，1，4 写在两道竖线之间.

27	1	15
15	1	12
12	4	3
12		

大厦公司销售某种货物，去年总收入为 36 963 元. 今年每件货物的售价(单价)不变，总收入 59 570 元. 如果单价(以元为单位)是大于 1 的整数，那么今年与去年各售这种货物多少件？

解　单价是 36 963 与 59 570 的公约数，由辗转相除法得出

$$(36\,963,\ 59\,570) = 37.$$

36 963	1	59 570
22 607	1	36 963
14 356	1	22 607
8 251	1	14 356
6 105	1	8 251
4 292	2	6 105
1 813	1	2 146
1 665	5	1 813
148	2	333
148		296
—	4	37

因为 37 的约数只有 1 与本身，所以 36 963，59 570 的大于 1 的公约数只有 37，即单价为 37 元.

于是，今年售出 59 570 ÷ 37 = 1 610(件)，去年售出 36 963 ÷ 37 = 999(件).

思考

如果去年、今年的总收入分别为 36 972 元、59 544 元，那么今年与去年各售这种货物多少件?

探究

如何求 n 个数 a_1, a_2, …, a_n 的最大公约数呢?

可以用连续求两个数的最大公约数的方法去完成，即先求出 $d_1 = (a_1, a_2)$，再求 $d_2 = (d_1, a_3) = (a_1, a_2, a_3)$. 这样继续下去，最后得出

$$d_{n-1} = (d_{n-2}, a_n) = \cdots = (a_1, a_2, \cdots, a_n).$$

辗转相除法不仅可以实际求出 (a, b)，而且还可以推导出关于最大公约数的一个重要性质.

定理 设整数 a, b 不同时为 0，则存在一对整数 u, v，使得

$$(a, b) = ua + vb.$$

证 运用求两个数 a, b 最大公约数中的等式

$$r_{n-2} = q_n r_{n-1} + r_n,$$

即

$$(a, b) = r_n = r_{n-2} - q_n r_{n-1}. \tag{*}$$

类似地(将 n 换作 $n-1$)，

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}.$$

代入(*)式得

$$(a, b) = u_1 r_{n-2} + v_1 r_{n-3},$$

其中 u_1, $v_1 \in \mathbf{Z}$.

再将 $r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}$ 代入(*)式消去 r_{n-2}，…直至产生要证的恒等式.

上面的证明方法也给出了 u，v 的具体算法.

两个容器，一个容量为 27 L，另一个为 15 L，如何利用它们从一桶油中倒出 6 L 油来？

解　不难求得 $(27,\ 15)=3$，且

$$27=1\times15+12,$$
$$15=1\times12+3,$$

从而

$$3=15-1\times12=15-1\times(27-1\times15),$$

即

$$3=2\times15-27,$$

于是

$$6=4\times15-2\times27.$$

这表明，需往小容器里倒 4 次油，每次倒满就往大容器里倒，大容器满了就往桶里倒. 这样在大容器第二次倒满时，小容器里剩下的就是 6 L 油.

2. 最小公倍数

大小两个互相啮合的齿轮，齿数分别为 68，51，在转动过程中同时啮合的两齿到下次再同时啮合时，分别转过多少圈？

这一问题的实质就是求出一个最小的正整数，它同时是 68 和 51 的倍数，也就是求这两个数的最小公倍数.

一般地，如果整数 a 是整数 b_i $(i=1,\ 2,\ \cdots,\ n)$ 的倍数，那么 a 称为 $b_1,\ b_2,\ \cdots,\ b_n$ 的公倍数. 正公倍数中最小的称为最小公倍数，记为 $[b_1,\ b_2,\ \cdots,\ b_n]$.

例如，-3，4，18 的公倍数有

$$36,\ -36,\ 72,\ -72,\ 108,\ -108,\ \cdots$$

其中最小公倍数是 36，即

$$[-3,\ 4,\ 18]=36.$$

探究

设 a, b 为整数,那么(a, b), $[a, b]$与 a, b 之间有没有关系呢? 试选取几组不同的 a, b 的值进行探讨.

可以发现,(a, b), $[a, b]$与 a, b 之间存在以下关系:

$$(a, b)[a, b] = ab.$$

由此可知,已知两数 a, b 及它们的最大公约数(a, b),就可以求出它们的最小公倍数$[a, b]$.

求[144, 480].

解 因为

$$480 = 3 \times 144 + 48,$$
$$144 = 3 \times 48,$$

所以

$$(144, 480) = 48,$$

从而可得

$$[144, 480] = \frac{144 \times 480}{(144, 480)} = 1\,440.$$

6.1.3 质因数分解定理

我们知道，正整数可以按所含因数的多少分为3类：

第一类仅包含一个数1，称为单位.

第二类中的数叫做质数或素数(prime). 质数大于1，并且仅有两个因数，即1与自身，如2，5，7，31等.

第三类中的数叫做合数(composite). 合数有真因数，即有不同于1与自身的因数.

质数中只有2是偶数，其余的质数都是奇数. 当然，奇数不都是质数，如 $15=3\times 5$ 是合数.

如果质数 p 是正整数 a 的因数(约数)，那么 p 称为 a 的质因数

证明：已知 a，b 为正整数，如果质数 p 是 ab 的因数，那么 p 一定是 a 或 b 的因数.

证　如果质数 p 不是 a 的因数，那么 p 与 a 的公因数只有1.

由 $(a, b)=ua+vb$ 的特殊情形可知，存在整数 u，v，使得

$$1=ua+vp,$$

从而

$$b=uab+vpb.$$

又 $p|ab$，所以上式右边两项均能被 p 整除，因而，左边的 b 能被 p 整除.

例1体现了质数的基本特性. 由此我们还可以进一步得到质因数分解定理(又称算术基本定理).

质因数分解定理　每一个大于1的整数 n 都能分解成质因数的乘积，并且若不考虑因数的次序，则分解的方式是惟一的，即 n 可以惟一地表示成

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},$$

其中 p_1，p_2，…，p_k 为不同的质数，α_1，α_2，…，$\alpha_k\in\mathbf{N}^*$.