经全国中小学教材审定委员会2005年初审通过

普通高中课程标准实验教科书

数学

（选修4-6）

初等数论初步

SHUXUE

北京师范大学出版社

经全国中小学教材审定委员会2005年初审通过

普通高中课程标准实验教科书

数学（选修4-6）

初等数论初步

SHUXUE

主　　编　严士健　王尚志

副 主 编　张饴慈　李延林　张思明

本册主编　严士健

编写人员　（按姓氏笔画排序）

王肖玉　严士健　张饴慈

高　阳　梁丽平

北京师範大學出版社

·北京·

引　言

数论是研究整数性质的一个数学分支，初等数论以算术方法为主要方法．它是古老而又基础的数学，从产生之初便有着让人难以抗拒的魅力．它的问题浅显易懂，并不需要过多的预备知识，只须掌握一些基本的数学知识，初学者便可登堂入室，理解它的许多重要内容．人们着迷于它的简捷和优美．因此，数论不仅吸引了无数的数学家，也吸引了无数的数学爱好者．数论中一些问题的解决对现代数学的发展起了重要的推动作用，也产生了一些直接与数学有关的新的重要数学分支．尤其在 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，数论在信息安全中作出了重大的贡献．

在本专题中，我们将学习有关整数和整除的知识，探索运用辗转相除法求解简单的一次不定方程、简单同余方程、同余方程组等．从中可以体会一些重要的思想方法，了解我国古代数学的一些重要成就．这个专题的内容比较完整，可以很好地锻炼同学们的逻辑思维能力，形成较好的数学基础．

目　录

第一章 带余除法与数的进位制

整除性理论是初等数论的基础．对于“整数”，相信大家都不会感到陌生，本章我们将从数论中最基本的概念——整除和带余除法出发，认识数、学习进位制.

§1 整除与带余除法

1.1 整 除

我们早就已经学习过“整数”，知道两个整数的和、差、积仍然是整数．但是，用不等于零的整数去除另一个整数时，所得的商却不一定是整数，例如：

$4\div 2=2$，2 是整数，通常说 2 可以整除 4；

$3\div 2=1.5$，1.5 不是整数，通常说 2 不能整除 3.

一般地，我们给出如下关于整除的定义：

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

$$a=bq$$

成立，那么就说 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（或约数），把 a 叫作 b 的倍数.

若上式中的整数 q 不存在，则称 b 不整除 a（或 a 不能被 b 整除），记作 $b\nmid a$.

例如：$2\mid 4$，$3\nmid 5$.

由整除的定义，不难得到如下性质：

如果 a,b,c 都是非零的整数，就有

1. 若 $a|b, b|c$，则 $a|c$；

2. 若 $a|c$，则 $ab|cb$；

3. 若 $a|b$ 且 $a|c$，则对于任意整数 m, n 都有 $a|(mb+nc)$；

4. 若 $a|b$，则 $|a| \leqslant |b|$.

下面仅以性质 1 为例进行证明.

证明 由 $a|b$ 可知：存在整数 p，使得

$$b=pa, \qquad ①$$

又因为 $b|c$，所以，存在整数 q，使得

$$c=qb. \qquad ②$$

由①②可知

$$c=qb=q(pa)=(qp)a.$$

所以，$a|c$.

1.2 带余除法

我们熟悉正整数的除法法则. 例如：

用 3 去除 20，得到的商是 6，余数是 2，可以写成：$20=3\times6+2$；

用 5 去除 25，得到的商是 5，余数是 0，可以写成：$25=5\times5+0$.

这就是带余除法，它是初等数论的证明中最重要、最基本、最常用的工具. 一般地可以表述为：

定理 1 （带余除法）设 a, b 是两个给定的整数，其中 $b>0$，那么，一定存在唯一的一对整数 q 及 r，满足

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

可以看出：$b|a$ 的充要条件是 $r=0$. 我们称 r 是 b 除 a 所得的余数.

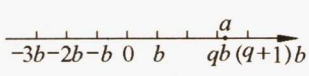


图 1-1

证明 (1)存在性 考察 b 的所有倍数组成的序列

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

则 a 必在上述序列的某两项之间(如图 1-1)，即存在一个整数 q，使得

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

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

(2)唯一性 若还有整数 q' 与 r' 满足

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

不妨设 $r'\geqslant r$，则 $0\leqslant r'-r<b$，且

$$r'-r=(q-q')b.$$

由整除的定义可知：$b\mid(r'-r)$. 若 $r'-r\neq 0$，则 $b\leqslant(r'-r)$. 这与 $0\leqslant r'-r<b$ 矛盾. 所以，必有 $r'=r$，进而 $q'=q$.

上面我们讨论了 $b>0$ 的情形，当 $b<0$ 时，带余除法可以表述为：

设 a,b 是两个给定的整数，其中 $b<0$，那么一定存在唯一的一对整数 q 及 r，满足

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

在后面的讨论中，我们只考虑 $b>0$ 的情形.

定理中我们要求余数满足 $0\leqslant r<b$，例如 $-13=(-3)\times 5+2$，而不能写成 $-13=(-2)\times 5-3$.

根据上述定理，我们可将所有整数按除数 b 与余数 r 进行分类. 如：

除数为 2 时，任何整数被 2 除，余数或者为 0，或者为 1. 这样，所有整数就可以分为两类：一类余数为 0，即我们所说的偶数，一类余数为 1，即我们所说的奇数，分别表示为：$2n$ 和 $2n+1$.

除数为 3 时，任何整数被 3 除，余数或者为 0，或者为 1，或者为 2. 这样，所有整数就可以分为 3 类：一类余数为 0，一类余数为 1，一类余数为 2，分别表示为：$3n,3n+1,3n+2$.

例　对于任意的整数 n，求证：$3\mid n(n+1)(2n+1)$.

证明　除数为 3 时，所有整数可分为 3 类：$3k,3k+1,3k+2$. 所以，下面可分 3 种情况来考虑：

(1) $n=3k(k\in\mathbf{Z})$ 时，$3\mid n$，所以，$3\mid n(n+1)(2n+1)$；

(2) $n=3k+1(k\in\mathbf{Z})$ 时，$2n+1=2(3k+1)+1$

$$=6k+3=3(2k+1),$$

所以，$3\mid 2n+1$，于是，$3\mid n(n+1)(2n+1)$；

(3) $n=3k+2(k\in\mathbf{Z})$ 时，$n+1=3k+2+1$

$$=3k+3=3(k+1),$$

所以，$3\mid n+1$，于是，$3\mid n(n+1)(2n+1)$.

综合(1)(2)(3)可知：对于任意的整数 n，都有

$$3\mid n(n+1)(2n+1).$$

习 题 1—1

1. 用整除或不整除的符号(|,∤)填空：

(1)2 ____ 3；　(2)3 ____ 6；　(3)n ____ n^2(n 为正整数).

2. 利用整除的定义证明整除的性质 2,3,4.

3. 已知除数 $b=5$,对于下列一组数 a

$$12,-13,15,-3,$$

按照带余除法确定 q,r 的值,使得 $a=bq+r,0\leqslant r<b$.

4. 除数为 7,请将所有整数按 7 及其余数分类.

5. 对于任意的整数 n,求证:$2\mid n(n^2+1)$.

6. 对于任意的整数 n,求证:$6\mid n(n^2-1)$.

7. 对于任意整数 x,y,求证:$8\nmid(x^2-y^2-2)$.

§2　二　进　制

在计数和运算中，我们常用的是“逢十进一”，这种计数方法称为**十进制**，10 称为**基数**.

十进制是一种世界上使用非常广泛的计数方式. 但是，在生活中常常还会遇到其他的“进制”. 例如

关于时间的计数方法：1 时＝60 分，1 分＝60 秒，这是六十进制，基数为 60；

关于星期的计数方法：一周有 7 天，这是七进制，基数为 7；

在现代社会中，计算机使用二进制来处理各种信息.

二进制与十进制的互化

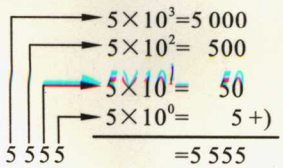
我们知道：十进制中，用 0，1，2，…，9 这十个数码就可以表示所有的数字，同一数码在不同的位置上意义不同，如 5 555：

从右起，第一位上的 5 代表 5×10^0，即 5；

第二位上的 5 代表 5×10^1，即 50；

第三位上的 5 代表 5×10^2，即 500；

第四位上的 5 代表 5×10^3，即 5 000.



用式子表示也就是

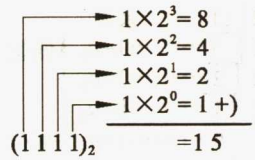
$$5\,555=5\times10^3+5\times10^2+5\times10^1+5\times10^0.$$

问题提出

在二进制中，我们可以只用两个数码 0 和 1 来表示所有的整数，如何表示呢？

为与十进制进行区分，我们常把用二进制表示的数 a 写成 $(a)_2$，其中 a 的各个数码均为 0 或者 1.

二进制计数的方法是“逢二进一”，类比于十进制，我们可以知道：二进制表示的数 $(1111)_2$ 中，右起第一位上的 1 表示 1×2^0，第二位上的 1 表示 1×2^1，第三位上的 1 表示 1×2^2，第四位上的 1 表示 1×2^3.



也就是说

$$(1111)_2=1\times2^3+1\times2^2+1\times2^1+1\times2^0=15.$$

这样，我们就把二进制表示的数$(1111)_2$转化为了十进制表示的数 15.

抽象概括

任意一个二进制表示的数$(a_na_{n-1}\cdots a_0)_2$(其中$a_j=0$或 1，$0\leqslant j\leqslant n$)，都可以利用上面的方法表示为十进制表示的数，这个数就等于

$$a_n\cdot2^n+a_{n-1}\cdot2^{n-1}+\cdots+a_1\cdot2+a_0.$$

例 1 把下列二进制表示的数转化为十进制表示的数.

(1)$(101011)_2$；　　(2)$(10010)_2$.

解 (1)$(101011)_2$

$$=1\times2^5+0\times2^4+1\times2^3+0\times2^2+1\times2^1+1\times2^0=43;$$

(2)$(10010)_2=1\times2^4+0\times2^3+0\times2^2+1\times2^1+0\times2^0=18.$

如何把一个用十进制表示的数转化为用二进制表示的数呢?

以 11 为例，我们可以假设 11 的二进制表示为$(a_na_{n-1}\cdots a_0)_2$，其中$a_i=0$或 1，$i=0,1,2,\cdots,n$. 则

$$\begin{aligned}11&=a_n\cdot2^n+a_{n-1}\cdot2^{n-1}+\cdots+a_0\cdot2^0\\&=2(a_n\cdot2^{n-1}+a_{n-1}\cdot2^{n-2}+\cdots+a_1)+a_0,\end{aligned}$$

所以，a_0就等于 11 除以 2 所得的余数 1，$a_n\cdot2^{n-1}+a_{n-1}\cdot2^{n-2}+\cdots+a_1$就等于 11 除以 2 所得的商 5. 根据

$$\begin{aligned}5&=a_n\cdot2^{n-1}+a_{n-1}\cdot2^{n-2}+\cdots+a_1\\&=2(a_n\cdot2^{n-2}+a_{n-1}\cdot2^{n-3}+\cdots+a_2)+a_1\end{aligned}$$

可以得到：a_1等于 5 除以 2 所得的余数 1，$a_n\cdot2^{n-2}+a_{n-1}\cdot2^{n-3}+\cdots+a_2$等于 5 除以 2 所得的商 2. 同理，由

$$\begin{aligned}2&=a_n\cdot2^{n-2}+a_{n-1}\cdot2^{n-3}+\cdots+a_2\\&=2(a_n\cdot2^{n-3}+a_{n-1}\cdot2^{n-4}+\cdots+a_3)+a_2\end{aligned}$$

可得：a_2等于 2 除以 2 所得的余数 0，$a_n\cdot2^{n-3}+a_{n-1}\cdot2^{n-4}+\cdots+a_3$等于 2 除以 2 所得的商 1，于是$a_3=1$.

这样，我们就得到了 11 的二进制表示$(a_3a_2a_1a_0)_2=(1011)_2$.

上述过程可以用带余除法简捷地表示如图 1-2.

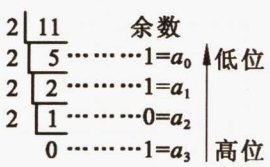


图 1-2

例 2　求出下列十进制数的二进制表示：

(1)2 005；　　(2)16.

解

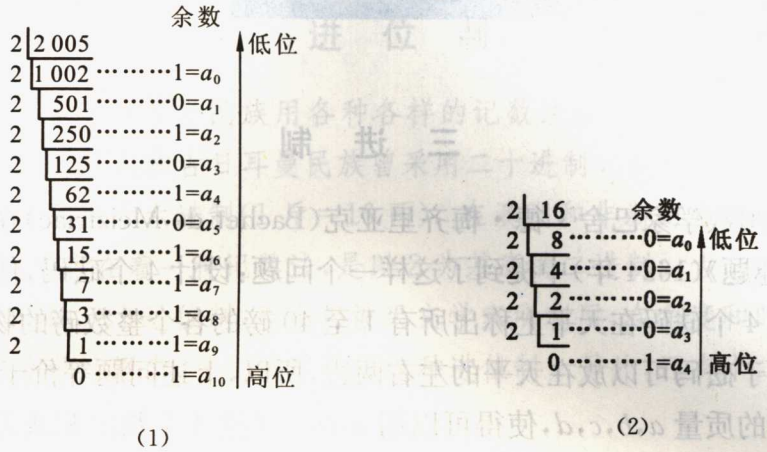


图 1-3

由图 1-3(1)(2)所示的带余除法可知，2 005＝$(11111010101)_2$，16＝$(10000)_2$.

根据上面的分析，我们可以把每一个十进制数转化为二进制数，这就意味着每一个正整数都可以用二进制表示.

习 题 1—2

A 组

1. 试用二进制数表示十进制的 0,1,2,3,…,9.
2. 把下列十进制数转化为二进制数：

   (1)1 024；　　(2)341；　　(3)255.
3. 把下列二进制数转化为十进制数：

   (1)$(11110)_2$；　　(2)$(1010110)_2$.

B 组

利用带余除法证明，任一正整数 n 必可唯一表示为

$$n=a_k\cdot 2^k+a_{k-1}\cdot 2^{k-1}+\cdots+a_1\cdot 2+a_0,$$

其中整数 $k\geqslant 0$，$a_k\neq 0$，且对于任意的 $0\leqslant j\leqslant k$，均有 $a_j=0$ 或 1.

课题学习

三 进 制

法国数学家巴舍·德·梅齐里亚克(Bachet de Meiziriac)在他的《数学趣题》(1624 年)中提到了这样一个问题:设计 4 个砝码,使得可以用这 4 个砝码在天平上称出所有 1 至 40 磅的各个整数磅的物体.

由于砝码可以放在天平的左右两边,所以,上述问题等价于:求 4 个砝码的质量 a,b,c,d,使得可以用 a,b,c,d 这 4 个数的和或差表示从 1 到 40 的所有整数.

用逻辑推理的方法能够得出答案:$(a,b,c,d)=(1,3,9,27)$.

运用三进制可以更为简捷地解决这个问题. 下面,我们首先来了解三进制.

三进制是以 3 为基数的,根据带余除法,我们可以证明:任一正整数 n 必可唯一表示为

$$n=a_k\cdot 3^k+a_{k-1}\cdot 3^{k-1}+\cdots+a_1\cdot 3^1+a_0,$$

其中整数 $k\geqslant 0$,$a_k\neq 0$,且对于任意的 $0\leqslant j\leqslant k$,均有 $a_j=0$ 或 1 或 2.

问题 1 证明上述事实.

由此可知,我们只用 3 个数码 0,1,2 就可以表示任意的整数 n. 记 n 的三进制表示为 $(a_ka_{k-1}\cdots a_1a_0)_3$.

问题 2 如何进行三进制与十进制之间的转换.

请把下面三进制表示的数转换为十进制表示的数.

(1)$(10212)_3$; (2)$(1000)_3$; (3)$(2222)_3$.

并写出十进制 8,14,17,21 的三进制表示.

问题 3 仿照十进制的加法运算,推导三进制下数的加法法则.

问题 4 仿照十进制的乘法运算和“九九乘法表”,推导三进制下数的乘法法则,构造相应的乘法表.

问题 5 运用三进制,解决“砝码问题”.

阅读材料

进　位　制

世界上各个民族用各种各样的记数法来组织他们的数. 古代玛雅人和古日耳曼民族曾采用二十进制. 我国在计量方面曾采用十六进制(1 斤=16 两). 在澳洲和非洲的原始民族中,还存在着一种记数法,是以 2 为基底的二进制. 古老的巴比伦的六十进位制,至今仍被天文学家所利用,在角度和时间的分秒计算中,我们仍然采用这种进位制. 另外,还有十二进制、五进制等.

这些记数法是为什么和如何创造出来的? 虽然绝大多数都难以考证了,但谁都不怀疑,广为采用的十进制,来源于人类利用他们的手指进行记数. 二十进制可能起源于记数时手指脚趾并用的原始部落. 至于六十进制,古巴比伦人为什么要引进如此大的基数? 人们猜测,它可能来源于两个具有不同基数的进位制的结合,比如说 10 和 12 的最小公倍数就是 60.

在所有的进位制中,哪一种的优势更为明显? 这是一个很难回答的问题.

18 世纪后期的大博物学家布封(Buffon,1707—1788)曾经提议:应该举世公用十二进制. 他指出:12 有 4 个不等于零或本身的除数,而 10 只有两个. 他坚持说,正是由于我们的十进制,世世代代以来,都感到极为不便,所以虽然 10 是公认的基底,而在大多数的度量衡中,都有着以 12 为基底的辅助单位.

另一方面,大数学家拉格朗日(Lagrange,1736—1813)宣称:用素数作基数有很大的好处. 他指出:用素数作基底,每个整分数就都不能化简,因此表示该数的方法只有一种. 例如在十进制中,小数 0.36,就代表着许多个分数:$\frac{36}{100},\frac{18}{50},\frac{9}{25},\cdots$若用 11 等质数作基底,这种暧昧不明之处就大大减少了.

在电子计算机出现以前,十进制在所有的数值计算领域内占有至高无上的地位,而对其他记数法的兴趣,主要是出于历史和文化上的原因. 仅有少数几个孤立的数学问题,用二进制和三进制可以给出最好的表述.

当计算机以多种形式发展起来时，如何设计制造出这样的“硬件”：使得其尽可能地有效，体积尽可能地小？这就引起了对各种记数法的深入研究．出于很多的理由，人们最终选择了“二进制”．虽然，对于大多数人来说，只需要经过不多的简单努力，就可以像对十进制一样，自如地运用二进制．然而，由于我们毕竟是在一种不同的遗产——十进制——中成长起来的，所以，人们就设计让计算机进行十进制与二进制的转化．这样，我们看到的输入和输出计算机的数据都是十进制的，二进制的运算主要是在计算机内部．

信息技术应用

把十进制数 a 转换为二进制数，其算法可用图 1-4 表示．

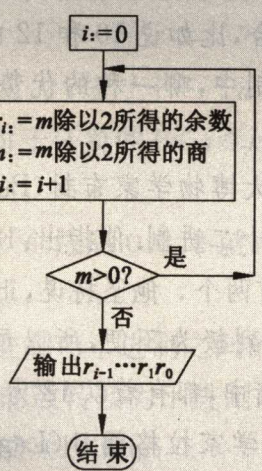


图 1-4

复习题一

A 组

1. 若 $a|b,c|d$，求证：$ac|bd$.
2. 试证：当 x 是整数时，多项式 $f(x)=\frac{1}{3}x^3-2x^2+\frac{11}{3}x-2$ 的值仍为整数.
3. 对于任意整数 n，求证：$6|n(n+1)(2n+1)$.
4. 试写出下列十进制数的二进制表示：

   (1)38；　　(2)2 008；

   (3)$2^{2^2}+1$；　　(4)$4^{2m}+2^m+1(m=1,2)$.
5. 已知函数 $f(x)=x^5+x^3+x^2+1$，试写出 $f(2)$ 的二进制表示.
6. 根据十进制运算，我们知道：$5+3=8$，请将这个加法算式写成二进制表示，并由此猜想二进制加法法则.
7. 若 a,b 是任意两个整数，且 $b>0$，仿照定理 1 证明：存在两个整数 s 及 t，使得

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

成立，并且当 b 是奇数时，s,t 是唯一存在的. 当 b 为偶数时结果如何？

B 组

1. 已知 $a|c,b|c$，且存在整数 s 与 t 使得 $as+bt=1$，求证：$ab|c$.
2. 若 $3|n$，且 $7|n$，求证：$21|n$.
3. 对任意整数 n，证明：

   (1)若 $2\nmid n$，则 $8|n^2-1,24|n(n^2-1)$；

   (2)若 $2\nmid n$ 且 $3\nmid n$，则 $24|n^2+23$.

第二章 可 约 性

本章从认识素数与合数出发，了解确定素数的方法，还将通过实例，学习利用辗转相除法求两个整数最大公因数的方法，理解互素的概念，探索公因数和公倍数的性质，了解算术基本定理. 在此基础上，学会用辗转相除法求解一次不定方程.

§1 素数与合数

在正整数中，1 的正因数只有它本身，并且 1 是任何整数的因数，因此在整数中 1 占有特殊的地位. 任一个大于 1 的整数，都至少有两个正因数，即 1 和它本身 . 我们把这些数再加以分类，就得到

定义　一个大于 1 的正整数，如果它的正因数只有 1 和它本身，就叫作素数，否则就叫作合数.

说　明

负整数与正整数有类似的性质 . 素数总是指正的 .1 既不是素数也不是合数 .

例如　2,3,5,7,11,13,17 都是素数，而 4,6,8,9,10,12,14,15,16 都是合数.

由定义立刻可以推出：

大于 1 的整数 a 是合数的充要条件是：存在整数 $1<d,e<a$，使得 $a=de$.

如果 d（或 e）还是合数，则这个过程可以继续下去，直到素数出现. 因此，不难知道：若 a 是合数，则必存在素数 $p|a$. 我们把 p 称为 a 的素因数.