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·

营销中心电话　010-58802783
服务中心电话　010-58802795
邮购科电话　010-58808083
传　　真　010-58802838
学科编辑电话　010-58802811　58802790
电子邮箱　shuxue3@bnupg.com
通信地址　北京师范大学出版社基础教育分社(100875)

出版发行：北京师范大学出版社　www.bnup.com.cn
北京新街口外大街19号
邮政编码：100875
印　刷：江西教育印务实业有限公司
经　销：江西省新华书店
开　本：890mm × 1240mm　1/16
印　张：4.75
字　数：73千字
版　次：2007年5月第2版
印　次：2019年7月第24次印刷
定　价：4.55元
ISBN 978-7-303-07674-1
责任编辑：焦继红　兰小银　装帧设计：王　蕊
责任校对：陈　民　责任印制：孙文凯　窦春香

前　言

你们将进入更加丰富多彩的数学世界.

你们将学到更多重要和有趣的数学知识、技能及应用.

你们将更多地感受到深刻的数学思想和方法.

你们将进一步体会数学对发展自己思维能力的作用，体会数学对推动社会进步和科学发展的意义，体会数学的文化价值.

你们正在长大，需要考虑自己未来的发展. 要学习的东西很多，高中数学的内容都是基础的，时间有限，选择能力是很重要的，你们需要抓紧时间选择发展的方向，选择自己感兴趣的专题，这是一种锻炼.

在高中阶段，学习内容是很有限的. 中国古代有这样的说法："授之以鱼，不如授之以渔"，学会打鱼的方法比得到鱼更重要. 希望同学们不仅关注别人给予你们的知识，更应该关注如何获得知识. 数学是提高"自学能力"最好的载体之一.

在数学中，什么是重要的（What is the key in Mathematics）？20 世纪六七十年代，在很多国家都讨论了这个问题. 大部分人的意见是：问题是关键（The problem is the key in Mathematics）. 问题是思考的结果，是深入思考的开始，"有问题"也是创造的开始. 在高中数学的学习中，同学们不仅应提高解决别人给出问题的能力，提高思考问题的能力，还应保持永不满足的好奇心，大胆地发现问题、提出问题，养成"问题意识"和交流的习惯，这对你们将来的发展是非常重要的.

在学习数学中，有时会遇到一些困难，树立信心是最重要的. 不要着急，要有耐心，把基本的东西想清楚，逐步培养自己对数学的兴趣，你会慢慢地喜欢数学，她会给你带来乐趣.

本套教材由 26 册书组成：必修教材有 5 册；选修系列 1 有 2 册，选修系列 2 有 3 册，它们体现了发展的基本方向；选修系列 3 有 6 册，选修系列 4 有 10 册，同学们可以根据自己的兴趣选修其中部分专题. 习题分为三类：一类是可供课堂教学使用的"练习"；一类是课后的"习题"，分为 A，B 两组；还有一类是复习题，分为 A，B，C 三组.

研究性学习是我们特别提倡的. 在教材中强调了问题提出，抽象概括，分析理

解，思考交流等研究性学习过程．另外，还专门安排了“课题学习”和“探究活动”．

“课题学习”引导同学们递进地思考问题，充分动手实践，是需要完成的部分．

在高中阶段，根据课程标准的要求，学生需要至少完成一次数学探究活动，在必修课程的每一册书中，我们为同学们提供的“探究活动”案例，同学们在教师的引导下选做一个，有兴趣也可以多做几个，我们更希望同学们自己提出问题、解决问题，这是一件很有趣的工作．

同学们一定会感受到，信息技术发展得非常快，日新月异，计算机、数学软件、计算器、图形计算器、网络都是很好的工具和学习资源，在条件允许的情况下，希望同学们多用，“技不压身”．它们能帮助我们更好地理解一些数学的内容和思想．教材中有“信息技术建议”，为同学们使用信息技术帮助学习提出了一些具体的建议；还有“信息技术应用”栏目，我们选取了一些能较好体现信息技术应用的例子，帮助同学们加深对数学的理解．在使用信息技术条件暂时不够成熟的地方，我们建议同学们认真阅读这些材料，对相应的内容能有所了解．教材中信息技术的内容不是必学的，仅供参考．

另外，我们还为同学们编写了一些阅读材料，供同学们在课外学习，希望同学们不仅有坚实的知识基础，而且有开阔的视野，能从数学历史的发展足迹中获取营养和动力，全面地感受数学的科学价值、应用价值和文化价值．

我们祝愿同学们在高中数学的学习中获得成功，请将你们成功的经验告诉我们，以便让更多的朋友分享你们成功的喜悦．

我们的联系方式是：北京师范大学出版社基础教育分社（100875），010-58802811．

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 $a\mid b$，$b\mid c$，则 $a\mid c$；

2. 若 $a\mid c$，则 $ab\mid cb$；

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

$$b=pa, \tag{1}$$

又因为 $b|c$，所以，存在整数 q，使得

$$c=qb. \tag{2}$$

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.

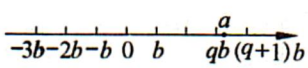


图 1-1

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：$b|(r'-r)$. 若 $r'-r\neq0$，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 $-13=(-3)\times5+2$，而不能写成 $-13=(-2)\times5-3$.

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.

$$\begin{array}{l}5\times10^3=5\,000\\5\times10^2=\ \ 500\\5\times10^1=\ \ \ 50\\5\times10^0=\ \ \ \ 5\ +)\\\hline\qquad\quad =5\,555\end{array}\qquad 5\,555$$

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.

$$\begin{array}{l}1\times2^3=8\\1\times2^2=4\\1\times2^1=2\\1\times2^0=1\ +)\\\hline\qquad\ =15\end{array}\qquad (1111)_2$$

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$(a_n a_{n-1}\cdots a_0)_2$(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

$$a_n\cdot 2^n+a_{n-1}\cdot 2^{n-1}+\cdots+a_1\cdot 2+a_0.$$

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)$(101011)_2$

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

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

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$(a_n a_{n-1}\cdots a_0)_2$,其中 $a_i=0$ 或 $1, i=0,1,2,\cdots,n$. 则

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

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

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

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

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

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

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

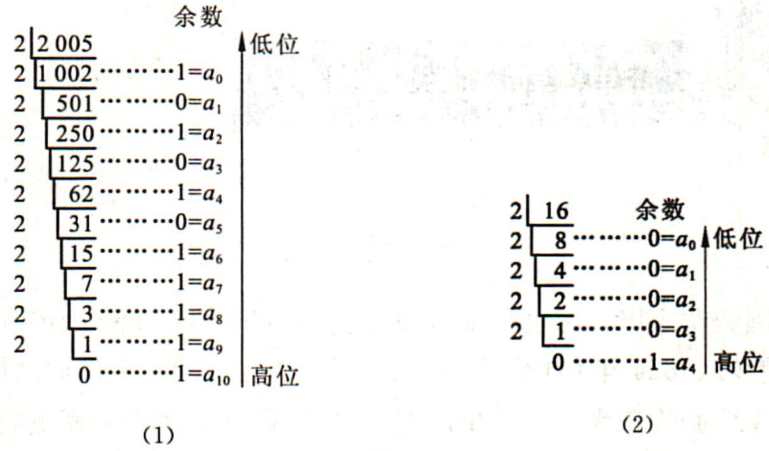


图 1-3

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

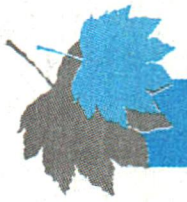
1. 试用二进制数表示十进制的 0,1,2,3,…,9.
2. 把下列十进制数转化为二进制数：
   (1)1 024；　(2)341；　(3)255.
3. 把下列二进制数转化为十进制数：
   (1)$(11110)_2$；　(2)$(1010110)_2$.

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等素数作基底,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.

把十进制数 a 转换为二进制数，其算法可用图 1-4 表示.

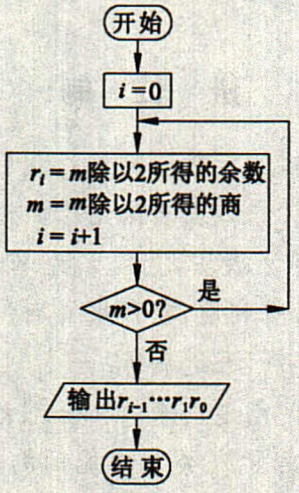


图 1-4

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.

1.1　素数的判别

问题提出

如何判断一个正整数是不是素数?

为了确定 241 是不是素数,原则上需要考察从 1 到 240 的所有正整数能否整除 241. 这个方法能否简化呢?

我们知道,如果 d 是 a 的因数,那么 $\frac{a}{d}$ 也一定是 a 的因数,d 与 $\frac{a}{d}$ 不可能都大于 $\sqrt{a}$. 因此,为了确定 a 是否为素数,我们只需考察所有不大于 $\sqrt{a}$ 的正整数能否整除 a. 进而可以知道:只需考察所有不大于 $\sqrt{a}$ 的素数即可.

以上给出了一个寻找素数的有效算法.

例 1　判断 241 是否为素数.

解　由于 $\sqrt{241}<16$,只需考查小于 16 的所有素数:2,3,5,7,11,13 能否整除 241. 通过验证它们都不能整除 241,所以 241 是素数.

例 2　求出不超过 100 的所有素数.

解　为了求出不超过 100 的所有素数,只要把 1 以及不超过 100 的所有正合数都删去即可.

由上可以知道:所有不超过 100 的正合数必有一个素因数 $p\leqslant\sqrt{100}=10$. 所以,我们只需先求出不超 10 的所有素数 2,3,5,7,然后,在 1～100 中,依次删去 2,3,5,7 之外的所有 2 的倍数、3 的倍数、5 的倍数、7 的倍数. 剩下的正好就是不超过 100 的全部素数. 具体做法见图 2-1.

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~
~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~
31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~
~~46~~ 47 ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ 59 ~~60~~
61 ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73 ~~74~~ ~~75~~
~~76~~ ~~77~~ ~~78~~ 79 ~~80~~ ~~81~~ ~~82~~ 83 ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~
~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

图 2-1

由图 2-1 可以看出,没有被删去的数共有 25 个,它们是:

2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97.

这样,我们就得到了不超过 100 的所有素数. 按照这样的做法,对于任意给定的正整数 N,可以找出不超过 N 的全部素数. 这种寻找素数的方法,是希腊时期埃拉托塞尼(Eratosthenes,约公元前 274－194)发明的,它好像用筛子筛出素数一样,所以通常叫作埃拉托塞尼筛法.

1.2　素数的个数

问题提出

容易知道:所有大于 2 的偶数都是合数,除此之外,个位数字是 5 的整数都是 5 的倍数,因此,它们也都是合数(5 除外)……

这样看来,似乎素数的个数远少于合数的个数,那么素数有多少个? 是有限个吗?

这是一个非常有趣的问题,早在公元前约 300 年时,欧几里得第一次证明了素数的个数是无穷的.

定理 1　素数有无穷多个.

证明　用反证法.

假设只有有限多个素数,不妨设它们是 $p_1,p_2,\cdots,p_k$,考虑整数

$$a=p_1p_2\cdots p_k+1.$$

显然,a 是不同于 $p_i(i=1,2,\cdots,k)$ 的整数,所以,a 为合数,故必存在素数 $q\mid a$.

由假设可知:q 必等于 $p_i(i=1,2,\cdots,k)$ 中的某一个,不妨设 $q=p_1$,则 $p_1\mid(p_1p_2\cdots p_k+1)$,这是不可能的.

因此,假设不正确,即素数有无穷多个.

习　题　2—1

1. 判断下列各数是否为素数.

(1)241;　　(2)391;

(3)1 277;　　(4)2 003.

2. 利用埃拉托塞尼筛法,写出 101～200 内所有的素数.

§2　最大公因数与辗转相除法

有了带余除法，我们就可以着手研究整数的最大公因数了. 那么，整数的最大公因数是如何定义的呢?

给定 12,18 两个整数，我们知道，这两个整数公共的因数有 2,3,6. 其中，6 是这些公因数中最大的，称之为 12 和 18 的最大公因数.

设 a,b 是两个不全为零的整数，若整数 d 是它们所有公因数中最大的一个，则称 d 为它们的最大公因数，记作 $d=(a,b)$.

特别地，当 $(a,b)=1$ 时，称为 a,b 互素.

素数是一个数本身的性质，互素是指两个数之间的关系，并不要求互素的两个数是素数. 例如 $(8,9)=1$，8 与 9 互素，但是，8 和 9 本身都是合数.

对于特殊的整数 0，我们知道：任何非零整数都是 0 的因数. 因此若整数 $b>0$，则 $(0,b)=b$.

根据定义，对于两个正整数，我们可以求出它们所有的公因数，再确定最大公因数. 是否存在更方便快捷的方法呢?

“辗转相除法”可以帮助我们快捷地求出最大公因数. 为此，我们首先证明下面的定理：

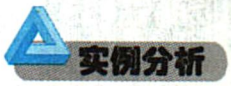
定理 2　对于三个不全为零的正整数 a,b,c 来说，若 $a=bq+c$，其中 q 是非零正整数，则 a,b 与 b,c 有相同的公因数，且 $(a,b)=(b,c)$.

证明　设 d 是 a,b 的任一公因数，由定义知，$d\mid a$ 且 $d\mid b$. 根据整除的性质可知，$d\mid(a-bq)$，即 $d\mid c$，因而 d 也是 b,c 的一个公因数.

同理可证，b,c 的任一公因数也是 a,b 的公因数. 所以 a,b 与 b,c 有相同的公因数. 等式 $(a,b)=(b,c)$ 随之显然成立.

根据这个定理，利用带余除法 $a=bq+r(0\leqslant r<b)$，我们可以将

“求两个较大数 a 与 b 的最大公因数问题”，转化为“求两个较小数 b 与 r 的最大公因数问题”.



例 1　求(1 426,1 021).

解　因为 1 426=1 021×1+405,

所以(1 426,1 021)=(405,1 021).

这个过程可以继续下去

1 021=405×2+211,则(405,1 021)=(405,211);

405=211×1+194,则(405,211)　=(194,211);

211=194×1+17,　则(194,211)　=(194,17);

194=17×11+7,　则(194,17)　=(7,17);

17=7×2+3,　则(7,17)　=(7,3);

7=3×2+1,　则(7,3)　=(1,3)=1.

所以，　(1 426,1 021)=1.

上述方法称为**辗转相除法**，用这种方法可以帮助我们求出两个数的最大公因数.

辗转相除法　给定两个正整数 $u_0>u_1$，我们可以运用第一章定理 1(带余除法)得到下面的 $k+1$ 个等式

$$\begin{aligned}
&u_0=q_0u_1+u_2, && 0<u_2<u_1,\\
&u_1=q_1u_2+u_3, && 0<u_3<u_2,\\
&u_2=q_2u_3+u_4, && 0<u_4<u_3,\\
&\cdots\\
&u_{k-1}=q_{k-1}u_k+u_{k+1}, && 0<u_{k+1}<u_k,\\
&u_k=q_ku_{k+1}.
\end{aligned}$$

由于余数 $u_2,u_3,\cdots$是正整数，且 $u_0>u_1>\cdots>0$. 因此，在有限步内余数一定为 0($u_{k+2}=0$).

辗转相除法为我们提供了求两个数的最大公因数的方法：根据定理 2，不难看出：

$$(u_0,u_1)=(u_1,u_2)=(u_2,u_3)=\cdots=(u_{k-1},u_k)=(u_k,u_{k+1})=u_{k+1}.$$

例 2　利用辗转相除法求 1 859 与 1 573 的最大公因数.

解　1 859 =1×1 573+286,　则(1 859,1 573)=(286,1 573);

1 573 =286×5+143,　则(286 ,1 573) =(286,143);

286 =143×2,　则(286,143)　=143.

所以,(1 859,1 573)=(286,1 573)=(286,143)=143.

用短除的形式可以把带余除法的过程表示如下,为了篇幅紧凑,我们采用被除数写在左边,除数写在右边的格式:

$$
\begin{array}{rr|l}
 & u_0=1\,859 & 1\,573=u_1 \\
 & 1\,573 & 1=q_0 \\
\hline
u_1=1\,573 & 286=u_2 & \\
1\,430 & 5=q_1 & \\
\hline
u_2=286 & 143=u_3 & \\
286 & 2=q_2 & \\
\hline
0 & &
\end{array}
$$

例 3　求(515,110).

解法一　我们可以考虑直接运用辗转相除法,得到

(515,110)=(75,110)=(75,35)=(5,35)=5;

解法二　因为 5|515,且 5|110,又

$$\left(\frac{515}{5},\frac{110}{5}\right)=(103,22)=(15,22)=1,$$

所以

$$(515,110)=5\left(\frac{515}{5},\frac{110}{5}\right)=5.$$

设 a,b 是任意两个不全为零的正整数. 则

①对于任意正整数 c,均有 $(ac,bc)=c(a,b)$;

②若 δ 是 a,b 的任一正公因数,则 $\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{\delta}$,特别地,

$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1.$

事实上,将辗转相除法中的各式两边都乘 c,则应用定理 2 得知

$$(ac,bc)=(u_0c,u_1c)=cu_{k+1}=c(a,b).$$

所以①成立.

其次,在②的假设下,$\frac{a}{\delta},\frac{b}{\delta}$是整数,则由①知

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

两边除以 δ,即得

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

对于 3 个或 3 个以上整数的最大公因数问题，我们可以将其转化为两个整数的最大公因数问题. 如

$$(216,64,1\ 000)=((216,64),1\ 000)=(8,1\ 000)=8.$$

练　习

1. 利用辗转相除法，求下列各组数的最大公因数.

(1) 1 927 与 386；　　(2)1 234 与 243.

2. 求值.

(1) (1 234,324)；　　(2)(205,25).

我们已经知道，辗转相除法可以帮助我们求出两个数 u_0,u_1 的最大公因数 u_{k+1}. 那么，是否可以用 u_0,u_1 表示 u_{k+1}，即找到两个整数 s,t，使得 $u_{k+1}=su_0+tu_1$？

从辗转相除法的 $k+1$ 个式子我们不难得到

$$u_2=u_0-q_0u_1;\qquad (1)$$

$$u_3=u_1-q_1u_2;\qquad (2)$$

$$\cdots$$

$$u_{k-1}=u_{k-3}-q_{k-3}u_{k-2};\qquad (k-2)$$

$$u_k=u_{k-2}-q_{k-2}u_{k-1};\qquad (k-1)$$

$$u_{k+1}=u_{k-1}-q_{k-1}u_k.\qquad (k)$$

从第(k)式出发，依次将$(k-1)$式、$(k-2)$式……(1)式代入，则可以得出下面的结论

$$\begin{aligned}u_{k+1}&=u_{k-1}-q_{k-1}u_k\\&=u_{k-1}-q_{k-1}(u_{k-2}-q_{k-2}u_{k-1})\\&=-q_{k-1}u_{k-2}+(1+q_{k-1}q_{k-2})u_{k-1}\\&=-q_{k-1}u_{k-2}+(1+q_{k-1}q_{k-2})(u_{k-3}-q_{k-3}u_{k-2})\\&=(1+q_{k-1}q_{k-2})u_{k-3}-(q_{k-1}+q_{k-3}+q_{k-1}q_{k-2}q_{k-3})u_{k-2}\\&=\cdots\\&=su_0+tu_1\ .\end{aligned}$$

其中 s,t 均为由上述 k 个式子确定的整数.

也就是说，我们证明了如下定理

定理 3　对于任意不全为零的两个正整数 a,b，必存在整数 s,t，

使得

$$(a,b)=sa+tb.$$

特别地，当 a,b 互素时，必存在整数 s,t，使得 $sa+tb=1$.

推论　**若 $a\mid bc$，且 a,b 互素，则 $a\mid c$.**

证明　因为 a,b 互素，所以，存在整数 s,t，使得

$$sa+tb=1.$$

两端同乘 c，得

$$a(sc)+t(bc)=c.$$

因为 $a\mid a$ 且 $a\mid bc$，所以，$a\mid(a(sc)+t(bc))$，即 $a\mid c$. 命题得证.

应用这个推论，可以证明以下的事实：

若素数 $p\mid q_1q_2\cdots q_t$，其中 $q_1,q_2,\cdots,q_t$ 都是素数，则一定存在某个 q_i，使得 $p=q_i$.

事实上，如果 $p\neq q_1$，因为 p,q_1 都是素数，那么 p,q_1 互素，由推论知：$p\mid q_2q_3\cdots q_t$. 依此类推，必定有一个 q_i，使得 $p=q_i$.

例 4　已知 $(36,83)=1$，利用辗转相除法求出整数 s,t，使得 $36s+83t=1$.

解　先用辗转相除法写出下列式子

$$83=2\times36+11,$$
$$36=3\times11+3,$$
$$11=3\times3+2,$$
$$3=2+1.$$

所以，$1=3-2=3-(11-3\times3)=4\times3-11$

$=4\times(36-11\times3)-11=4\times36-13\times11$

$=4\times36-13\times(83-2\times36)=30\times36-13\times83$

由此求得　　$s=30,t=-13.$

辗转相除的过程也可用短除表示如下.

$$\begin{array}{r|l}
u_0=83 & 36=u_1 \\
72 & 2=q_0 \\
\hline
u_1=36 & 11=u_2 \\
33 & 3=q_1 \\
\hline
u_2=11 & 3=u_3 \\
9 & 3=q_2 \\
\hline
u_3=3 & 2=u_4 \\
2 & 1=q_3 \\
\hline
1=u_5 &
\end{array}$$

即 $11=83-36\times2$

即 $3=36-11\times3$

即 $2=11-3\times3$

即 $1=3-2\times1$

习 题 2—2

A 组

1. 为什么对两个相邻整数 n 与 $n+1$ 必有 $(n,n+1)=1$?
2. 求下列各对数的最大公因数.
   (1) 360 与 1 970;　　(2)30 与 365;
   (3) 530 145 与 165 186;　　(4)81 719 与 33 649.
3. 定理 3 的逆命题是否成立? 证明你的结论.
4. 若 a,b,n 均为正整数,求证:$(a^n,b^n)=(a,b)^n$.
5. 设 a,b,c 为 3 个整数,且 $a\neq 0$,b,c 不全为 0,试用辗转相除法证明:$(ab,ac)=a(b,c)$.

B 组

已知 a,b,c 为 3 个非零整数,且 $(a,b)=1$,求证 $(ac,b)=(c,b)$.

§3　算术基本定理

3.1　算术基本定理

前面我们已经知道：任意一个合数 a 必有素因数，记为 p_1，因此，存在整数 q_1，使得 $a=p_1q_1$，其中 $q_1<a$. 若 q_1 是素数，则 a 就表成了两个素数的乘积；若 q_1 是合数，则可以继续把 q_1 表成 p_2q_2 的形式，其中 p_2 为素数. 依次下去……由于 $a>q_1>q_2>\cdots>0$，所以，这个过程不可能无限进行下去. 于是，我们可以得出下面的算术基本定理：

定理 4　任一大于 1 的整数 a 能表成素数的乘积

$$a=p_1p_2\cdots p_s, \tag{1}$$

其中 p_i $(1\leqslant i\leqslant s)$ 是素数. 且在不计次序的意义下，表示式(1)是唯一的.

如　$100=2\times50=2\times2\times25=2\times2\times5\times5$.

这个表示式(1)的唯一性是需要证明的，下面我们就来证明这个表示式的唯一性.

证明　由于 p_i 不计次序，我们不妨设

$$a=p_1p_2\cdots p_s,\ p_1\leqslant p_2\leqslant\cdots\leqslant p_s.$$

若还有素数 $q_1,q_2,\cdots,q_t$，使得 $a=q_1q_2\cdots q_t$，$q_1\leqslant q_2\leqslant\cdots\leqslant q_t$. 则

$$p_1p_2\cdots p_s=q_1q_2\cdots q_t \tag{2}$$

下面我们首先来证明 $p_1=q_1$.

显然，$p_1\mid q_1q_2\cdots q_t$，由上一节的推论知，必存在 q_i，使得 $p_1=q_i$. 又因为 $q_1\leqslant q_i$，所以 $q_1\leqslant p_1$.

同理可证：$p_1\leqslant q_1$，所以 $p_1=q_1$.

由此可知 $p_2p_3\cdots p_s=q_2q_3\cdots q_t$. 同法可得 $p_2=q_2$，递推下去，则可得到 $t=s$，且 $p_i=q_i$，$i=1,2,\cdots,s$.

把(1)式中的相同素数的乘积写成幂的形式，即可得到

推论　任一大于 1 的正整数 a 能够唯一地写成

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}, \tag{3}$$

其中 α_i $(i=1,2,\cdots,s)$ 为正整数，p_1，p_2，…，p_s 为素数，且满足

$p_1 < p_2 < \cdots < p_s$.

式(3)称为 a 的标准素因数分解式.

例 1　把下列合数分解素因数,并写出其标准素因数分解式.

(1)120;　　(2)255.

解　(1)$120=2\times2\times2\times3\times5=2^3\times3\times5$;

(2)$255=3\times5\times17$.

例 2　试求所有小于 1 000,且与 1 000 互素的正整数的个数.

分析　因为 $1\,000=2^3\times5^3$,所以,与 1 000 互素的数,也就是与 2,5 均互素的数.

如图 2-2,从反面考虑,我们只需求出 1 000 以内 2 的倍数、5 的倍数以及 10 的倍数.

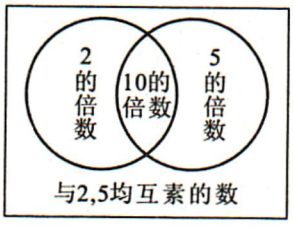


图 2-2

解　不大于 1 000 的正整数中,2 的倍数共有 $\frac{1\,000}{2}=500$ 个,5 的倍数共有 $\frac{1\,000}{5}=200$ 个,10 的倍数共有 $\frac{1\,000}{10}=100$ 个,所以,与 2,5 均互素的数的个数为

$$1\,000-(500+200-100)=400\text{ 个}.$$

一般地,我们用 $\varphi(m)$ 来表示所有小于正整数 m,且与 m 互素的正整数的个数. 例如,$\varphi(1\,000)=400$. 这是一个定义在正整数集合上的函数,通常称为**欧拉函数**. 有关欧拉函数的问题,我们将在第三章中进一步介绍.

练　习

1. 写出下列各数的标准素因数分解式.

   (1) 120;　　(2)365;　　(3)2 008.

2. 试求与 10 000 互素的 4 位数的个数.

3. 试求 $\varphi(6)$,$\varphi(11)$.

3.2　最小公倍数与算术基本定理的应用

学习算术基本定理之后，我们可以进一步认识约数与倍数. 那么，整数的最小公倍数是如何定义的呢?

给定 12,8 两个整数，我们知道，这两个整数的公共的倍数有 24，48,72,…其中，24 是这些公倍数中最小的正数，称之为 12 和 8 的最小公倍数.

定义　设 a,b 是两个整数，若整数 d 是它们所有公倍数中最小的一个正数，则称 d 为它们的**最小公倍数**，记作 $d=[a,b]$.

问题提出

不难知道：

$[2,3]=6$;　(1)

$[10,11]=110$;　(2)

$[4,6]=12$;　(3)

$[6,9]=18$.　(4)

从以上 4 个式子不难看出，当两个数的最大公约数等于 1 时，最小公倍数就等于这两个数的乘积，如(1)(2)两式；当两个数的最大公因数不等于 1 时，最小公倍数就不等于这两个数的乘积，如(3)(4)两式. 这就引发我们思考这样的问题：两个数的最小公倍数与最大公约数以及两个数的乘积之间存在怎样的关系?

实例分析

我们知道：$30=2^1\times3^1\times5^1$，$100=2^2\times5^2$.

可以发现：2,3,5 是 30 与 100 的所有素因数，我们不妨把 30 与 100 写成

$$30=2^1\times3^1\times5^1,100=2^2\times3^0\times5^2.$$

而 $(30,100)=10=2^1\times3^0\times5^1$，$[30,100]=300=2^2\times3^1\times5^2$.

对于素因数 2，在 30 和 100 中分别出现了 2^1 和 2^2，其中次数较高的 2^2 出现在最小公倍数 300 中，次数较低的 2^1 出现在最大公因数 10 中. 同样地，3^1，5^2 出现在最小公倍数中，3^0，5^1 出现在最大公因数中. 可以用图 2-3 表示.

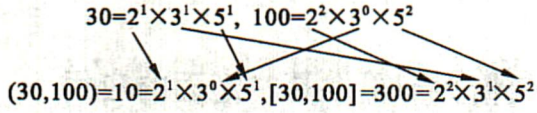


图 2-3

这样，我们就有$(30,100)\times[30,100]=10\times300=30\times100$.

抽象概括

由上面的例子可以看出：对于任意两个整数a,b，设$p_1,p_2,\cdots,p_s$是a和b的所有素因子，记$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s}$，其中$p_i$为素数，整数$\alpha_i,\beta_i\geqslant0$ $(i=1,2,\cdots,s)$，则

$(a,b)=p_1^{u_1}p_2^{u_2}\cdots p_s^{u_s}$，其中$u_i=\min(\alpha_i,\beta_i)$，$i=1,2,\cdots,s$；

$[a,b]=p_1^{v_1}p_2^{v_2}\cdots p_s^{v_s}$，其中$v_i=\max(\alpha_i,\beta_i)$，$i=1,2,\cdots,s$.

这里，$\min(\alpha_i,\beta_i)$表示α_i,β_i中最小的数，$\max(\alpha_i,\beta_i)$表示α_i,β_i中最大的数.

因此，可以得到：

定理 5　设 a,b 是两个正整数，则

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

特别地，当$(a,b)=1$时，$[a,b]=ab$.

例 3　求 39 与 93 的最大公因数和最小公倍数.

解　$(39,93)=3(13,31)=3$，所以，$[39,93]=\dfrac{39\times93}{3}=1\ 209$.

习 题 2—3

A 组

1. 利用最大公因数的性质求下列各组数的最大公因数.
   (1) 216 与 64；　　(2)2 400 与 14 000.
2. 求下列各组数的最大公因数与最小公倍数.
   (1) 48 与 84；　　(2)360 与 810；　　(3)1 260 与 3 150.
3. 求下列各数的标准素因数分解式.
   (1) 16 500；　　(2)1 452 990；　　(3)9 828.

4. 利用标准素因数分解式，求下列各组数的最大公因数与最小公倍数．

(1) 391 与 493；　　(2)209 与 665；　　(3)1 834 与 30 261.

5. 甲、乙两个班的学生人数分别是 54 人、48 人，为了上英语口语课，需要将每个班的同学都分成若干个学习小组，若要求两个班所有小组的人数都相同，则每个小组的人数最多是多少？这时，甲、乙两个班各被分成几个小组？

6. 在团体操表演过程中，要求在队伍变换成 10 行、15 行、18 行时队形都能成为长方形，问：参加团体操表演最少需要多少人？

B　组

1. 若 a,b,c 都是整数，且方程 $x^3+ax^2+bx+c=0$ 有有理数根．求证：这个根一定是整数.

2. 写出 1 200 的标准素因数分解式，并由此求出其所有正约数的个数.

阅读材料

费马数与梅森数

研究素数的性质是数论的核心问题之一，围绕素数在历史上有许多有趣的问题.

法国修道士梅森对于搜寻素数很投入，并且试图找出能产生所有素数的完美公式(今天知道，这是不可能的). 他曾经研究过形如 $M_n=2^n-1$(n 为正整数)的数. 在 1644 年出版的他的著作《物理数学随感录》的序言中，梅森宣称：对于 $n=2,3,5,7,13,17,19,31,67,127,257$，数 $M_n=2^n-1$ 是素数. 而对于所有小于 257 的其他素数 n，M_n 是合数.

他怎么会如此肯定地下此结论呢？无人知晓. 但人们却由此猜想：在这一类数中出现素数的机会可能比较多. 人们要寻找更大的新素数，往往就到这类数里去淘金. 为了纪念梅森，人们便把形如 2^n-1(n 为正整数)的素数称为梅森素数. 历史上，人们对于梅森素数的研究，花费了大量的时间和精力，迄今为止，人们已经知道：当 $n=2,3,5,7,13,17,19,31,127$ 时，$M_n=2^n-1$ 都是素数，但 M_{67} 却是一个合数.

发现 M_{67} 的因子的过程非常有趣. 1903 年，在美国纽约举行的一个报告会上，数学家科尔一言不发地走到黑板前，首先他计算了 2 的 67 次幂，将其结果再减去 1，然后他又把193 707 721和 761 838 257 287 相乘. 两次演算的答案竟然一模一样！最后他默默无声地回到自己的座位上，全体听众报以热烈的掌声.

在科尔报告之前，人们还指望 M_{67} 能被确定是一个大的素数. 科尔通过板演，告诉他的同行们，M_{67} 不是一个素数，而是一个有 21 位的合数，还具体求出了这个大合数的两个素因数. 在科尔的年代，还没有电子计算器，要靠手算得出这样的结果，非常不容易. 科尔为此用去了 3 年中所有的星期天.

现代的加密技术需要判断和找出大的素数，例如 50 位或者更高位数的素数；解密技术需要分解大数. 虽然理论上我们可以通过“筛法”逐一把素数找出来，也可以把任何一个大数分解素因数，但实际上，即使动用超级计算机，要想求出一个大的素数，例如 100 位以上的素数，也是非常困难的. 分解大数就更为困难.

人们通过研究还发现 M_{61}，M_{89}，M_{107} 也是合数. 1930 年，美国数学家 D. H. 莱默经过 700 个小时的艰苦努力终于验证 M_{257} 是合数. 到此为止，梅森的“猜想”全部被揭晓.

电子计算机的普及大大促进了梅森素数的研究：截至 2004 年，人们发现的最大的梅森素数为 $M_{24\,036\,583}$. 是否有无穷多个梅森素数是一个尚未解决的难题. 无疑，寻找梅森素数的活动还会进行下去，它不仅考验着人类的智慧，也促进着科技的发展.

另一个经典的问题是费马数.

费马年近30才开始认真研究数学,并且只是利用业余时间从事这种专业研究,然而这并不妨碍他在数学上取得累累硕果.费马不仅和笛卡儿同时发明了解析几何,在数论方面,他还完成了自己最伟大的工作.可以说,近代数论是从费马真正开始的,他是数论发展史上一个承前启后的人物.他具有非凡的直觉能力,提出了一批当时未被证明的"定理"(实际上是猜想),推动了近代数论的发展,因而他被称之为"近代数论之父".事实上,在高斯名著《算术研究》出版之前,数论的发展始终是跟费马的推动联系在一起的.如数学史家E. T. 贝尔所评价的:费马是一个第一流的数学家,一个无可指责的诚实的人,一个历史上杰出的算术学家.

1640年,费马发现形如 $F_n=2^{2^n}+1$ 的数,当 n 取0,1,2,3,4时,这个式子对应的值分别为3,5,17,257,65 537,都是素数.他猜想对所有的整数 n,"费马数" F_n 一定为素数.

进一步验证费马的猜想并不容易.因为随着 n 的增大,F_n 迅速增大.对后人来说,第一个需要检验的 $F_5=4\ 294\ 967\ 297$ 已经是一个10位数了.这个问题吸引了欧拉,1732年,年仅25岁的欧拉得出 $F_5=641\times 6\ 700\ 417$.这一结果意味着 F_5 是一个合数,因此证明费马的猜想是错的.

此后人们对更多的费马数进行了研究.随着电子计算机的发展,计算机成为数学家研究费马数的有力工具.但即使如此,在所知的费马数中竟然没有再添加一个费马素数.迄今为止,费马素数除了被费马本人所证实的那5个外竟然没有再发现一个!那么到底还有没有费马素数?人们开始猜想:在所有的费马数中,除了前5个是素数外,是否其他的都是合数.这就是今天的费马数猜想.

§4　不定方程

中国古代数学家张邱建曾经解答了下面的题目：

“鸡翁一，值钱五，鸡母一，值钱三，鸡雏三，值钱一. 百钱买百鸡. 问鸡翁、母、雏各几何?”

设用 x,y,z 分别代表鸡翁、鸡母、鸡雏的数目，就得到下面的方程

$$\begin{cases}5x+3y+\dfrac{1}{3}z=100,\\ x+y+z=100.\end{cases}$$

消去 z，再化简，即得

$$7x+4y=100.$$

形如这样的方程，称为**二元一次不定方程**. 要解决这个问题，就是要求出上述方程的非负整数解. 本节中，我们研究不定方程

$$ax+by=c(a,b,c\text{ 均为整数且 }ab\neq 0)$$

的整数解问题. 当常数项系数 $c=0$ 时，称上述方程为**齐次方程**.

说　明

本章中我们提到的不定方程，均指系数为整数的不定方程，其求解的问题也只研究整数解.

一方面，不定方程在历史上有极其丰富的研究，文献极其丰富，也留下了很多经典难题；另一方面，由于数学应用的空前普遍，方程及不等式的整数解问题研究，也有了很大的应用前景.

我们首先来研究这个二元一次不定方程整数解的存在性问题.

实例分析

请看下面的例子：

(1) $2x-4y=1$；

(2) $3x+2y=1$；

(3) $9x+3y=22$；

(4) $10x+2y=6$.

不难发现，因为方程 $2x-4y=1$ 的左边为 2 的倍数，而右边不能被 2 整除，所以，方程(1)无整数解；同理，方程 $9x+3y=22$ 的左边为 3 的倍数，而右边不能被 3 整除，所以，方程(3)也无整数解.

由此我们可以得出结论：

对于方程 $ax+by=c$，如果 $(a,b)\nmid c$，则方程无整数解.

另一方面，如果$(a,b)|c$，那么方程$ax+by=c$是否一定有整数解呢？

这个问题的回答是肯定的.

考虑方程(2)，$3x+2y=1$.

由于$(3,2)=1$，所以，根据辗转相除法，我们知道：必存在x_0,y_0，使得$3x_0+2y_0=1$（如$x_0=1,y_0=-1$），即方程$3x+2y=1$有整数解.

再来分析方程(4)，$10x+2y=6$.

由于$(10,2)=2$，所以，根据辗转相除法，必存在x_0,y_0，使得$10x_0+2y_0=2$（如$x_0=1,y_0=-4$），两边同乘3，得到$10\times 3x_0+2\times 3y_0=6$，所以，$(x,y)=(3x_0,3y_0)$就是方程$10x+2y=6$的一个整数解.

抽象概括

对于不定方程$ax+by=c$，a,b,c均为整数且$ab\neq 0$.

如果$(a,b)\nmid c$，则方程无整数解.

如果$(a,b)|c$，则方程一定有整数解. 根据辗转相除法可以知道：一定存在整数x_0，y_0使得$ax_0+by_0=(a,b)$，则$(x,y)=\left(\frac{cx_0}{(a,b)},\frac{cy_0}{(a,b)}\right)$就是方程$ax+by=c$的一组整数解.

例1　判断下列方程是否有整数解，若有解，试求出一个解.

(1) $7x+4y=100$；　　(2)$111x-321y=75$.

解　(1)因为$(7,4)=1$，且$1|100$，所以，方程$7x+4y=100$有整数解.

下面首先利用辗转相除法求出方程$7x+4y=1$的一个解. 作除法如下：

$$
\begin{array}{r|l}
u_0=7 & 4=u_1 \\
4 & 1=q_0 \\
\hline
u_1=4 & 3=u_2 \longrightarrow \text{即}3=7-4\times 1 \\
3 & 1=q_1 \\
\hline
 & 1=u_3 \longrightarrow \text{即}1=4-3\times 1
\end{array}
$$

从最后一式开始逐步代回，可得

$$1=4-3=4-(7-4)=(-1)\times 7+4\times 2.$$

由此得到方程$7x+4y=1$的一个整数解$\begin{cases}x=-1,\\ y=2.\end{cases}$所以$\begin{cases}x=-1\times 100=-100,\\ y=2\times 100=200\end{cases}$就是方程$7x+4y=100$的一个整数解.

(2) 因为(111,321)=3,且 3|75,所以,方程 $111x-321y=75$ 一定有整数解,且解与方程 $37x-107y=25$ 的完全相同.

因为(37,107)=1,下面利用辗转相除法求出方程 $37x-107y=1$ 的一个解. 作除法如下

$$
\begin{array}{r|l}
u_0=107 & 37=u_1 \\
74 & 2=q_0 \\
\hline
u_1=37 & 33=u_2 \quad \text{即} 33=107-37\times 2 \\
33 & 1=q_1 \\
\hline
u_2=33 & 4=u_3 \quad \text{即} 4=37-33\times 1 \\
32 & 8=q_2 \\
\hline
1=u_4 & \text{即} 1=33-4\times 8
\end{array}
$$

从最后一式开始逐步代回,可得

$$
\begin{aligned}
1 &= 33-4\times 8 \\
&= 33-(37-33)\times 8 \\
&= 33\times 9-37\times 8 \\
&= (107-37\times 2)\times 9-37\times 8 \\
&= 107\times 9-37\times 26.
\end{aligned}
$$

所以 $\begin{cases} x=-26, \\ y=-9 \end{cases}$ 就是方程 $37x-107y=1$ 的一个整数解,由此可得,$\begin{cases} x=-26\times 25=-650, \\ y=-9\times 25=-225 \end{cases}$ 就是方程 $111x-321y=75$ 的一个整数解.

练　习

判断下列不定方程是否有整数解. 若有解,试求出一个解;若无解,说明理由.

(1) $2x+3y=2$;　　(2) $2x+4y=5$;

(3) $3x-5y=2$;　　(4) $12x-20y=21$;

(5) $72x+157y=1$;　　(6) $133x-105y=217$.

问题提出

以上我们解决了二元一次不定方程整数解的存在性问题,并通过辗转相除法得到了方程的一个特解. 下面我们继续讨论:当二元一次不定方程有整数解时,如何找出所有的解?

分析理解

当方程 $ax+by=c(a,b,c$ 均为整数且 $ab\neq 0)$ 有解时,根据前面

的方法可以得到一个特解(x_0,y_0). 若(x_1,y_1)是此方程的任意一个解,则

$$ax_0+by_0=c,$$
$$ax_1+by_1=c.$$

两式相减得

$$a(x_0-x_1)+b(y_0-y_1)=0,$$

这两个解(x_0,y_0)与(x_1,y_1)的差(x_0-x_1,y_0-y_1)是齐次方程$ax+by=0$的解. 为了得到方程$ax+by=c$的所有解,我们只需求出齐次方程$ax+by=0$的所有解.

由$ax+by=0$可得

$$ax=-by.$$

两边同时除以(a,b),得

$$\frac{a}{(a,b)}x=\frac{-b}{(a,b)}y. \tag{1}$$

又因为$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$,所以,$\frac{a}{(a,b)}\mid y$,且$\frac{b}{(a,b)}\mid x$.

由此可知,必存在整数m,n使得

$$\begin{cases}x=m\cdot\dfrac{b}{(a,b)},\\ y=n\cdot\dfrac{a}{(a,b)}.\end{cases}$$

代入(1)可得　　$n=-m$.

这样,我们就得到了方程$ax+by=0$的所有整数解

$$\begin{cases}x=m\cdot\dfrac{b}{(a,b)},\\ y=-m\cdot\dfrac{a}{(a,b)}.\end{cases}$$

于是我们证明了下面的定理:

定理6　设二元一次不定方程

$$ax+by=c(a,b,c\text{ 均为整数且 }ab\neq0) \tag{2}$$

有一整数解$x=x_0,y=y_0$;又设$a_1=\frac{a}{(a,b)},b_1=\frac{b}{(a,b)}$,则(2)的一切整数解可以表示为

$$x=x_0-b_1m,\quad y=y_0+a_1m, \tag{3}$$

其中$m=0,\pm1,\pm2,\cdots$

到此为止,我们可以完整地解答张邱建的问题了.

根据例1,我们可以得到方程$7x+4y=100$的一个特解$x=-100,y=200$. 于是,方程的$7x+4y=100$的一切解可以表示为

$$x=-100-4m,y=200+7m,m=0,\pm1,\pm2,\cdots$$

由于 x,y,z 分别代表鸡翁、鸡母、鸡雏的数目，所以

$$x\geqslant0,y\geqslant0,z=100-x-y\geqslant0,$$

解得　$m=-28,-27,-26,-25.$

由此得到该问题的 4 组解为

$$\begin{cases}x=12,\\y=4,\\z=84;\end{cases}\quad\begin{cases}x=8,\\y=11,\\z=81;\end{cases}\quad\begin{cases}x=4,\\y=18,\\z=78;\end{cases}\quad\begin{cases}x=0,\\y=25,\\z=75.\end{cases}$$

例 2　求方程 $5x+3y=52$ 的所有正整数解.

解　不难看出：$x=-1,y=2$ 是方程 $5x+3y=1$ 的一个解，所以，$x=-52,y=104$ 是方程 $5x+3y=52$ 的一个解. 由定理可知：方程 $5x+3y=52$ 的所有解为

$$x=-52-3m,y=104+5m,m=0,\pm1,\pm2,\cdots$$

令 $x>0,y>0$，解得：$-20\frac{4}{5}<m<-17\frac{1}{3}$，所以，$m=-18,-19,-20$. 方程 $5x+3y=52$ 的所有正整数解为

$$\begin{cases}x=2,\\y=14;\end{cases}\quad\begin{cases}x=5,\\y=9;\end{cases}\quad\begin{cases}x=8,\\y=4.\end{cases}$$

信息技术应用

一、求 1 000 以内素数表的算法框图，如图 2-4 所示.

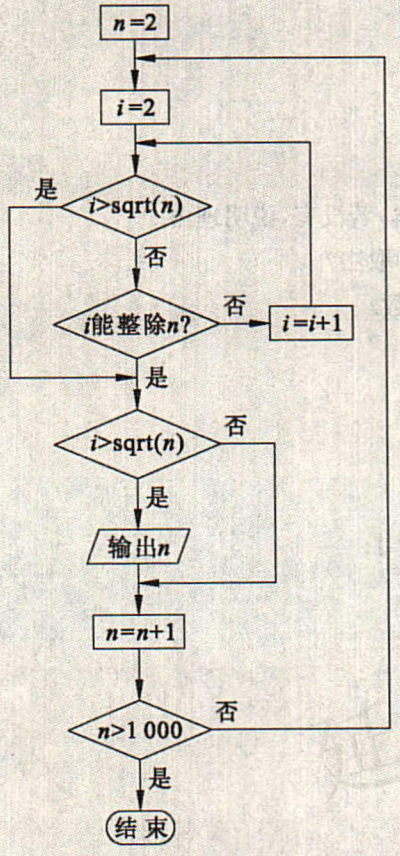


图 2-4

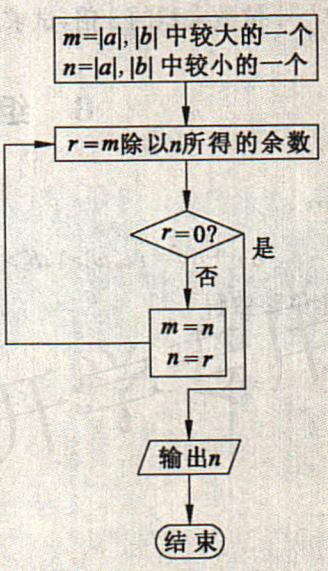


图 2-5

二、用辗转相除法求 a 与 b 的最大公因数的算法框图，如图 2-5 所示.

习 题 2—4

A 组

1. 解下列不定方程：

   (1) $15x+25y=100$；　　(2)$306x-360y=630$；

   (3) $7x+19y=213$.

2. 判断方程 $13x+21y=290$ 是否有正整数解. 若有，求出这个解；若没有，说明理由.

3. 取 1 分、2 分、5 分的硬币共 10 枚，组成 1 角 8 分钱，有多少种取法？

4. 某个两位数是其个位数与十位数乘积的 3 倍，试求这个两位数.

B 组

求证：二元一次不定方程

$$ax+by=N,a>1,b>1,(a,b)=1,$$

当 $N>ab-a-b$ 时有非负整数解.

复习题二

A　组

1. 判断 10 301，13 331，16 361，19 391 是素数还是合数.
2. 判断以下结论是否一定正确，对的给出证明，错的举出反例.

   (1)若$(a,b)=(a,c)$，则$[a,b]=[a,c]$；

   (2)若$(a,b)=(a,c)$，则$\frac{[a,b]}{b}=\frac{[a,c]}{c}$；

   (3)若$d\mid a,d\mid a^2+b^2$，则$d\mid b$；

   (4)若$a^4\mid b^2$，则$a\mid b$；

   (5)若$d\mid a^2+1$，则$d\mid a^4+1$；

   (6)若$d\mid a^2-1$，则$d\mid a^4-1$.
3. 设$n\in\mathbf{N}_+$，求$(21n+4,14n+3)$.
4. 求 198 和 252 的最大公约数，并根据辗转相除法，把它表成 198 与 252 的整系数的线性组合.
5. 给出 3 个整数，它们的最大公约数是 1，但任何两个整数的最大公约数都不等于 1.
6. 设$n\geqslant 1$，记$n!=1\times 2\times 3\times\cdots\times n$. 求证：$(n!+1,(n+1)!+1)=1$.
7. 求最大公约数：$(n-1,n^2+n+1)$.
8. 写出 20! 的标准素因子分解式.
9. 写出 180 的标准素因子分解式，并由此求出 180 的所有正的奇约数的个数.
10. 求$907x+731y=2\ 107$的所有整数解.
11. 求以下方程的所有正整数解.

    (1) $5x+7y=41$；　　(2)$7x+3y=123$.
12. 方程$63x+110y=6\ 893$有无正整数解？

B　组

1. 设m为大于 1 的正整数，且$m\mid(m-1)!+1$. 求证：m为素数.
2. 设$n\geqslant 0,F_n=2^{2^n}+1$. 证明：若$d>1$，且$d\mid F_n$，则对于任意正整数$m\neq n$，必有$d\nmid F_m$. 并由此推出素数有无穷多个.

第三章 同 余

在日常生活中，我们关注的常常不是某些整数本身，而是用这些数除以某一固定整数所得的余数，这就涉及数论中非常重要的一个概念——同余. 本章首先从同余的概念出发，介绍同余的基本性质及其应用，其中有一些是在算术和日常生活中的应用. 在此基础上，引出剩余类、完全剩余系、简化剩余系等概念. 最后引入同余方程组的概念. 本章还介绍了几个重要的定理：欧拉定理、费马定理及孙子定理.

§1 同余及其应用

问题提出

考虑这样一个问题：2004 年 9 月 10 日是教师节 20 周年，这一天是星期五，那么 9 月 17 日是星期几呢？9 月 24 日呢？我们数一下就可以得出这几天都是星期五. 这个现象很有意思，这中间有什么规律吗？

1.1 同 余

观察下面 3 组除式：

(1)	(2)	(3)
$5\div3=1\cdots\cdots2$, $8\div3=2\cdots\cdots2$, $11\div3=3\cdots\cdots2$, …	$4\div3=1\cdots\cdots1$, $7\div3=2\cdots\cdots1$, $10\div3=3\cdots\cdots1$, …	$3\div3=1\cdots\cdots0$, $6\div3=2\cdots\cdots0$, $9\div3=3\cdots\cdots0$, …

不难总结出下面的规律

1. 任意一个整数被 3 除，所得的余数只有 0，1，2 三种情况.

2. 每组除式中余数都相同.

3. 每组除式中，任意两个被除数的差都能被除数 3 整除.

……

为了准确地描述这些规律，我们引入同余的概念：

定义　给定一个正整数 m，我们把它叫作模. 如果 $a-b$ 能被 m 整除，我们说“两个整数 a，b 对模 m 同余”，记作 $a\equiv b(\mathrm{mod}\ m)$，读作“$a$ 与 b 对模 m 同余”. 如果 $a-b$ 不能被 m 整除，我们就说“a 与 b 对模 m 不同余”，记作 $a\not\equiv b(\mathrm{mod}\ m)$.

例如，$8-5$ 能被 3 整除，我们就说 8 与 5 对模 3 同余，记作 $8\equiv 5(\mathrm{mod}\ 3)$.

现在我们回到本节开始所提出的问题. 由于 9 月 17 日与 9 月 10 日相隔 7 天，9 月 24 日与 9 月 10 日相隔 14 天，而 $7\equiv 0(\mathrm{mod}\ 7)$，$14\equiv 0(\mathrm{mod}\ 7)$，所以这两天都是星期五；另一方面，若与 9 月 10 日相隔的天数与 0 对模 7 不同余，则这天一定不是星期五.

同余是数论中的一个非常重要的概念. 由以上定义可以知道，如果两个数对模 m 同余，则这两个数被 m 除所得的余数相同，即这两个数的差能被 m 整除：存在一个整数 k，使得 $a-b=km$. 用式子表示为

如果 $a\equiv b(\mathrm{mod}\ m)$，那么 $a-b=km$，即 $a=km+b$.

从某个角度来说，也可认为 b 是 a 被 m 除所得的“余数”. 这也反映出同余和带余除法之间的内在联系.

例 1　证明：若 m 是奇数，则 $m^2\equiv 1(\mathrm{mod}\ 8)$.

证明　因为 m 是奇数，所以可设 $m=2k+1$，其中 k 为整数，所以

$$m^2=(2k+1)^2=4k^2+4k+1.$$

因此有

$$m^2-1=4k^2+4k=4k(k+1).$$

而对于任何整数 k，k 和 $k+1$ 中一定有一个为偶数，所以 m^2-1 是 8 的倍数，即

$$m^2\equiv 1(\mathrm{mod}\ 8).$$

思考交流

任何一个平方数被 9 除，其余数可能是什么？

练　习

1. 1979 年 8 月 16 日是星期四，8 月 26 日是星期几呢？
2. 如果现在是早晨 9 点，那么，2 h 之前是几点呢？过 13 h 之后是几点？28 h之后呢？

1.2　同余的性质

处理整数问题时，同余符号在某种程度上比整除符号和除法算式要方便、快捷. 为了更好地应用同余符号，我们首先来学习同余的性质.

根据同余的定义，我们很容易得到性质

1. $a\equiv a(\mathrm{mod}\ m)$.
2. 如果 $a\equiv b(\mathrm{mod}\ m)$，那么 $b\equiv a(\mathrm{mod}\ m)$.
3. 如果 $a\equiv b(\mathrm{mod}\ m)$且 $b\equiv c(\mathrm{mod}\ m)$，那么 $a\equiv c(\mathrm{mod}\ m)$.

同余式与等式有很多类似的性质，类比于等式，我们可以思考下面的问题：

	因为6=6， 4=4， 所以6+4=6+4		若2≡5(mod 3)， 1≡4(mod 3)， 是否有2+1≡5+4(mod 3)
由	因为6=6， 4=4， 所以6×4=6×4	想一想：	若2≡5(mod 3)， 1≡4(mod 3)， 是否有2×1≡5×4(mod 3)
	因为6=6， 所以$6^2=6^2$		若2≡5(mod 3)， 是否有$2^2\equiv 5^2$(mod 3)

容易判断右面方框中问题的答案是肯定的. 一般地，我们可以得出性质

4. 若 $a\equiv b(\mathrm{mod}\ m)$，$c\equiv d(\mathrm{mod}\ m)$，则 $a+c\equiv b+d(\mathrm{mod}\ m)$.

证明　由 $a\equiv b(\mathrm{mod}\ m)$，$c\equiv d(\mathrm{mod}\ m)$，根据同余的定义可知

$$m\mid(a-b),\ m\mid(c-d),$$

根据整除的性质，有

$$m\mid[(a-b)+(c-d)],$$

也就是

$$m\mid[(a+c)-(b+d)],$$

即

$$a+c\equiv b+d(\mathrm{mod}\ m).$$

类似地，可以证明

5. 若 $a\equiv b(\bmod m)$，$c\equiv d(\bmod m)$，则 $ac\equiv bd(\bmod m)$.

6. 若 $a\equiv b(\bmod m)$，则 $a^n\equiv b^n(\bmod m)$.

7. 当 $c>0$ 时，若 $a\equiv b(\bmod m)$，则 $ca\equiv cb(\bmod cm)$；

若 $ca\equiv cb(\bmod cm)$，则 $a\equiv b(\bmod m)$.

同余式和等式的性质是否都是类似的呢？我们再思考下面的问题：

由 因为2×3=2×3，所以 3=3　想一想：若6×3≡6×8(mod 10)，是否有3≡8(mod 10)

想一想：若7×3≡7×13(mod 10)，是否有3≡13(mod 10)

显然，$3\not\equiv 8(\bmod 10)$，而 $3\equiv 13(\bmod 10)$，也就是说，同余式和等式的性质并不是完全相同的. 但在一定的条件下，同余式仍然能够保持“消去律”. 事实上可以证明：

8. 若 $ca\equiv cb(\bmod m)$，且 $(c,m)=1$，则

$$a\equiv b(\bmod m).$$

即当 c,m 互素时，同余式两边可约去 c.

证明　由 $ca\equiv cb(\bmod m)$ 可得 $m\mid c(a-b)$，

因为 $(c,m)=1$，根据整除的性质得 $m\mid(a-b)$，即为

$$a\equiv b(\bmod m).$$

例如：我们知道 $21\equiv 9(\bmod 2)$，而 21 和 9 有公约数 3，并且 $(3,2)=1$，所以，可在同余式两边同除以 3，就得到 $7\equiv 3(\bmod 2)$.

根据这个性质，我们也可以知道，由于 6 与 10 不互素，上面方框中右边第一个式子的答案是否定的.

思考交流

你还能根据等式的运算性质，找出同余式的其他运算性质吗？

例 2　试根据同余的性质说明若 $117\equiv 57(\bmod 10)$，则 $39\equiv 19(\bmod 10)$.

解　因为 $117=39\times 3$，$57=19\times 3$，而 $(3,10)=1$，根据性质 8 可知 $39\equiv 19(\bmod 10)$.

例 3　求 3^{406} 写成十进制数时的个位数.

解　因为 $3^4 \equiv 1 \pmod{10}$，

由性质 6 可得

$$3^{404} \equiv 1 \pmod{10}.$$

又因为 $3^2 \equiv 9 \pmod{10}$，

由性质 5 可得

$$3^{406} \equiv 3^{404} \times 3^2 \equiv 9 \pmod{10},$$

所以 3^{406} 写成十进制数时的个位数是 9.

练　习

1. 证明性质 6.
2. 3^{999} 写成十进制数时，最后一位数是什么？最后两位数是什么？

1.3　整除的判断与弃九法

问题提出

我们已经知道下面的结论：

在十进制中，

1. 一个整数能被 2 整除的充要条件是，这个整数的末位数字是一个偶数.

2. 一个整数能被 5 整除的充要条件是，这个整数的末位数字是 5 或 0.

那么，你知道这是为什么吗？

更进一步，你知道一个整数能被 3 整除的充要条件是什么吗？能被 9 整除的充要条件又是什么……

下面，我们尝试用同余的性质对整除的判断问题作出解释.

一、整除的判断

以 $3 \mid 237$ 为例.

我们知道：$237 = 2 \times 100 + 3 \times 10 + 7$.

因为 $10 \equiv 1 \pmod{3}$，所以 $30 \equiv 3 \pmod{3}$.

因为 $100 \equiv 1 \pmod{3}$，所以 $200 \equiv 2 \pmod{3}$.

根据同余的性质，可知 $200 + 30 + 7 \equiv 2 + 3 + 7 \pmod{3}$.

因此，我们知道，如果 2＋3＋7 能够被 3 整除，那么 200＋30＋7 就能够被 3 整除，而 2＋3＋7 恰好是 237 的各位数码之和.

仿照上面的分析，可以证明下面的一般规则：

一个整数能被 3 整除的充要条件是，它的各位数码之和能被 3 整除.

因为 $10\equiv 1(\mathrm{mod}\ 9)$，$10^n\equiv 1(\mathrm{mod}\ 9)$，仿照上面的推导，我们还可以得到下面的结论：

一个整数能被 9 整除的充要条件是，它的各位数码之和是 9 的倍数.

例 4　试判断 745 623 是否能被 9 整除.

解　因为 7＋4＋5＋6＋2＋3＝27，而 9|27，所以 745 623 能被 9 整除.

对于除数为 3 和 9 的情形，可以看到，问题解决的关键在于讨论 10^n 与除数的关系. 下面我们来探讨除数为 7，11，13 的情形.

当除数为 11 时，由于

$10\equiv -1(\mathrm{mod}\ 11)$，$100\equiv 1(\mathrm{mod}\ 11)$，$1\ 000\equiv -1(\mathrm{mod}\ 11)$，…

例如：121＝1×100＋2×10＋1，根据同余的性质有

$$100+20+1\equiv 1-2+1(\mathrm{mod}\ 11)\equiv 0(\mathrm{mod}\ 11).$$

可知 121 能被 11 整除.

所以，一个数能否被 11 整除，就归结为：这个数的奇数位数字之和与偶数位数字之和的差是否为 11 的倍数. 为方便，不妨规定从个位数字开始计数，即个位数字为第 1 位，十位数字为第 2 位……

仿照上面的方法，寻求一个整数能被 13 整除的方法.

二、弃九法

问题提出

小明是一个很马虎的孩子，下面的两个式子是他某次运算的结果，请你判断正误. 并尝试找到一种迅速判断正误的方法.

(1) $15\times23=345$；　　(2)$41\times20=810$.

动手实践

按照图 3-1 的要求，用(1)(2)两个式子的对应结果填空，然后观察左右两个蓝色方框之间有何规律 .

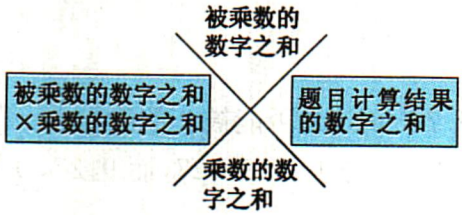


图 3-1

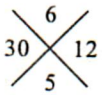


图 3-2

(1)按图 3-1 的要求对式子 $15\times23=345$ 的对应结果填空可得图 3-2.

通过计算和观察，我们发现计算结果正确，并且左右两个方框中的数对模 9 同余.

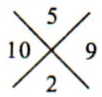


图 3-3

(2)按图 3-1 的要求对式子 $41\times20=810$ 的对应结果填空可得图 3-3.

这时我们发现计算结果不正确，并且左右两个方框中的数对模 9 不同余.

上面这个现象说明什么问题呢？通过分析，我们可以猜想：如果乘积计算正确，左右两个方框中的数对模 9 同余；如果乘积计算不正确，左右两个方框中的数对模 9 不同余. 下面我们一般地给出说明.

分析理解

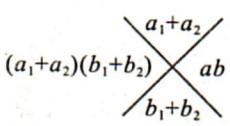


图 3-4

对于任意两个整数 a,b，设 $a=a_2\times10+a_1$，$b=b_2\times10+b_1$，按照图 3-1 的要求得到图 3-4.

而$\begin{cases}(a_1+a_2)(b_1+b_2)=a_1b_1+a_1b_2+a_2b_1+a_2b_2,\\ ab=a_1b_1+a_1b_2\times10+a_2b_1\times10+a_2b_2\times100.\end{cases}$

又 $10\equiv 1 \pmod 9$，所以 $a_1b_2\times 10+a_2b_1\times 10\equiv a_1b_2+a_2b_1 \pmod 9$，

$100\equiv 1 \pmod 9$，所以 $a_2b_2\times 100\equiv a_2b_2 \pmod 9$，

所以 $ab\equiv a_1b_1+a_1b_2+a_2b_1+a_2b_2 \pmod 9$.

因此，若 $ab\not\equiv (a_1+a_2)(b_1+b_2) \pmod 9$，则计算结果错误.

在实际计算时，根据 $9\equiv 0 \pmod 9$，验算时可以“逢 9 变 0”. 如

(1)$15\times 23=345$(见图 3-5)；

(2)$41\times 20=810$(见图 3-6)；

(3)$131\times 18=2\ 358$(见图 3-7).

图 3-5

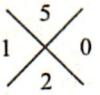


图 3-6

图 3-7

因此，这种验算结果的方法又称为“弃九法”. 需要特别强调的是，在验算乘积结果时，如果左右两个方框中的数关于 9 同余，也不能完全肯定乘积结果是正确的.

例 5　设 $a=67$，$b=35$，如果按照普通计算方法得到 a，b 的乘积为 $P=2\ 335$，这个结果是否正确？

解　根据弃九法可得

$$a\equiv 4 \pmod 9,\ b\equiv 8 \pmod 9,\ P\equiv 4 \pmod 9.$$

但 $4\times 8\not\equiv 4 \pmod 9$，故知计算有误.

问题与思考

想一想，这是为什么？

练　习

1. 试说明 3 能整除 12，123，12 345，但不能整除 1 234.
2. 探究一个整数能被 7 整除的方法.

习 题 3—1

A 组

1. 利用同余的性质证明：对于任何整数 n，$\frac{n(n+1)}{2}$ 的最后一位数不会出现 2，4，7，9.
2. 试证明若一整数的末两位数是 4(或 25)的倍数，则此整数是 4(或 25)的倍数.
3. 已知 7 位数 9 2□□ 427 是 99 的倍数，试求此数.
4. 给定一个整数 n，如 $n=2\ 374$，我们可以把它写成 $10a+b$ 的形式，这时 $a=237$，$b=4$. 我们要看它是否能被 7 整除，先看 $a-2b$ 是否能被 7 整除，如果可以的话，则 n 能被 7 整除. 请你试着用同余的性质来证明这个方法是正确的.
5. 用弃九法检查下列计算题的正确性.

(1) $764+997=1\ 761$；　　(2) $5\ 000-505=4\ 995$；

(3) $84\times86=7\ 224$；　　(4) $4\ 700\div25=188$.

B 组

1. 哪些整数 n 具有这样的性质：n 和 n^2 被 4 除后有相同的余数.
2. 给定一个整数 n，我们可以把它写成 $10a+b$ 的形式，如果 $a\equiv2b\pmod 7$. 求证：n 能被 7 整除.
3. 法国数学家费马在 1635 年曾经提出这样一个问题：如何找出 $5^{999\,999}$ 被 7 除后的余数，请你尝试解决这个问题.

提示：先观察 $5,5^2,5^3,5^4,\cdots$ 被 7 除后的余数，看看能找出什么规律.

§2　欧拉定理

2.1　剩　余　类

我们知道整数可以分为偶数和奇数，如图 3-8 所示，其中偶数为被 2 除余数为 0 的一类；奇数为被 2 除余数为 1 的一类. 类似地，我们还可以把整数按照被 3 除的余数进行分类，余数为 0 分作一类；余数为 1 分作一类；余数为 2 分作一类. 以上说明，整数可以有不同的分类方式，这就是我们下面要谈到的剩余类的问题.

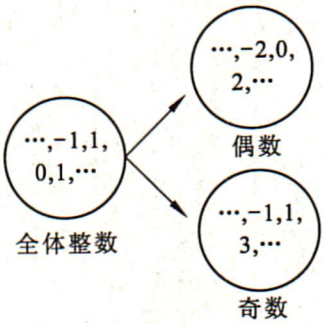


图 3-8

抽象概括

对于给定的模 m，全体整数可以按照对模 m 是否同余分成 m 个两两不相交的集合，使得在同一个集合中的任意两个整数对模 m 一定同余，而属于不同集合中的两个整数对模 m 一定不同余. 每一个这样的集合都称为是**模 m 的一个同余类**，或**模 m 的剩余类**. 我们以 $r \bmod m$ 表示 r 所属的模 m 的同余类，称 r 为所属的剩余类的代表.

根据剩余类的定义，我们知道整数可以分为模 2 的两个剩余类 $0 \bmod 2$ 和 $1 \bmod 2$；或分为模 3 的 3 个剩余类 $0 \bmod 3$，$1 \bmod 3$ 和 $2 \bmod 3$. 我们知道整数还可以按照模 4、模 5、模 6 等分为不同的剩余类.

在某种意义上，每个剩余类都可以用一个整数来代表，于是，整数的集合就可以用几个有限的整数来代表. 类比数的运算法则，我们可以为剩余类定义运算法则，下面我们给出剩余类的加法和乘法运算.

我们以模 5 的剩余类为研究对象进行说明：

模 5 的剩余类有：

$$0 \bmod 5, 1 \bmod 5, 2 \bmod 5, 3 \bmod 5, 4 \bmod 5.$$

我们从 $2 \bmod 5$ 和 $4 \bmod 5$ 中各选择一个元素，例如 2 和 4，那么

$$2+4 \equiv 1 \pmod 5,$$

所以 2+4 一定属于 1 mod 5，据此，我们可以定义

$$2 \bmod 5+4 \bmod 5=(2+4) \bmod 5.$$

亦即

$$2 \bmod 5+4 \bmod 5=1 \bmod 5;$$

类似地，定义

$$2 \bmod 5 \times 4 \bmod 5=(2 \times 4) \bmod 5.$$

根据同余的性质可知 $(2\times4)\bmod 5=8 \bmod 5=3 \bmod 5$，

即

$$2 \bmod 5 \times 4 \bmod 5=3 \bmod 5.$$

例 1　根据上面剩余类的运算定义，计算 $3 \bmod 6 \times 2 \bmod 6$.

解　根据剩余类的乘法定义，我们知道

$$3 \bmod 6 \times 2 \bmod 6=(3 \times 2) \bmod 6=0 \bmod 6.$$

剩余类的加法和乘法运算，与数的加法和乘法运算有什么异同？

从以上讨论可以看到，剩余类的运算可以归结为代表元的运算，代表元的性质决定了剩余类的性质，因此，我们给出如下定义：

定义　若 m 个整数，其中任何两数都不在同一个剩余类里，则这 m 个整数叫作模 m 的一个完全剩余系.

例如　0,1 是模 2 的一个完全剩余系；

0,4,8 是模 3 的一个完全剩余系；

0,5,10,15 是模 4 的一个完全剩余系；

……

$0,1,2,\cdots,m-1$ 是模 m 的一个完全剩余系.

通常我们取 $0,1,2,\cdots,m-1$ 作为模 m 的一个完全剩余系.

练　习

1. 利用剩余类的知识判断：n^2 被 9 除的余数可能是什么？并证明你的结论.
2. 计算 $(3 \bmod 7+5 \bmod 7) \times (2 \bmod 7)$.

2.2　欧拉定理·费马小定理

我们在第二章第三节曾经提到过欧拉函数 $\varphi(m)$，它是指不大于 m 而和 m 互素的正整数的个数. 例如，

不大于 1 而与 1 互素的正整数有 1 个，$\varphi(1)=1$；

不大于 2 而与 2 互素的正整数有 1 个，$\varphi(2)=1$；

不大于 3 而与 3 互素的正整数有 2 个，$\varphi(3)=2$；

不大于 4 而与 4 互素的正整数有 2 个，$\varphi(4)=2$；

……

考虑模 6 的剩余类 0 mod 6，1 mod 6，2 mod 6，3 mod 6，4 mod 6，5 mod 6，其中剩余类 1 mod 6，5 mod 6 里的所有的数均与 6 互素，我们称这两个剩余类为与 6 互素的剩余类.

抽象概括

给定模 m，如果模 m 的一个剩余类里面的某个数与 m 互素，就把这个剩余类叫作**一个与模 m 互素的剩余类**.

因此，在模 3 的剩余类中，1 mod 3，2 mod 3 为与 3 互素的剩余类，在模 4 的剩余类中，1 mod 4，3 mod 4 为与 4 互素的剩余类，等等.

我们知道，1 mod 6，5 mod 6 为所有与 6 互素的剩余类，那么我们在这两个剩余类中任取一个数，例如 1 和 5，则由这两个数组成的集合{1,5}，称为模 6 的一个简化剩余系.

定义　在与模 m 互素的全部剩余类中，从每一类中任取一数所组成的数的集合，叫作模 m 的一个简化剩余系.

不难得到：与模 m 互素的剩余类的个数是 $\varphi(m)$，模 m 的每一简化剩余系是由与 m 互素的 $\varphi(m)$ 个对模 m 不同余的整数组成的.

思考交流

如果 $a_1,a_2,\cdots,a_{\varphi(m)}$ 是模 m 的一个简化剩余系，并且 $(a,m)=1$，那么 $aa_1,aa_2,\cdots,aa_{\varphi(m)}$ 也是模 m 的一个简化剩余系.

例 2　求值：$\varphi(2)$，$\varphi(4)$，$\varphi(8)$，$\varphi(16)$，$\varphi(32)$，$\varphi(64)$，

$\varphi(128)$，$\varphi(256)$.

解　$\varphi(2)=1$，　$\varphi(4)=2$，　$\varphi(8)=4$，　$\varphi(16)=8$，
$\varphi(32)=16$，　$\varphi(64)=32$，　$\varphi(128)=64$，$\varphi(256)=128$.

例 3　若 p 为素数，试求 $\varphi(p)$ 的值.

解　任何一个小于 p 的整数均与 p 互素，所以 $\varphi(p)=p-1$.

下面我们利用简化剩余系的性质来证明数论中两个著名的定理.

欧拉定理　**设 m 是一个大于 1 的整数，a 是一个整数，且满足条件 $(a,m)=1$，则有**

$$a^{\varphi(m)}\equiv 1 \pmod m.$$

证明　设 $a_1=1<a_2<\cdots<a_{\varphi(m)}$ 是不大于 m 且和 m 互素的全部正整数.

由于 $\{a_1,a_2,\cdots,a_{\varphi(m)}\}$ 是模 m 的一个简化剩余系，且由 $(a,m)=1$，由性质 8，$aa_1,aa_2,\cdots,aa_{\varphi(m)}$ 两两对模 m 不同余. 还可以证明(习题 2—2 B 组)任意 aa_j 与 m 互素. 因此 $\{aa_1,aa_2,\cdots,aa_{\varphi(m)}\}$ 也是模 m 的一个简化剩余系. 从而 $aa_1,aa_2,\cdots,aa_{\varphi(m)}$ 中的每一个 aa_j 必和 $a_1,a_2,\cdots,a_{\varphi(m)}$ 中的某一个 a_k 模 m 同余，且当 aa_j 不同时对应的 a_k 也不同. 所以

$$\begin{aligned} &a(aa_2)\cdots(aa_{\varphi(m)})\\ \equiv\ &a_2\cdots a_{\varphi(m)} \pmod m, \end{aligned}$$

进而得到

$$\begin{aligned} &a(aa_2)\cdots(aa_{\varphi(m)})\\ =\ &a^{\varphi(m)}a_2\cdots a_{\varphi(m)}\\ \equiv\ &a_2\cdots a_{\varphi(m)} \pmod m. \end{aligned}$$

因为 $a_2,\cdots,a_{\varphi(m)}$ 与 m 互素，所以

$$a^{\varphi(m)}\equiv 1 \pmod m.$$

例 4　求 3^{364} 的末两位数码.

解　本题相当于求 3^{364} 模 100 的余数.

由欧拉定理知 $3^{\varphi(100)}\equiv 1 \pmod{100}$，又 $\varphi(100)=40$，故有 $3^{40}\equiv 1 \pmod{100}$，从而

$$3^{364}\equiv 3^4\equiv 81 \pmod{100}.$$

故 3^{364} 末两位数码为 81.

在欧拉定理中，若 m 是素数 p，由 $\varphi(p)=p-1$ 便得到

费马小定理　设 p 为素数，且 $(p,a)=1$，则有

$$a^{p-1}\equiv 1 \pmod{p}.$$

练　习

1. 试求 $\varphi(31)$ 的值.
2. 证明 $2\,222^{5\,555}+5\,555^{2\,222}$ 被 7 整除.

阅读材料

公开密钥——RSA 体制

20 世纪 50 年代以来，通信技术获得了迅速发展，通信逐渐进入数字通信和网络通信时代．保密通信已不仅是政治、军事的需要，也是经济活动、管理活动、人们日常生活的需要．保密通信的范围更为广泛，同时产生了许多新问题．

传统的保密通信中，通信的每一对发方和收方都要拥有一对密钥：加密密钥 E 和解密密钥 D．发方将信息 x 送给收方以前，先将加密密钥 E 作用于 x，得到密文 $y=E(x)$；收方收到 y 后，用解密密钥 D 作用于 y，而得到 $x=D(y)$．过程如图 3-9 所示.

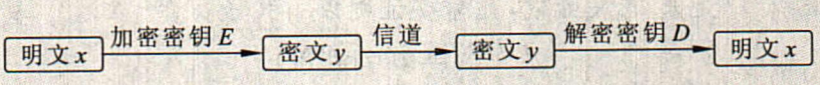


图 3-9

因此，E 和 D 是两个互为“反函数”的函数：$D(E(x))=E(D(x))=x$．

如果知道 D 和 E 其中的一个，可以很容易求出另一个，那么，D 和 E 就都需要保密．在这种情况下，一个公司和 N 个用户通信，公司就要保存 N 对加密和解密的密钥．如果有2 000个用户 A_k $(1\leqslant k\leqslant 2\,000)$ 彼此通信都需要保密，就需要 $2\,000\times 1\,999\div 2=1\,999\,000$ 对密钥，每个用户需要保存1 999对密钥．大量密钥的保存、更换和管理是一个严峻的问题，这个问题一直是通信界需要解决的基本问题.

1976 年，美国数学家和计算机专家 Diffie 和 Hellman 提出一种新的保密体制——公开密钥体制，很好地解决了大量密钥保存和数字签名问题，很快被应用到

信息安全的各种领域.

建立公开密钥问题的关键是用到数学中的一些单向函数.

如果知道加密密钥 E,但是很难求出或者在一段时间内无法求出解密密钥 D,通常我们把这样的加密运算(函数)E 称作“单向”(one way)函数.

当单向函数作为加密密钥时,即使把加密密钥(单向函数)E 公布于众,任何人得到用加密密钥 E 加密的信息,也无法破解它的含义. 这就是公开密钥的工作原理.

在通信上,理想的单向函数 E 需要满足:用现有最好的计算机(硬件)和已研制出来的最好算法(软件),在规定的保密时间内无法求出 E 的反函数 D.

在公开密钥体制中,所有用户的加密密钥 E 都是单向函数,可以公开,叫作公钥,像电话本一样编制成册(公钥簿),任何人都可查看. 每个用户只需保留自己的解密密钥 D,被称为私钥.

1977 年美国麻省理工学院(MIT)教授 R. Rivest, A. Shamir 和 L. Adleman 依据 Diffie 和 Hellman 的设想,提出了一个公开密钥体制. 它利用了数论的知识,建立了一类单向函数. 这种公开密钥体制被称为 RSA. 我们现在介绍这种体制的基本原理.

设 p,q 是两个不同的大素数,例如位数超过 100;$N=pq$;e,d 满足关系:$ed\equiv 1(\mathrm{mod}\ \varphi(N))$,其中 $\varphi(N)$ 是 N 的欧拉函数值. 这里加密密钥 E 和解密密钥 D 分别是

$$E(x)=x^e(\mathrm{mod}\ N),\text{其中 } 0\leqslant E(x)\leqslant N-1 \tag{1}$$

$$D(y)=y^d(\mathrm{mod}\ N),\text{其中 } 0\leqslant D(y)\leqslant N-1 \tag{2}$$

对于每一个信息 a,我们有

$$D(E(a))\equiv a^{ed}\equiv a^{1+k\varphi(N)}.$$

要肯定函数 D 是 E 的反函数,还需要证明以下式子:

$$a^{1+k\varphi(N)}\equiv a(\mathrm{mod}\ N) \tag{3}$$

当 $(a,N)=1$ 时,由欧拉定理知道(3)是成立的. 但是 a 不一定与 N 互素,还需要进一步的证明. 有兴趣的同学可以参考数论和信息安全方面的书.

现在还需要说明由(1)定义的 E 是单向函数. 显然它是由 e 和 N 给出的,要想由 E 求 D,就是要由 e 和 N 求 d. 由于 $ed\equiv 1(\mathrm{mod}\ \varphi(N))$,所以就必须知道 $\varphi(N)$. 求 $\varphi(N)$ 就需要知道 N 的素因子 p,q. 当 p,q 的位数很大时,例如上述 p,q 的位数超过 100,按照现有的数学方法,加上现有的超级计算机,也不可能在限定时间内通过分解 N 知道 p,q 的值,从而求出 $\varphi(N)$,因而也不可能知道 d. 这就说明 E 是单向函数.

关于 RSA 的保密性能,在历史上有一个有趣的故事,通过它揭示了一些有关的问题. 1977 年 RSA 的设计者用一个 129 位的数 N 和一个 4 位数 e 对一个关于秃鹰

的消息在RSA中加密，即所谓的RSA-129. 还悬赏100美元，奖给第一个破译该密码的人. 他们认为按照当时计算机的速度，估计分解这个129位的数大约要花23 000年. 计算速度提高可能会降低一两个数量级，但是安全性似乎仍然相当有保证. 然而出乎他们的预料，仅仅在17年之后，就有人解决了这个问题. 解决这个问题的核心思想在于发明了一种新的筛法——二次筛法. 这种新算法还有一个优点是能将工作分散到不同的计算机上去做. 人们组织了大约有600多人的因子分解迷，经过8个月的努力，找到了RSA-129的分别为64位和65位的两个素因数.

但是，RSA-129分解的成功，甚至包括数学家们近年来不断创造的诸多新算法，例如二次筛法、数域筛法、椭圆曲线算法，目前还不足以威胁RSA体制的安全性. 因子分解在一个长时期内仍然是个难题.

当今信息时代，保密通信不仅提出了密钥管理问题，还提出了一系列其他的重要的问题，这些统称为信息安全问题. 数论的方法在其中发挥了重要的作用.

通过上面对信息安全的简单介绍，可以说明以下两个重要的事实：

(1)在高技术中，即使像数论这样被认为是很抽象、“纯粹”而且古老的数学也会起重大的作用；

(2)数学的作用已经不仅仅是科学的基础和工具，而且发展成可以直接开发技术，为生产直接创造价值.

习 题 3—2

A 组

1. 证明每一个整数至少满足下列同余式中的一个：
   $x\equiv 0 \pmod 2$，$x\equiv 0 \pmod 3$，$x\equiv 1 \pmod 4$，$x\equiv 5 \pmod 6$，$x\equiv 7 \pmod{12}$.
2. 求出 243^{402} 的最后 3 位数字.
3. 某个一位数的 13 次幂的个位数是 7，求这个一位数.
4. 求 7^{7^7} 的末位数字.
5. 若正整数 a，b 与 5 460 互素，求证：$a^{12}-b^{12}\equiv 0 \pmod{5\,460}$.

B 组

1. 1732 年，著名数学家欧拉说：“我从一个优美的定理推出某一结果，我虽不会证明它，但我肯定它是正确的：若 a 和 b 均不能被素数 $n+1$ 整除，则 a^n-b^n 可被 $n+1$ 整除.”试证之.
2. 设 a 为正整数，如果今天是星期天，请问经过 a^{2^3} 天后是星期几？
3. 利用费马小定理证明：p 和 $8p^2+1$，除了 $p=3$ 以外，不能够同时为素数.

§3 同余方程(组)

在代数中,含有未知数的等式叫作方程. 同样地,我们把含有未知数 x 的同余式

$$f(x)\equiv 0 \pmod m \tag{1}$$

(其中 $f(x)$是整系数多项式)称为**模 m 的同余方程**.

本节我们研究一次同余方程和方程组的解.

3.1 同余方程(组)

什么是同余方程的解呢?

类似于代数中方程解的定义,可以作如下定义:

设整数 c 满足

$$f(c)\equiv 0 \pmod m,$$

显然,此时剩余类 $c \pmod m$ 中的任一整数满足上述同余式. 于是,我们称剩余类 $c \pmod m$ 是同余方程(1)的一个解,这个解记为

$$x\equiv c \pmod m.$$

当 c_1, c_2 均满足同余方程(1)且对 m 不同余时,我们就称 $c_1 \pmod m, c_2 \pmod m$ 为同余方程(1)的不同的解.

下面我们首先来研究一次同余方程的解.

设 $m\nmid a$,模 m 的一次同余方程为

$$ax\equiv b \pmod m. \tag{2}$$

如果同余方程(2)有解 $x_1 \pmod m$,则有某个整数 y_1 使得

$$ax_1 = b + my_1. \tag{3}$$

反之,若 x_1, y_1 是(3)的解,则 $x_1 \pmod m$ 是(2)的解.

(3) 是关于 x_1, y_1 的不定方程,由第二章 §4 的知识,我们知道(3)有解的充要条件是

$$(a,m)\mid b.$$

因此,方程(2)有解的充要条件是

$$(a,m)\mid b. \tag{4}$$

例 1 找出同余方程 $15x\equiv 7 \pmod{44}$ 的一个解.

解　设 $x\pmod{44}$ 是方程的一个解，则存在整数 y 使得

$$15x-44y=7,$$

解此不定方程，很容易得到一个解 $(21,7)$.

所以 $x\equiv 21\pmod{44}$ 是同余方程 $15x\equiv 7\pmod{44}$ 的一个解.

当 $m\nmid a$ 时，模 m 的一次同余方程 $ax\equiv b\pmod{m}$ 有解的充要条件是 $(a,m)\mid b$.

例如，对于同余方程

$$4x\equiv 2\pmod{8}.$$

因为 $(4,8)=4\nmid 2$，所以方程无解.

事实上，对于任何一个整数 x，$4x$ 或者能被 8 整除，或者被 8 除余数为 4，不可能余数为 2.

考虑同余方程

$$3x\equiv 2\pmod{8}.$$

因为 $(3,8)=1$，满足条件(4)，所以该同余方程有解. 事实上，$x\equiv 6\pmod{8}$ 就是方程的一个解.

定义　**我们把含有未知数 x 的一组同余式**

$$f_j(x)\equiv 0\pmod{m_j},(1\leqslant j\leqslant k),\tag{5}$$

称为同余方程组(其中 $f_j(x)(1\leqslant j\leqslant k)$ 是整系数多项式).

给定同余方程组 $\begin{cases}x\equiv 1\pmod 5,\\ x\equiv 2\pmod 3,\end{cases}$

不难看出

$$\cdots,6,11,16,21,26,\cdots$$

是满足 $x\equiv 1\pmod 5$ 的所有整数；

$$\cdots,5,8,11,14,17,20,23,26,\cdots$$

是满足 $x\equiv 2\pmod 3$ 的所有整数. 由此我们可以找到满足同余方程组

$$\begin{cases}x\equiv 1\pmod 5,\\ x\equiv 2\pmod 3\end{cases}$$

的所有整数

$$\cdots,11,26,\cdots$$

我们把满足同余方程组 $\begin{cases}x\equiv 1\pmod 5,\\ x\equiv 2\pmod 3\end{cases}$ 的所有整数称为该方程组的解.

抽象概括

若整数 c 同时满足同余方程组

$$f_j(c)\equiv 0(\bmod m_j),\ (1\leqslant j\leqslant k),$$

则称 c 是**同余方程组的解.**

练　习

1. 判断下面同余方程是否有解. 如果有解,请找出一个解.

(1) $3x\equiv 7(\bmod 11)$;　　(2) $4x\equiv 2(\bmod 12)$.

2. 试判断 $x=2$ 和 $x=1$ 是否均为同余方程 $x^3+x+1\equiv 0(\bmod 3)$ 的解.

3.2　孙子定理

问题提出

对于同余方程组 $\begin{cases} x\equiv 1(\bmod 3), \\ x\equiv 2(\bmod 5), \end{cases}$ 你能求出它的一个解吗?

首先考虑方程 $x\equiv 1(\bmod 3)$,我们知道 1,4,7,10,…均为它的解,我们从这些数中再找出满足第 2 个方程 $x\equiv 2(\bmod 5)$ 的一个解即可. 很容易得出 7 即为满足第 2 个方程的一个解. 因此 7 为上述同余方程组的一个解.

那么,我们很容易想到一个问题:上面这个同余方程组除了 7 还有其他的解吗? 对于任意一个同余方程组,我们有没有一个一般的方法来求解呢? 这就是我们本节要解决的主要内容.

在我国古代著名的数学著作《孙子算经》(纪元前后)里提出了这样的一个问题:“今有物不知其数,三三数之剩二,五五数之剩三,七七数之剩二,问物几何?”“答曰:二十三.”

孙子给出解法:“术曰:三三数之剩二,置百四十;五五数之剩三,置六十三;七七数之剩二,置三十,并之,得二百三十三,以二百一十减之即得.”

所谓“孙子定理”,便是蕴涵在这解法中的数学原理. 它要解决的问题的一般形式是:

“已知 m_1,m_2,m_3 是两两互素的正整数，求最小正整数 x，使它被 m_1,m_2,m_3 除所得余数分别为 a_1,a_2,a_3.”

这个问题的实质就是要求解同余方程组

$$x\equiv a_1(\bmod m_1),x\equiv a_2(\bmod m_2),x\equiv a_3(\bmod m_3).$$

孙子定理的求解思想是：

第一步：找一个被 m_1 除余 1 而被另两个数 m_2,m_3 整除的数 x_1，即解同余方程组

$$x_1\equiv 1(\bmod m_1),x_1\equiv 0(\bmod m_2),x_1\equiv 0(\bmod m_3). \tag{1}$$

这样，就有

$$a_1x_1\equiv a_1(\bmod m_1),a_1x_1\equiv 0(\bmod m_2),a_1x_1\equiv 0(\bmod m_3).$$

第二步：找一个被 m_2 除余 1 而被另两个数 m_1,m_3 整除的数 x_2，即解同余方程组

$$x_2\equiv 0(\bmod m_1),x_2\equiv 1(\bmod m_2),x_2\equiv 0(\bmod m_3). \tag{2}$$

这样，就有

$$a_2x_2\equiv 0(\bmod m_1),a_2x_2\equiv a_2(\bmod m_2),a_2x_2\equiv 0(\bmod m_3).$$

第三步：找一个被 m_3 除余 1 而被另两个数 m_1,m_2 整除的数 x_3，即解同余方程组

$$x_3\equiv 0(\bmod m_1),x_3\equiv 0(\bmod m_2),x_3\equiv 1(\bmod m_3), \tag{3}$$

这样，就有

$$a_3x_3\equiv 0(\bmod m_1),a_3x_3\equiv 0(\bmod m_2),a_3x_3\equiv a_3(\bmod m_3).$$

那么 $a_1x_1+a_2x_2+a_3x_3$ 即为满足该同余方程组的一个解.

由于要求的是符合条件的正整数中最小的正整数，故将上面的解 $a_1x_1+a_2x_2+a_3x_3$ 减去 $m_1m_2m_3$（记为 m）的整数倍（0,1,2,…）即可.

在第一步中，如何求解同余方程组(1)呢？

由于要求 x_1 满足 $x_1\equiv 0(\bmod m_2),x_1\equiv 0(\bmod m_3)$. 所以 x_1 一定是 m_2m_3（记为 M_1）的倍数（因为 $(m_2,m_3)=1$），即 $x_1=M_1'M_1$，其中 M_1' 是一个整数. 于是问题化成求 M_1'，使得 $M_1'M_1\equiv 1(\bmod m_1)$.

类似地，在第二步中要求 M_2' 使得 $M_2'M_2\equiv 1(\bmod m_2)$（其中 M_2 表示 m_1m_3）；在第三步中要求 M_3' 使得 $M_3'M_3\equiv 1(\bmod m_3)$（其中 M_3 表示 m_1m_2）.

对于上面《孙子算经》里的问题，其解法可以列表，如表 3-1.

表 3-1

m_k（除数）	a_k（余数）	最小公倍数	M_k（衍数）	M_k'（乘率）	$M_kM_k'a_k$（各总）	答　数	最小答数
3	2	3×5×7=105	5×7	2	2×70	2×70+3×21+2×15=233	233−2×105=23
5	3		3×7	1	3×21		
7	2		3×5	1	2×15		

把上面的结果加以推广，即为

定理(孙子定理)　设 $m_1,m_2,\cdots,m_k$ 是两两互素的正整数. 那么，对任意整数 $a_1,\cdots,a_k$，一次同余方程组

$$x\equiv a_j \pmod{m_j},(1\leqslant j\leqslant k), \tag{1}$$

必有唯一解.

事实上，同余方程组(1)的解是

$$x\equiv M_1M'_1a_1+M_2M'_2a_2+\cdots+M_kM'_ka_k \pmod m, \tag{2}$$

这里，$m=m_1m_2\cdots m_k$，$m=m_jM_j(1\leqslant j\leqslant k)$，$M'_j$是满足

$$M_jM'_j\equiv 1 \pmod{m_j},(1\leqslant j\leqslant k) \tag{3}$$

的一个整数(即是 M_j 对模 m_j 的逆).

我们把这个方法也列表，如表 3-2.

表 3-2

除数	余数	最小公倍数	衍数	乘率	各总	答数
m_1	a_1	$m=m_1m_2\cdots m_k$	M_1	M'_1	$M_1M'_1a_1$	$x\equiv M_1M'_1a_1+\cdots+M_kM'_ka_k \pmod m$
m_2	a_2		M_2	M'_2	$M_2M'_2a_2$	
…	…		…	…	…	
m_k	a_k		M_k	M'_k	$M_kM'_ka_k$	

这个算法在我国有许多名称，如“韩信点兵”“鬼谷算”“隔墙算”“剪管术”“神奇妙算”等，题目与解法均载于《孙子算经》中. 一般认为这是三国或晋时的著作，比刘邦生活的年代要晚近 500 年. 算法口诀诗则载于明朝程大位的《算法统宗》，诗中数字隐含的口诀我们前面已经解释了. 宋朝的数学家秦九韶把这个问题推广，并把解法称为“大衍求一术”. 这个解法传到西方后，被称为“中国剩余定理”.

例 2　求 3 除余 2，5 除余 3，7 除余 4 的最小正整数.

解　这里$m_1=3,m_2=5,m_3=7$；

$a_1=2,a_2=3,a_3=4.$

易求得

$$M_1M'_1=2\times(5\times7)=70,$$
$$M_2M'_2=1\times(3\times7)=21,$$
$$M_3M'_3=1\times(3\times5)=15.$$

故所求的正整数为

$$a_1M_1M'_1+a_2M_2M'_2+a_3M_3M'_3-2\times3\times5\times7$$
$$=2\times70+3\times21+4\times15-210$$

$=53$.

例 3　韩信点兵　有兵一队，若列成五行纵队，则末行一人；成六行纵队，则末行五人；成七行纵队，则末行四人；成十一行纵队，则末行十人．求兵数.

解　这里$m_1=5, m_2=6, m_3=7, m_4=11$；

$a_1=1, a_2=5, a_3=4, a_4=10$；

$M_1=462, M_2=385, M_3=330, M_4=210$.

由

$$M_iM'_i\equiv 1(\bmod m_i),(i=1,2,3,4),$$

得

$$M'_1=3, M'_2=1, M'_3=1, M'_4=1.$$

因此

$$\begin{aligned}x &\equiv 3\times 462a_1+385a_2+330a_3+210a_4 (\bmod 2\ 310)\\ &\equiv 2\ 111 (\bmod 2\ 310).\end{aligned}$$

练　习

1. 求一个不超过 100 的正整数，当它被 3,5 和 7 除时，所得的余数分别等于 2,4 和 3.
2. 求解同余方程组：$x\equiv 7(\bmod 15), x\equiv 2(\bmod 35), x\equiv 16(\bmod 21)$.

习　题　3—3

A　组

1. 解同余方程组：$x=3(\bmod 5)$；$x=6(\bmod 7)$.
2. 判断下面同余方程是否有解. 如果有解，请找出一个解.

   (1) $5x\equiv 9(\bmod 11)$；　　(2) $7x\equiv 1(\bmod 3)$.
3. 解同余方程组：

   $x\equiv 1(\bmod 2), x\equiv 1(\bmod 3), x\equiv 6(\bmod 7)$.
4. 解同余方程组：

   $x\equiv 1(\bmod 3), x\equiv -1(\bmod 5), x\equiv 2(\bmod 7), x\equiv -2(\bmod 11)$.
5. 求一个最小的 4 位数，它用 11 除余 1，用 13 除余 3，用 17 除余 7.

B　组

1. 求相邻的 4 个整数，它们依次可被 2^2，3^2，5^2 及 7^2 整除．
2. 解同余方程组：

   $x\equiv 3 \pmod 8$，$x\equiv 11 \pmod{20}$，$x\equiv 1 \pmod{15}$．

复习题三

1. 举例说明存在整数 a,b,m 使得 $ab\equiv 0 \pmod m$，但 $a\not\equiv 0 \pmod m$，且 $b\not\equiv 0 \pmod m$.

2. 判断下列整数能否同时被 7 和 13 整除.

1 234；728；8 467；3 864；13 467.

3. 用弃九法检查下列计算题的正确性.

(1)1 428+357=1 785；　　(2)2 376−505=1 861；

(3)196×23=4 408；　　(4)32 856÷37=888.

4. 计算：

(1)(7 mod 11+5 mod 11)×(3 mod 11)；

(2)(9 mod 13+4 mod 13)×(3 mod 13)；

(3)(6 mod 14+8 mod 14)×(2 mod 14).

5. 求欧拉函数 $\varphi(18),\varphi(22),\varphi(23),\varphi(40),\varphi(43)$ 的值.

6. 判断下面同余方程是否有解. 如果有解，请找出一个解.

(1)$5x\equiv 3 \pmod{13}$；　　(2)$6x\equiv 3 \pmod{12}$；

(3)$7x\equiv 18 \pmod{37}$.

7. 解同余方程组：

(1)$x\equiv 2 \pmod 3, x\equiv -2 \pmod 7, x\equiv 3 \pmod{13}$；

(2)$x\equiv 1 \pmod 5, x\equiv -1 \pmod 7, x\equiv 3 \pmod{13}, x\equiv 7 \pmod{17}$.

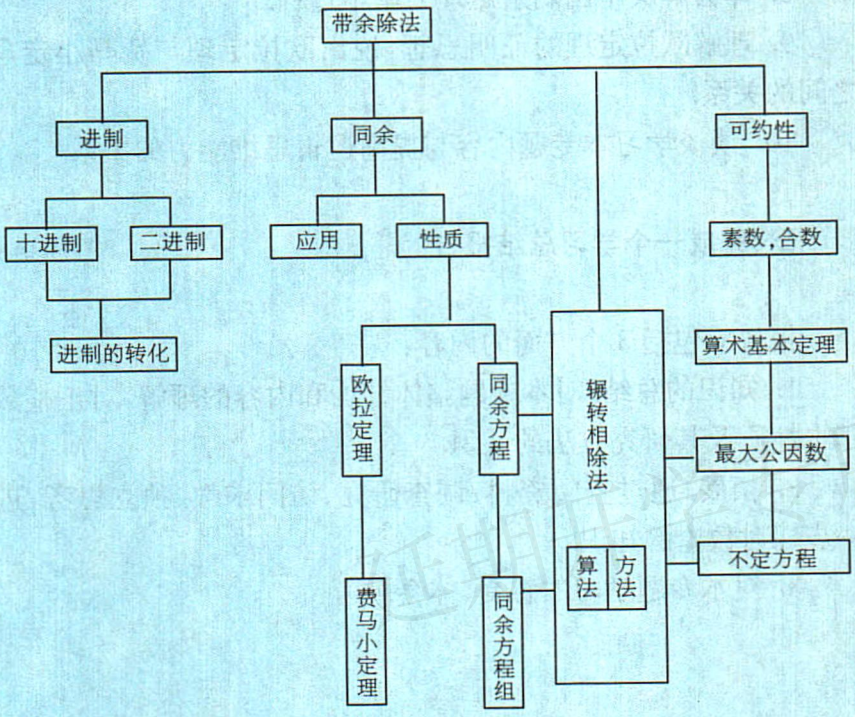
8. 求满足下列条件的所有正整数：

(1)不超过 10 000；

(2)它被 7 除余 2，被 11 除余 3，被 13 除余 8.

◆ 复习小结建议

一、知识框架



二、思考下列问题

1. 谈谈自己所理解的进位制和不同进位制之间的转换. 以二进制与十进制间的转换为例，设计实现这个转换的算法框图.

2. 讨论素数在整数中的地位和作用. 如何判断一个数是素数?

3. 理解辗转相除的基本思想和算法过程. 体会辗转相除法在本专题中的作用.

4. 什么是两个数的最大公因数？体会最大公因数在求解不定方程中的作用.

5. 什么叫两个数互素？互素的概念和素数有什么不同？体会素数和互素在同余理论中的作用.

6. 比较同余性质与等式性质的异同.

7. 在求解同余方程的过程中，如何利用辗转相除的思想和方法？

8. 体会解决中国剩余定理的基本过程.

9. 理解欧拉定理的证明思想，说出欧拉定理与费马小定理之间的关系.

10. 谈谈学习本专题内容与提高逻辑思维能力的关系.

三、完成一个学习总结报告

报告应包括 3 个方面的内容：

1. 知识的总结. 对本专题整体结构和内容的理解，对正整数基本性质及其研究方法的认识.

2. 拓展. 通过查阅资料、调查研究、访问求教、独立思考，进一步探讨数论的知识.

3. 对本专题学习的感受、体会.

附录 1

部分数学专业词汇中英文对照表

中文	英文
素数	prime number
因数	factor
最大公因数	greatest common divisor
最小公倍数	least common multiple
十进制	decimal scale
带余除法	division algorithm
辗转相除法	Euclid algorithm
互素	coprime, relatively prime
余数	remainder
除数	divisor
整除	divisible
同余	congruence
同余类	congruent class
一次不定方程	linear indeterminate equation
同余方程	congruence equation
同余方程组	congruence equation system
欧拉函数	Euler function
费马小定理	Fermat little theorem
欧拉定理	Euler's theorem
中国剩余定理	Chinese remainder theorem

附录 2

信息检索网址导引

基础教育教材网

http://www.100875.com.cn/

简介：基础教育教材网是由北京师范大学出版社创建的一个综合性网站，内容主要涉及新课程标准改革研究、课题研究、教学研究、评价研究和教学资源等几个方面. 网站在提供教学实例、教学课件的同时，也给教师和学生提供了交流互动的宽松平台.

后　记

本套教材是按照国家教育部于2003年4月颁布的《普通高中数学课程标准(实验)》编写的.我们在编写过程中强调了数学课程的基础性和整体性,突出了数学的思想性和应用性,尊重学生的认知特点,创造多层次的学习活动,为不同的学生提供不同的发展平台,注意发挥数学的人文教育价值.好学好用.

教材的建设是长期、艰巨的任务,每一位教师在教学实践中要自主地开发资源,创造性地使用教材.我们殷切希望教材的使用者与我们携手合作,对教材的逐步完善提供有力的支持,促进基础教育课程改革的深入发展.

本套教材的编委会组成如下(按姓氏笔画排序):

王希平、王尚志、王建波、任志瑜、刘美仑、吕世虎、吕建生、李亚玲、李延林、汪香志、严士健、张丹、张饴慈、张思明、姚芳、赵大悌、徐勇、戴佳珉.

由于时间仓促,教材中的错误在所难免,恳请广大使用者批评指正.

北京师范大学出版社