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

人民教育出版社　课程教材研究所
中学数学教材实验研究组　编著

人民教育出版社
B版

普通高中课程标准实验教科书

数学

选修 4-6

B 版

初等数论初步

人民教育出版社　课程教材研究所
中学数学教材实验研究组　编著

*

人民教育出版社 出版发行

网址：http://www.pep.com.cn

北京四季青印刷厂印装　全国新华书店经销

*

开本：890 毫米×1 240 毫米　1/16　印张：3.75　字数：84 000

2007 年 4 月第 2 版　2010 年 6 月第 8 次印刷

ISBN 978-7-107-18755-1
G·11845（课）　定价：4.00 元

主　　编　　高存明

编　　者　　曹惠中　罗声雄

责任编辑　　龙正武

美术编辑　　李宏庆　王　喆

封面设计　　李宏庆

本册导引

人类早期就认识了自然数. 它好像很简单，可又神秘莫测. 在征服自然界的进程中，人们要向自然数的奥秘进军，如同探索宇宙和生命的奥秘，经过几千年的奋斗，人类已经揭示出自然数的很多规律，但时至今日，还有许多问题没有解决. 在研究自然数的进程中，形成了一门数学学科，叫做数论. 数论者，乃论数也，专门讨论整数.

当你翻阅本书时，出现在你面前的是一堆抽象数字和生疏符号，你的第一感觉也许是陌生，甚至有点畏惧，当你怀着探索的欲望，真正进入书本后，你会发现那是错觉. 原来，你从刚懂事开始，便与自然数打交道，与它的亲密接触达十多年之久，随着学习的深入，你会逐渐感受到数论的亲和力，以及它的魅力.

同学们在以往的学习中，用各种方法和技巧解决了许多整数问题，同时也遇到了不少困难. 本书的目的是提供一些初等的一般理论与方法，在这些理论与方法的引导下，解决现实的整数问题，其中包括一些古老的、经典的整除问题和现代信息技术问题.

许多整数问题看上去好像很简单，其实十分艰深. 毋庸置疑，学数论有一定的难度，但征服困难，正是培养毅力，提高智力水平的重要途径. 本书力图深入浅出，结合同学们的实际，帮助同学们渡过一道道难关，以获得数论的初步知识.

本书共分三章，内容分别为整数的整除性、同余及同余方程. 这三部分内容是数论的基础. 同学们在以往的学习中，均有所接触. 我们相信，只要你有信心，并且用心就能学好用好，为今后的学习和工作奠定良好的基础.

数论无论在理论方面或在实际应用方面都有重要作用，它是数学的基础学科，掌握数论的初步知识，对一个现代社会的文明公民是十分必要的. 我们热切希望同学们选修这门课程，向自然数的奥秘进军.

目　录

整数的整除性

在日常生活中，我们经常遇到整数的整除问题. 例如，一箱苹果有48个，按个数分给7个人，能否分配公平？你马上知道，这不可能，原因是7不能整除48. 又如，本年级105人参加团体操，要求队形呈长方形（不能排成一行或一列），问排列的行数如何选择？你会立即给出答案：行数可为3，5，7，15，21，35. 这是因为除1和105之外，只有这六个正整数能整除105.

研究整除问题，不仅是现实的需要，而且饶有兴味. 研究整数的整除不仅是数论的开端，而且所形成的方法与理论是数论的基础. 同学们与整除打交道有丰富的经验，本章不过是将你的经验与知识加以整理，使之更具普遍性和系统性.

1.1 整　除

同学们在做整数除法的时候，都知道三件事：(1) 除数切忌为0；(2) 除法是乘法的逆运算，例如，$3\times7=21$，那么$21\div7=3$；(3) 如果$a\div b$商为整数，余数为0，则说b整除a，否则就说b不能整除a. 由此引出

定义 设a，b是整数，$b\neq0$. 如果有整数q，使$a=qb$，则称b整除a，记作$b|a$. 并称b是a的约数(或因数)，a是b的倍数. 否则称b不能整除a，记作$b\nmid a$.

例如，$7|105$，105是7的倍数；$7\nmid48$，48不是7的倍数；1，3，5，7，15，21，35，105都是105的约数；1和11是11的约数等等.

注意，0不是任何整数的约数，但0是任何整数的倍数. 符号$b|a$本身包含了条件$b\neq0$. a，b可以是负整数.

整除具有如下性质，请同学们自己验证.

(1) 若$b|a$，$c|b$，则$c|a$.

(2) 若$c|a$，$c|b$，则对任意整数x，y，必有$c|(ax+by)$.

(3) 若$b|a$，$a\neq0$，则$|b|\leqslant|a|$.

(4) 若$b|a$，$a\neq0$，则$\dfrac{a}{b}\Big|a$.

例1 设$3|m$，$7|m$，则$21|m$.

证明：由$3|m$，可写$m=3q$，由此及$7|m$知$7|3q$. 由$7|7q$，$7|3q$及性质(2)可得$7|[7q-2\times(3q)]$，即$7|q$. 因此可令$q=7d$，于是，有$m=3q=3\times7d=21d$，故$21|m$.

例 2 设 q_1，q_2，…，q_k 是正整数 n 的所有的正约数，证明

$$(q_1q_2\cdots q_k)^2=n^k.$$

证明：由性质(4)知，$\frac{n}{q_1}$，$\frac{n}{q_2}$，…，$\frac{n}{q_k}$也是 n 的所有的正约数. 不妨设 $q_1<q_2<\cdots<q_k$，则有 $q_1=\frac{n}{q_k}$，$q_2=\frac{n}{q_{k-1}}$，…，$q_k=\frac{n}{q_1}$. 因此

$$q_1q_2\cdots q_k=\frac{n}{q_k}\times\frac{n}{q_{n-1}}\times\cdots\times\frac{n}{q_1},$$

$$\Rightarrow(q_1q_2\cdots q_k)^2=n^k.$$

例如，1，2，3，4，6，12 是 12 的全部正约数，因而$\frac{12}{1}$，$\frac{12}{2}$，$\frac{12}{3}$，$\frac{12}{4}$，$\frac{12}{6}$，$\frac{12}{12}$也是 12 的全部正约数. 后者不过是将前者倒过来排列. 因此

$$1\times2\times3\times4\times6\times12=\frac{12}{12}\times\frac{12}{6}\times\frac{12}{4}\times\frac{12}{3}\times\frac{12}{2}\times\frac{12}{1},$$

$$\Rightarrow(1\times2\times3\times4\times6\times12)^2=12^6\ (\text{这里 } k=6).$$

例 3 证明：若正整数 n 的全部正约数有奇数个，则 n 为平方数.

证明：设约数个数为 $2k+1$，由例 2 可知，将 n 的全部正约数从小到大排列 q_1，q_2，…，q_k，q_{k+1}，…，q_{2k+1}. 则与约数$\frac{n}{q_{2k+1}}$，…，$\frac{n}{q_{k+1}}$，$\frac{n}{q_k}$，…，$\frac{n}{q_1}$对应相等. 这两列数中位于正中央的分别是 q_{k+1}，$\frac{n}{q_{k+1}}$，因此 $q_{k+1}=\frac{n}{q_{k+1}}$，于是 $n=q_{k+1}^2$.

习题 1-1

1. 证明：

(1) 若 $a|b$，$m\neq0$，则 $ma|mb$；

(2) 设 a，b 为正整数，$a|b$ 且 $b|a$，则 $a=b$.

2. 证明：三个连续正整数之和是 3 的倍数.

3. 证明：若 $6|(a+b)$，则 $6|(a^3+b^3)$.

4. 设 n 为正整数，证明 $6|[n(n+1)(2n+1)]$. (提示：$2n+1=(n+2)+(n-1)$)

5. 15 位校友聚会，能否每个人都握手 5 次？

6. 设 $n>1$，$(n-1)|(n+11)$，求 n. (提示：将 $n+11$ 表为 $(n-1)+12$)

1.2 素数与合数

同学们知道，2，3，5，7，11，13，17，19，…除去 1 和自身外，不能被其他正整数整除，这类大于 1，而且正约数只有 1 和自身的整数叫做素数. 素数也称为质数. 要特别

注意，1 不是素数. 如果大于 1 的整数不是素数，则称其为合数. 研究素数是数论的核心内容之一.

素数在自然数中的分布很不规律，有时隔一个数就有一个素数，如 3，5；有时隔三个数有一个素数，如 19，23. 有的相邻两素数相隔很远，寻找素数和判别一个数是否为素数是很艰难的. 下面的定理给出了一个寻找素数的有效算法.

定理 1 设 a 是任一大于 1 的整数，则 a 的除 1 以外的最小正约数 q 必是素数. 当 a 是合数时，$q\leqslant\sqrt{a}$.

证明：用反证法. 设 q 不是素数，由 $q>1$ 知 q 是合数. 由此可知存在 q 的正约数 q_1，使 $1<q_1<q$. 由 $q_1\mid q$，$q\mid a$，可得 $q_1\mid a$，这与 q 是 a 除 1 以外的最小正约数矛盾.

当 a 是合数时，设 $a=a_1q$，其中 q 是 a 的大于 1 的最小正约数. 则 $a_1\geqslant q$，故 $q^2\leqslant a$，即 $q\leqslant\sqrt{a}$.

由定理 1 知，对于每一个合数 n，存在素数 p，使 $p\mid n$，且 $p\leqslant\sqrt{n}$. 由此可得到找出不超过 N 的全体素数的方法：

先找出不超过 $\sqrt{N}$ 的全体素数，且按大小顺序排列

$$2=P_1<P_2<\cdots<P_S\leqslant\sqrt{N},$$

然后把大于 1，且不超过 N 的自然数按从小到大顺序排列

$$2，3，\cdots，N. \qquad ①$$

在①中留下 $P_1=2$，而把 P_1 的倍数全部划掉. 再留下 $P_2=3$，而把 P_2 的倍数全部划掉. 继续这一手续，直到最后留下 P_S，而把 P_S 的倍数全部划掉. 留下的就是不超过 N 的全体素数. 这种寻找素数的方法，称为厄拉多塞筛法.

例如，为寻求 100 以内的全体素数，先找出不超过 $\sqrt{100}=10$ 的全体素数

$$2，3，5，7，$$

把从 2 到 100 的数按从小到大排列，把 2，3，5，7 留下，再先后划掉 2，3，5，7 这四个数的倍数，剩下的就是 100 以内的全部素数.

判断一个正整数 a 是否为素数，原则上要用不超过 $\sqrt{a}$ 的素数逐个试除. 对较小的数 a，工作量不是很大. 例如，$a=97$，你会一眼看出它是素数，因为 97 不是 2，3，5，7 的倍数. 又如 $a=191$，$\sqrt{a}<14$，容易看出，191 不是 2，3，5，7，11，13 的倍数，因此 191 是素数.

现在提出一个问题，素数究竟只是有限多个呢？还是有无穷多个？

定理 2 素数有无穷多个.

证明：用反证法. 假设自然数中只有有限多个素数，不妨记为 P_1，P_2，$\cdots$，P_k. 考虑整数 $N=P_1P_2\cdots P_k+1$. 由 $N>1$ 及定理 1 知存在素数 $P\mid N$. 此时必有 $P\neq P_i$，$1\leqslant i\leqslant k$（否则 $P\mid 1$）. 所以 P 是上述 k 个素数以外的素数. 这导出矛盾. 所以素数有无穷多个.

习题 1-2

1. 判断 359 是不是素数.
2. 利用厄拉多塞筛法找出 100 以内的全体素数.
3. 找出五个连续自然数，每个数都是合数.
4. 证明：大于 11 的自然数可以表示成两个合数之和.（提示：分奇、偶数考虑）

1.3 带余除法

同学们都会做整数除法，例如 $201\div13$，得到整数商 15，余数 6. 我们可以用除数、商和余数还原被除数，如上例 $201=13\times15+6$. 这就是带余除法，一般地，带余除法表述为如下定理.

定理 1 设 a，b 是两个整数，其中 $b>0$，则存在唯一的一对整数 q 及 r，使

$$a=bq+r,\ 0\leqslant r<b. \tag{①}$$

证明：存在性. 作整数序列

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

则 a 或者等于这个序列的某一项，或者在某相邻两项之间，即存在整数 q，使

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

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

唯一性. 设 q_1，r_1 是满足①式的另一对整数，则有

$$bq_1+r_1=bq+r,$$

于是有

$$b(q-q_1)=r_1-r$$

及

$$b|q-q_1|=|r_1-r|.$$

因为 r 和 r_1 都是小于 b 的非负整数，所以 $0\leqslant|r_1-r|<b$. 但 $b\mid|r_1-r|$，故有 $|r_1-r|=0$. 因此 $r=r_1$，$q=q_1$.

思考与讨论

如果定理 1 中的条件 $b>0$ 改成 $b\neq0$，定理 1 应做怎样的修改？

例 写出 a 被 b 除的带余除法表示式：

（1）$a=255$，$b=15$；　　（2）$a=-81$，$b=15$.

解：(1) $255=15\times17+0$；

(2) $-81=15\times(-6)+9$.

注意，虽然$-81=15\times(-5)-6$，$-81=15\times(-7)+24$也成立，但它们都不是带余除法表达式，因为不满足余数条件：$0\leqslant r<b$.

同学们知道，十进制数

$$a_n a_{n-1}\cdots a_1 a_0=a_n\times10^n+a_{n-1}\times10^{n-1}+\cdots+a_1\times10+a_0.$$

其中a_n，a_{n-1}，…，a_1，a_0在0，1，2，…，9中取值($a_n\neq0$，$n>0$)．例如

$$4\ 376=4\times10^3+3\times10^2+7\times10^1+6.$$

我们平常所用的数都是十进制的，现在计算机上用的数是二、八及十六进制的，下述结论表明自然数可以表示成任意$q(>1)$进制数.

设q是大于1的整数，则任意自然数n可表示为

$$n=c_m q^m+\cdots+c_1 q+c_0, \qquad ②$$

其中$m\geqslant0$，$0\leqslant c_i<q$，$0\leqslant i\leqslant m$，$c_m\neq0$．对于给定的q，这种表示方法是唯一的.

②式称为n的q进制表示.

例如，运用带余除法，可将十进制数101分别表为二进制数和八进制数：

$$101=2^6+2^5+2^2+1=(1100101)_2,$$

$$101=8^2+4\times8+5=(145)_8.$$

在十进制中，数字符号有10个：0，1，2，…，9．在二进制中，数字符号只有2个：0，1．在q进制中，数字符号有q个：0，1，2，…，$q-1$.

将q进制数化为十进制数，可按公式②直接计算．将十进制数化为q进制数的方法如下：设a为十进制数，用q去除a，余数就是右起第一位数．将商除以q的余数，得到右起第二位数．如此继续，直到商小于q为止.

习题 1-3

1. 写出$-1\ 999$被17除的带余除法表示式.

2. 请在503后面添加三个数字，使所得的六位数能被7，9，11整除.

3. 将101表成三进制数.

4. $5\times6=42$是什么进制的乘法？

1.4 辗转相除法与最大公约数

本节讲述辗转相除法，此方法在本书中有重要的应用．在我国古代的著名数学著作《九章算术》里就有了辗转相除法，书中把此方法叫做“更相减损术”.

对整数 $a>0$，$b>0$ 反复运用带余除法，可得下列等式

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

由于 $b>r_1>r_2>\cdots$，故经过有限次带余除法后，最终总可以得到一个余数是零的带余除法表达式，即①中最后一式的 $r_{n+1}=0$.

①式所指出的计算方法叫辗转相除法，也称欧几里得算法.

例如，$a=361$，$b=93$，做辗转相除

$$\begin{aligned}
361&=93\times3+82,\\
93&=82\times1+11,\\
82&=11\times7+5,\\
11&=5\times2+1,\\
5&=1\times5.
\end{aligned}$$

又如，$a=-360$，$b=93$，做辗转相除

$$\begin{aligned}
-360&=93\times(-4)+12,\\
93&=12\times7+9,\\
12&=9\times1+3,\\
9&=3\times3.
\end{aligned}$$

由①式可知

$$\begin{aligned}
r_1&=a-q_1b,\\
r_2&=b-r_1q_2=b-(a-q_1b)q_2\\
&=-q_2a+(1+q_1q_2)b.
\end{aligned}$$

一步一步计算下去，总可以得到 r_n 关于 a，b 的表达式

$$r_n=pa+qb,$$

其中 p，q 为整数. 如何求出 p，q 呢？下面的定理给出了一个递推算法.

定理 1 设 a，b 是任意两个正整数，并进行了辗转相除法①式，则有

$$Q_ka-P_kb=(-1)^{k-1}r_k,\ 1\leqslant k\leqslant n.\tag{②}$$

其中 $\begin{cases}P_0=1,\ P_1=q_1,\ P_k=q_kP_{k-1}+P_{k-2}\\ Q_0=0,\ Q_1=1,\ Q_k=q_kQ_{k-1}+Q_{k-2}\end{cases}$ 而且 $2\leqslant k\leqslant n$.

证明：对 k 使用数学归纳法. 由①式知 $a=bq_1+r_1$，可写成 $Q_1a-P_1b=(-1)^{1-1}r_1$. 同样由①式可得

$$\begin{aligned}
b&=r_1q_2+r_2\\
&=(a-bq_1)q_2+r_2,
\end{aligned}$$

即 $q_2a-(q_1q_2+1)b=-r_2$，可写成

$$Q_2a-P_2b=(-1)^{2-1}r_2.$$

故当 $k=1$，2 时，②式成立. 以下可设 $n\geqslant 3$.

现在设定理对$(k-1)$，$k(2\leqslant k\leqslant n-1)$成立. 下面证明定理对$(k+1)$成立.

由 $r_{k-1}=r_kq_{k+1}+r_{k+1}$和归纳假设可得

$$\begin{aligned}r_{k+1}&=r_{k-1}-r_kq_{k+1}\\&=(-1)^{k-2}(Q_{k-1}a-P_{k-1}b)-(-1)^{k-1}(Q_ka-P_kb)q_{k+1},\end{aligned}$$

于是有

$$\begin{aligned}(-1)^kr_{k+1}&=Q_{k-1}a-P_{k-1}b+q_{k+1}Q_ka-q_{k+1}P_kb\\&=(q_{k+1}Q_k+Q_{k-1})a-(q_{k+1}P_k+P_{k-1})b\\&=Q_{k+1}a-P_{k+1}b.\end{aligned}$$

注：在定理 1 的证明中使用了下述形式的数学归纳法：

设 $f(n)$是关于自然数 n 的一个命题，如果（1）当 $n=1$，2 时，$f(1)$，$f(2)$成立；(2) 设 $k\geqslant 2$. 由假设 $f(k-1)$，$f(k)$成立，能推出 $f(k+1)$成立. 那么，$f(n)$对所有正整数 n 成立.

下面我们用辗转相除法求最大公约数. 先考虑两个实际问题：

(1) 一个地面面积为 3.6 m×5.6 m 的房间，假设不计缝隙和不剪裁地板砖，问能用边长最大是多少厘米的正方形地板砖铺地？

不难想出所需边长就是 360 cm 与 560 cm 的公有约数中的最大数.

(2) 某超市销售某种货物，去年总收入为 36 963 元，今年每件货物的售价不变，总收入为 59 570 元. 如果单价（元）是大于 1 的整数，问今年和去年至少各售出这种货物多少件？

回答这个问题，关键要知道货物可能的最高单价，它就是 36 963 元与 59 570 元的公有约数中的最大数.

定义 设 a_1，a_2，…，a_k 是不全为零的整数. 如整数 d 是每一个 $a_i(1\leqslant i\leqslant k)$的约数，则称 d 为 a_1，a_2，…，a_k 的公约数. a_1，a_2，…，a_k 的公约数中最大的一个，称为这 k 个数的最大公约数，记为$(a_1, a_2, \cdots, a_k)$. 当$(a_1, a_2, \cdots, a_k)=1$ 时，称 a_1，a_2，…，a_k 为互素. 特别地，当 a_1，a_2，…，a_k 中的任何两个数都互素时，称 a_1，a_2，…，a_k 为两两互素.

由于整数 a 与$|a|$的约数相同，故有

$$(a_1,a_2,\cdots,a_k)=(|a_1|,|a_2|,\cdots,|a_k|).$$

因此在以下讨论中可设 $a_i(1\leqslant i\leqslant k)$是正整数.

首先讨论 $k=2$ 的情况.

设 a，b 是任意两个整数，其中 $b>0$，由带余除法知，存在唯一的一对整数 q，r，使 $a=bq+r$，$0\leqslant r<b$，此时有

定理 1 $(a, b)=(b, r)$.

证明：设 $d_1=(a, b)$，$d_2=(b, r)$. 由 $d_1|a$，$d_1|b$ 及 $r=a-bq$ 知 $d_1|r$，故 d_1 是 b，r 的公约数. 因此有 $d_1\leqslant d_2$. 同理可证 d_2 是 a，b 的公约数，故有 $d_2\leqslant d_1$. 于是得到 $d_1=d_2$.

对 a，b 使用辗转相除法，不妨设算式为 §1.4 节的①式❶，则有

定理 2　$(a, b)=r_n$.

证明：由定理 1 和算式①即得

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

定理 2 给出了求(a, b)的一个具体算法.

例　求(6 409，42 823).

解：因为

$$\begin{aligned}
&42\ 823=6\ 409\times 6+4\ 369,\\
&6\ 409=4\ 369\times 1+2\ 040,\\
&4\ 369=2\ 040\times 2+289,\\
&2\ 040=289\times 7+17,\\
&289=17\times 17,
\end{aligned}$$

所以

$$(6\ 409,\ 42\ 823)=17.$$

使用辗转相除法不仅可以实际算出(a, b)，而且可以导出下述的在理论证明中极为重要的裴蜀恒等式.

定理 3　（裴蜀恒等式）任给整数 $a>0$，$b>0$，存在整数 m，n，使

$$(a,\ b)=ma+nb.$$

证明：在 1.4 节定理 1 中取 $k=n$，即得

$$(-1)^{n-1}r_n=Q_na-P_nb,$$

因此

$$(a,b)=[(-1)^{n-1}Q_n]a+[(-1)^nP_n]b.$$

例如

$$\begin{aligned}
&(6,\ 15)=3\times 6-1\times 15,\\
&(36,\ 8)=1\times 36-4\times 8.
\end{aligned}$$

推论　a，b 的任一公约数是其最大公约数的约数.

定理 4　设 $d|ab$，且$(d,\ a)=1$，则 $d|b$.

证明：由定理 3 知，使用辗转相除法可求得一对整数 x_0，y_0，使

$$dx_0+ay_0=1,$$

从而

$$(db)x_0+(ab)y_0=b.$$

由 $d|db$，$d|ab$ 及上式得 $d|b$.

定理 5　当 $m>0$ 时，有$(am,\ bm)=(a,\ b)m$.

证明：对 a，b 使用辗转相除法，再乘 m，则有

$$\begin{aligned}
&am=(bm)q_1+r_1m,\\
&bm=(r_1m)q_2+r_2m,
\end{aligned}$$

注

❶ 为了方便，以下凡对 a，b 使用辗转相除法，都假设算式为 §1.4 节的①式.

$$\cdots,$$

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

因此

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

现在讨论一般情况.

下述的定理表明求 k 个数 a_1，a_2，…，$a_k(k\geqslant 3)$ 的最大公约数可以由求两个数的最大公约数而逐步求出.

定理 6 设 $(a_1,\ a_2)=d_2$，$(d_2,\ a_3)=d_3$，…，$(d_{k-1},\ a_k)=d_k$，则

$$(a_1,\ a_2,\ \cdots,\ a_k)=d_k.$$

证明：记 $(a_1,\ a_2,\ \cdots,\ a_k)=d$. 由 $d_k\mid a_k$，$d_k\mid d_{k-1}$，$d_{k-1}\mid a_{k-1}$，$d_{k-1}\mid d_{k-2}$ 即得

$$d_k\mid a_{k-1},\ d_k\mid d_{k-2}.$$

由此类推，最后可得

$$d_k\mid a_k,\ d_k\mid a_{k-1},\ \cdots,\ d_k\mid a_1.$$

由 d_k 是 a_1，a_2，…，a_k 的公约数知 $d_k\leqslant d$.

另一方面，由 $d\mid a_1$，$d\mid a_2$ 可得 $d\mid d_2$. 由此类推，最后可得 $d\mid d_k$，因此有 $d\leqslant d_k$. 于是得到 $d=d_k$.

习题 1-4

1. 求 $(198,\ 252)$，$(1\ 008,\ 1\ 260)$.
2. 求 $(1\ 008,\ 1\ 260,\ 882,\ 1\ 134)$.
3. 证明：对任意的整数 x，y，$(a_1,\ a_2)=(a_1,\ a_2+a_1x)=(a_1+a_2y,\ a_2)$.
4. 证明：当 $(c,\ a)=1$ 时，有 $(c,\ ab)=(c,\ b)$.
5. 证明：当 $(a,\ b)=1$ 时，有 $(c,\ ab)=(c,\ a)(c,\ b)$.
6. 证明：$\left(\dfrac{a}{(a,\ b)},\ \dfrac{b}{(a,\ b)}\right)=1$.
7. 证明：$21n+4$ 与 $14n+3$ 互素.

1.5 最小公倍数

先考虑两个实际问题：

(1) 金星和地球在某一时刻相对于太阳处于某一确定位置. 已知金星绕太阳一周为 225 天，地球绕太阳一周为 365 天，问这两个行星至少要经过多少天才同时回到原来位置?

不难想到所要天数就是 225 与 365 的公有倍数中的最小数.

(2) 排练团体操时，要使队伍排成 10 行，15 行，18 行，24 行，队形都成矩形，问最少需要多少人参加排练?

易知所需人数就是 10，15，18，24 这四个数的公有倍数中的最小者.

定义 设 b_1，b_2，…，b_k 是都不为零的整数，如果整数 d 是每一个 $b_j(1\leqslant j\leqslant k)$ 的倍数，则称 d 为 b_1，b_2，…，b_k 的公倍数. b_1，b_2，…，b_k 的公倍数中的最小正数，称为这 k 个数的最小公倍数，记为$[b_1, b_2, \cdots, b_k]$.

思考与讨论

为什么最大公约数$(a_1, a_2, \cdots, a_n)$的定义中要求 a_1，a_2，…，a_n 不全为零? 为什么最小公倍数$[b_1, b_2, \cdots, b_m]$的定义中要求 b_1，b_2，…，b_m 都不为零?

由于整数 $b\neq 0$ 时，b 与 $|b|$ 的倍数相同，故有

$$[b_1, b_2, \cdots, b_m]=[|b_1|, |b_2|, \cdots, |b_m|].$$

因此在以下讨论中可设 $b_j(1\leqslant j\leqslant m)$ 是正整数.

现在讨论有关最小公倍数的重要性质.

定理 1 b_1，b_2，…，b_k 的任一公倍数必是其最小公倍数的倍数.

证明：用反证法. 记 s 和 b 分别为 b_1，b_2，…，b_k 的最小公倍数和任一公倍数. 如果 $s\nmid b$，则由带余除法可得

$$b=qs+r,\ 0<r<s.$$

由 $r=b-qs$ 知 r 也是 b_1，b_2，…，b_k 的公倍数. 但 $0<r<s$，与 s 是最小公倍数矛盾.

由于最大公约数可以用辗转相除法实际算出，因此下述定理给出了最小公倍数的求法.

定理 2 设 $a>0$，$b>0$，则

$$[a, b]=\frac{ab}{(a, b)}.$$

证明：由 $a|(ab)$，$b|(ab)$，故$[a, b]|(ab)$. 因此可设

$$ab=[a, b]s.$$

由此，$a=\dfrac{[a, b]}{b}s$，$b=\dfrac{[a, b]}{a}s$，所以 $s|a$，$s|b$. 因此有$s|(a,b)$. 于是

$$ab=[a, b]\frac{(a, b)}{l}. \qquad ①$$

另一方面，由$(a, b)|(ab)$，故可设

$$ab=(a, b)t.$$

由此，$t=\dfrac{a}{(a, b)}b$，$t=\dfrac{b}{(a, b)}a$，所以 $b|t$，$a|t$. 因此有$[a, b]|t$. 于是

$$ab=(a, b)[a, b]m. \qquad ②$$

由①式，②式即得 $l=m=1$.

定理 3 设 $m>0$，则$[ma_1, ma_2]=m[a_1, a_2]$.

证明：由定理 2 及 1.4 节定理 5 可得

$$[ma_1, ma_2]=\frac{(ma_1)(ma_2)}{(ma_1, ma_2)}=\frac{m^2a_1a_2}{m(a_1, a_2)}$$

$$=m\frac{a_1a_2}{(a_1, a_2)}=m[a_1, a_2].$$

求 $k(>2)$个数 b_1，b_2，…，b_k 的最小公倍数也可以用连续求两个数的最小公倍数去完成.

定理 4 设$[b_1, b_2]=s_2$，$[s_2, b_3]=s_3$，…，$[s_{k-1}, b_k]=s_k$，则

$$[b_1, b_2, \cdots, b_k]=s_k.$$

证明：记$[b_1, b_2, \cdots, b_k]=s$. 由 $s_i|s_{i+1}$，$2\leqslant i\leqslant k-1$，知$s_i|s_k$，$2\leqslant i\leqslant k-1$. 又因为 $b_1|s_2$，$b_i|s_i$，$2\leqslant i\leqslant k$，所以 s_k 是b_1，b_2，…，b_k 的一个公倍数. 因此有 $s|s_k$.

另一方面，由 $b_1|s$，$b_2|s$ 知 $s_2|s$. 同样由 $s_2|s$，$b_3|s$ 知 $s_3|s$. 依次类推最后得到 $s_k|s$.

于是得到 $s=s_k$.

习题 1-5

1. 回答本节开头提出的两个问题.
2. 求[24 871，3 468].
3. 设 a，b 是正整数，且$[a, b]=105$，$(a, b)=7$，求 a，b.
4. 设 a，b 是正整数，且$[a, b]=(a, b)$，证明：$a=b$.
5. 证明：$[a^3, b^3]=[a, b]^3$.
6. 证明：$[a, b, c](ab, ac, bc)=abc$.

1.6 算术基本定理

在本节中，我们讨论把自然数写成素数的乘积，结论就是著名的算术基本定理. 此定理建立了自然数与素数之间的一个重要的关系式. 在证明该定理时，要用到如下结论.

结论 1 设 p 是一个素数，a 是任一整数，则有 $p|a$ 或$(p, a)=1$.

证明：由$(p, a)|p$ 知，$(p, a)=1$ 或$(p, a)=p$，而后者即是 $p|a$.

结论 2 设 p 为素数，$p|ab$ 且 $p\nmid a$，则 $p|b$.

证明：由 $p\nmid a$ 及结论 1，知$(p, a)=1$. 故由 1.4 节定理 4，即知 $p|b$.

结论 3 设 $p|(a_1a_2\cdots a_s)$，则 p 至少能整除一个 a_i，$1\leqslant i\leqslant s$.

证明：如果 $p\nmid a_1$，则由结论 2 知 $p|(a_2\cdots a_s)$. 如果 $p\nmid a_2$，同理可得 $p|(a_3\cdots a_s)$. 依次类推，最终可得 p 至少能整除一个 a_i，$1\leqslant i\leqslant s$.

定理 1 （算术基本定理）设 $n>1$，则 n 可分解成素数的乘积

$$n = p_1 p_2 \cdots p_m, \tag{1}$$

如果不计这些素数的次序，则分解式①是唯一的.

证明：先证 n 可分解成素数的乘积.

当 n 是素数时，定理显然成立. 当 n 是合数时，记 p_1 为 n 的最小素因子，则有

$$n=p_1 n_1,\ 1<n_1<n.$$

若 n_1 是素数，则定理成立. 当 n_1 是合数时，记 p_2 为 n_1 的最小素因子，则有

$$n=p_1 p_2 n_2,\ 1<n_2<n_1<n.$$

继续上述过程得 $n>n_1>n_2>\cdots>1$，此过程不能超过 n 次，所以最后必有

$$n=p_1 p_2 \cdots p_m.$$

下证唯一性.

设 $n=p_1 p_2 \cdots p_m=q_1 q_2 \cdots q_t$，$p_1 \leqslant p_2 \leqslant \cdots \leqslant p_m$，$q_1 \leqslant q_2 \leqslant \cdots \leqslant q_t$，$p_i$，$q_j$，$1 \leqslant i \leqslant m$，$1 \leqslant j \leqslant t$，都为素数.

由 $p_1 \mid q_1 \cdots q_t$ 和结论 3 知 $p_1 \mid q_j$，即得 $p_1=q_j \geqslant q_1$. 同理可得 $q_1=p_i \geqslant p_1$. 因此有 $p_1=q_1$. 重复以上论证，依次可证明 $p_2=q_2$，…，$p_m=q_t$，$m=t$.

把①式中相同素数写成幂的形式，即得

$$n=p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r},\ p_1<p_2<\cdots<p_r,\ \beta_i \geqslant 1,\ 1 \leqslant i \leqslant r.$$

上式称为 n 的标准分解式，对给定的 n，标准分解式是唯一的.

思考与讨论

1 是正整数，且它的正约数只有 1，为什么不把 1 看成是素数呢？

下面是算术基本定理的两个应用.

定理 2 设 $n=p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ 是 n 的标准分解式，若用 $\tau(n)$ 表示 n 的所有正约数的个数，则有

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1).$$

证明：n 的正约数 d 必形如 $d=p_1^{l_1} \cdots p_s^{l_s}$，其中 l_1 可取 0 至 α_1，共有 (α_1+1) 种取法；l_2 可取 0 至 α_2，共有 (α_2+1) 种取法；……. 因此有

$$\tau(n)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1).$$

例如，$12=2^2 \times 3^1$，12 的正约数有 $(2+1)(1+1)=6$ 个. $360=2^3 \times 3^2 \times 5^1$，360 的正约数有 $(3+1)(2+1)(1+1)=24$ 个.

定理 3 设 a，b 是任意两个正整数，且

$$a=p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},\ \alpha_i \geqslant 0,\ 1 \leqslant i \leqslant k,$$

$$b=p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},\ \beta_i \geqslant 0,\ 1 \leqslant i \leqslant k,$$

则

$$(a,\ b)=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k},\ r_i=\min(\alpha_i,\ \beta_i),\ 1\leqslant i\leqslant k,$$
$$[a,\ b]=p_1^{l_1}p_2^{l_2}\cdots p_k^{l_k},\ l_i=\max(\alpha_i,\ \beta_i),\ 1\leqslant i\leqslant k.$$

证明留给读者.

习题 1-6

1. 用分解素因数法求：
   (1) (4 712，4 978，5 890)；
   (2) [4 712，4 978，5 890].
2. 求 $\tau(300\ 000)$.
3. 利用算术基本定理证明：
   (1) $\sqrt{6}$是无理数；
   (2) $\lg 7$ 是无理数.
4. 设 $\mathbf{N}^*$ 是只含素因数 2，3 的所有正整数构成的集合，$\mathbf{Q}_+$ 是正有理数集. 试建立一个 $\mathbf{Q}_+$ 到 $\mathbf{N}^*$ 的一一映射.

1.7 二元一次不定方程

不定方程是未知数的个数多于方程的个数且未知数受到某种限制的方程. 我国对不定方程的研究很早. 例如《周髀算经》中的商高定理“勾三股四弦五”，给出了不定方程 $x^2+y^2=z^2$ 的一组解$x=3$，$y=4$，$z=5$. 《九章算术》中的“五家共井”问题；《张丘建算经》中的“百钱买百鸡”问题；《孙子算经》中的“物不知其数”等都是中外闻名的不定方程问题. 古希腊数学家丢番图曾系统地研究了某些不定方程问题，因此不定方程也称丢番图方程.

我国古代数学家张丘建曾解答了如下一个问题：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 x_1，x_2，x_3 分别为鸡翁，鸡母，鸡雏的数目，由问题的条件可得

$$\begin{cases}5x_1+3x_2+\dfrac{1}{3}x_3=100\\ x_1+x_2+x_3=100\end{cases}$$

解此问题就是要求出上述不定方程组的非负整数解.

消去 x_3 可得

$$7x_1+4x_2=100.$$

上述方程就是二元一次不定方程的一个具体的例子，它的一般形式为

$$ax+by=c, \tag{①}$$

其中 a，b，c 是整数，且 a，b 都不为零.

解不定方程①就是要求求出①式的所有整数解.

定理 1 方程①有整数解的充分必要条件是 $(a,b)\mid c$.

证明：必要性是明显的. 下面证明充分性.

由裴蜀恒等式知存在整数 u_0，v_0，使

$$au_0+bv_0=(a,b).$$

于是 $x_0=u_0\dfrac{c}{(a,b)}$，$y_0=v_0\dfrac{c}{(a,b)}$ 就是①式的一组整数解.

若知道①式的一个特解❶ (x_0,y_0)，则立刻就可以写出①式的全部解.

注

❶ 不定方程的一个特解是指满足方程的一个具体的数（或数组），一般解是指满足方程的所有的数（或数组）的表达式.

定理 2 已知 (x_0,y_0) 是①式的一个解，则①式的全部解为

$$\begin{cases} x=x_0+\dfrac{b}{(a,b)}t \\ y=y_0-\dfrac{a}{(a,b)}t \end{cases} \text{其中 } t=0,\pm1,\pm2,\cdots. \tag{②}$$

证明：易知②式给出的所有 (x,y) 都满足方程①.

反之，设 (x,y) 是①式的任意一个解. 由

$$ax+by=c$$

及

$$ax_0+by_0=c,$$

可得

$$a(x-x_0)+b(y-y_0)=0,$$

进而有

$$\frac{a}{(a,b)}(x-x_0)=-\frac{b}{(a,b)}(y-y_0). \tag{③}$$

由 $\left(\dfrac{a}{(a,b)},\dfrac{b}{(a,b)}\right)=1$，知 $\dfrac{b}{(a,b)}\Big|(x_0-x)$. 因此存在整数 t，使

$$x=x_0+\frac{b}{(a,b)}t.$$

代入③式即得

$$y=y_0-\frac{a}{(a,b)}t.$$

以下说明怎样用辗转相除法具体求出①式的一个特解.

不妨设①式中的 a，b 互素，不然去解方程

$$\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=\frac{c}{(a,b)}$$

即可.

首先画出如下的框图，然后将由辗转相除法求出的 q_1，q_2，…，q_n（参看 §1.4 节的

①式）依次填在框图的第二行里，接着在第三行填上 $P_0=1$，$P_1=q_1$，在第四行填上 $Q_0=0$，$Q_1=1$. 最后利用 1.4 节定理 1 中的递推公式依次求出 P_2，Q_2，P_3，Q_3，…，P_n，Q_n.

	0	1	2	…	$k-2$	$k-1$	k	…	n
q		q_1	q_2		q_{k-2}	q_{k-1}	q_k		q_n
P	1	q_1	P_2		P_{k-2}	P_{k-1}	P_k		P_n
Q	0	1	Q_2		Q_{k-2}	Q_{k-1}	Q_k		Q_n

由 1.4 节定理 1(取 $k=n$) 知

$$Q_na-P_nb=(-1)^{n-1},$$

即

$$a[(-1)^{n-1}Q_nc]+b[(-1)^nP_nc]=c.$$

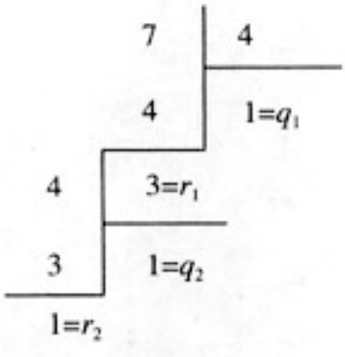
因此将以上求得的 P_n，Q_n 代入下式

$$\begin{cases}x_0=(-1)^{n-1}Q_nc\\ y_0=(-1)^nP_nc\end{cases} \qquad ④$$

即得①式的一个特解.

例 求不定方程 $7x+4y=100$.

解：$(7,4)=1$，故可用辗转相除法求一特解.



	0	1	2
q		1	1
P	1	1	$2=P_2$
Q	0	1	$1=Q_2$

由④式可得方程的一个特解为

$$\begin{cases}x_0=-100\\ y_0=200\end{cases}$$

由定理 2 即得方程的全部解为

$$\begin{cases}x=-100+4t\\ y=200-7t\end{cases} \text{ 其中 } t=0,\ \pm1,\ \pm2,\ \cdots.$$

也可以用如下方法求这个不定方程的一个特解：

由 $7x+4y=100$，推出 $x=\dfrac{100-4y}{7}=14+\dfrac{2-4y}{7}$，取 $y_0=4$，则 $x_0=12$.

不定方程的全部解为 $\begin{cases}x=12+4t\\ y=4-7t\end{cases}$ 其中 $t=0,\ \pm1,\ \pm2,\ \cdots.$

虽然用以上两种方法得到的解的表达式形式上不同，但本质上是相同的.

习题 1-7

1. 解不定方程 $37x-107y=25$.

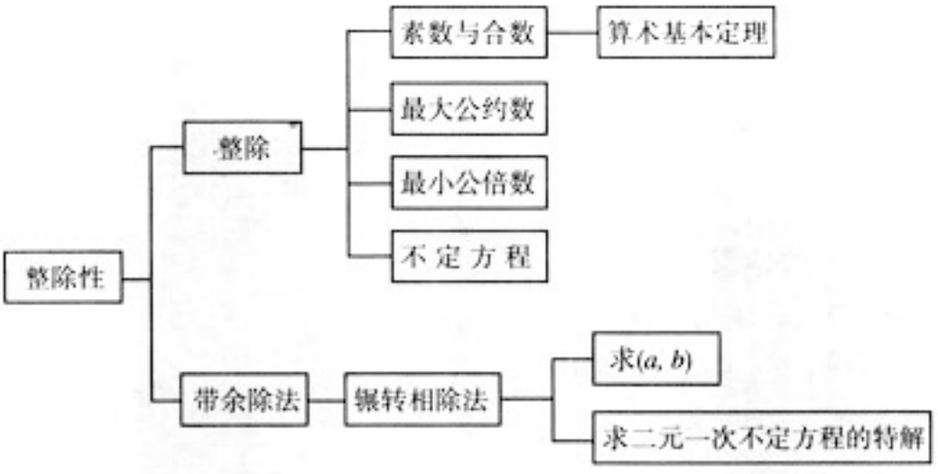
2. 求不定方程 $7x+19y=213$ 的正整数解.

3. 21 世纪有这样的年份，这个年份减去 22 等于它各个数字的和的 495 倍，求这个年份.

4. （百牛问题）有银百两，买牛百头，大牛每头十两，小牛每头五两，牛犊每头半两，问买的一百头牛中大牛，小牛，牛犊各几头?

本章小结

Ⅰ 知识结构



Ⅱ 思考与交流

1. 给出一个在实际问题中应用最大公约数的例子，并用辗转相除法算出结果.
2. 给出一个在实际问题中应用二元一次不定方程的例子，并用辗转相除法算出结果.
3. 设 a，b 为正整数，a，b 互素的充要条件是存在整数 x，y，使 $ax+by=1$. 这个结论正确吗?
4. 你能找到一个整系数二次多项式 $f(x)$，当 x 取正整数时，$f(x)$ 都是素数吗?

Ⅲ 巩固与提高

1. 证明：设 $n>0$，$a^n|b^n$，则 $a|b$.
2. 证明：若 2^n+1 为素数，必有 $n=2^m$，m 为自然数.
3. 设 $p>5$，且 p 和 $2p+1$ 都为素数，证明：$4p+1$ 必为合数. (提示：写 $p=3k+r$)
4. 设 $n>1$ 为奇数，证明：

$$n\left|\left(1+\frac{1}{2}+\cdots+\frac{1}{n-1}\right)(n-1)!\right.$$

（提示：考虑$\frac{1}{k}+\frac{1}{n-k}$，$1\leqslant k\leqslant n-1$）

5. 证明：设a，b为正整数，则等差数列a，$2a$，…，ba中能被b整除的项的个数等于(a,b).

6. 证明：$(a,[b,c])=[(a,b),(a,c)]$.

7. 设m为正整数，k为大于1的正整数，证明$m(m+1)$不是任何整数的k次幂.（提示：用算术基本定理）

8. 证明形如$4m+3$的素数有无穷多个.

Ⅳ 自测与评估

1. 求1 000 027的素因数分解式.

2. 求$(198,252)$.

3. 求$111x-321y=75$的正整数解.

4. 设$(m-p)\mid(mn+pq)$，证明：$(m-p)\mid(mq+np)$.

5. 设$(a,b)=1$，证明：$(a+b,a^2+b^2)=1$或2.
（提示：设$d=(a+b,a^2+b^2)$，证明$d\mid 2$）

秦九韶[1]

秦九韶（1202—1261）是我国南宋时期的数学家，年轻时随父亲在南宋京都（今杭州）太史局见习天文、历算. 1244 年和 1254 年曾先后两次在建康府（今南京）作官，都任职不久便离职回家. 1261 年左右又到梅州（今广东梅县）赴任，当年卒于住所. 1247 年 9 月著成数学名著《数学九章》18 卷，提出了求解一次同余方程组的“大衍求一术”和求高次方程数值解的“正负开方术”，是两项具有世界意义的学术成就，此外，在“联立一次方程”“勾股测量”等方面也有所创新. 他提出的“已知三边求三角形面积”的“秦九韶公式”与著名的“海伦公式”相当.

[1] 张奠宙主编《中学教学全书（数学卷）》，上海教育出版社，1996.

b 用 m 去除所得的余数相同，就称 a 和 b 对模 m 同余，记作 $a\equiv b(\mathrm{mod}\ m)$. 如果余数不同，则称 a，b 对模 m 不同余，记作 $a\not\equiv b(\mathrm{mod}\ m)$.

同余

当你看到一辆汽车跑过时，你思考过该车号码有什么特征吗？譬如，它是 3，9，7 或 11 的倍数吗？更普遍的是你在小学遇到的两整数相除的余数问题. 为解决这些问题以及更深层次的整数问题，本章引出同余的概念及其运算. 这类运算与你熟悉的运算不同. 例如，通常两数之积为零，其中至少有一数为零. 而同余乘法却不同，非零因子之积可能为零. 这确实有点怪异. 但当你进入这个领域，你会明白其中的道理，你还会发现许多新奇的数学事实.

2.1 同余及其基本性质

在日常生活中，常常需要考虑整数用某一固定的正整数去除的余数，比如知道某月 1 号是星期二，那么该月的 8 号，15 号，29 号都是星期二，因为这些号数用 7 去除余数都是 1，又如 10 岁的人属牛，那么 22 岁，34 岁，58 岁的人都属牛，因为这些年龄数用 12 去除余数都是相同的.

定义 给定一个正整数 m，把它称为模. 如果整数 a 和 b 用 m 去除所得的余数相同，就称 a 和 b 对模 m 同余❶，记作 $a\equiv b(\mathrm{mod}\ m)$. 如果余数不同，则称 a，b 对模 m 不同余，记作 $a\not\equiv b(\mathrm{mod}\ m)$.

注

❶“对模 m 同余”有时可说成“模 m 同余”.

例如，8 和 15 除以 7 都余 1，称 8 和 15 对模 7 同余，记为

$$8\equiv 15(\mathrm{mod}\ 7).$$

又如 34 和 58 除以 12 余数都是 10，称 34 和 58 对模 12 同余，记为

$$34\equiv 58(\mathrm{mod}\ 12).$$

例 1 (1) 说明 $-1\equiv 4(\mathrm{mod}\ 5)$；

(2) 证明：对任何整数 x，$x^2\equiv 0$ 或 $1(\mathrm{mod}\ 4)$.

解：(1) $-1=(-1)\times 5+4$，此式表明，-1 除以 5 的余数是 4.

(2) 设 $x=4k+r$，$r=0,1,2,3$. 则

$$\begin{aligned} x^2 &= 16k^2+8kr+r^2 \\ &= 4(4k^2+2kr)+r^2, \\ \Rightarrow x^2 &\equiv r^2\equiv 0 \text{ 或 } 1\ (\mathrm{mod}\ 4). \end{aligned}$$

由定义容易得到以下的基本性质：

(1) $a\equiv a(\bmod m)$；(自反性)

(2) 若 $a\equiv b(\bmod m)$，则 $b\equiv a(\bmod m)$；(对称性)

(3) 若 $a\equiv b(\bmod m)$，$b\equiv c(\bmod m)$，则 $a\equiv c(\bmod m)$. (传递性)

下面的定理建立了同余和整除之间的关系.

定理 1 整数 a，b 对模 m 同余的充分必要条件是 $m|(a-b)$.

证明：必要性. 设 $a=mq_1+r$，$b=mq_2+r$，$0\leqslant r<m$，则

$$a-b=m(q_1-q_2),$$

即 $m|(a-b)$.

充分性. 设 $a=mq_1+r_1$，$0\leqslant r_1<m$，$b=mq_2+r_2$，$0\leqslant r_2<m$，则

$$a-b=m(q_1-q_2)+(r_1-r_2).$$

因为 $m|(a-b)$，所以 $m||r_1-r_2|$. 但 $|r_1-r_2|<m$，故必有 $r_1=r_2$，即

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

由定理 1 和整除的性质可以得到下述与相等类似的性质.

性质 1 若 $a\equiv b(\bmod m)$，$a_1\equiv b_1(\bmod m)$，则

(1) $a+a_1\equiv b+b_1(\bmod m)$；

(2) $aa_1\equiv bb_1(\bmod m)$.

证明：(1) 由 $m|(a-b)$，$m|(a_1-b_1)$，可得 $m|[(a-b)+(a_1-b_1)]$，即

$$m|[(a+a_1)-(b+b_1)].$$

(2) 由 $m|(a-b)$，$m|(a_1-b_1)$，可得 $m|[a_1(a-b)+b(a_1-b_1)]$，即 $m|(aa_1-bb_1)$.

还可以得到与相等不类似的性质.

性质 2 若 $ac\equiv bc(\bmod m)$，且 $(c,m)=d$，则

$$a\equiv b\left(\bmod \frac{m}{d}\right).$$

例如，由 $17\times 6\equiv 25\times 6(\bmod 8)$及$(6,8)=2$，可知$17\equiv 25(\bmod 4)$.

证明：由 $m|c(a-b)$，知 $\dfrac{m}{d}\left|\dfrac{c}{d}(a-b)\right.$. 又由 $\left(\dfrac{m}{d},\dfrac{c}{d}\right)=1$，可得

$$\frac{m}{d}\left|(a-b)\right.,$$

对于不同模的同余式有

性质 3 若 $a\equiv b\ (\bmod m_i)$，$1\leqslant i\leqslant n$，则

$$a\equiv b\ (\bmod [m_1,m_2,\cdots,m_n]).$$

证明：由 $m_i|(a-b)$，$1\leqslant i\leqslant n$，知 $(a-b)$ 是 m_1，m_2，…，m_n 的一个公倍数，故有 $[m_1,m_2,\cdots,m_n]|(a-b)$.

例 2 证明：$641|F_5$，其中 $F_5=2^{32}+1$.

证明：$2^8=256$，$2^{16}=65\ 536\equiv 154\ (\bmod 641)$.

$2^{32}\equiv(154)^2=23\ 716\equiv 640\equiv -1\ (\bmod 641)$.

这个结果否定了费马的一个猜想：若 n 为自然数，则 $2^{2^n}+1$ 都是素数.

例 3 求 23^{23} 的末位数字.

解：$23^{23}\equiv 3^{23}\equiv(3^2)^{11}\cdot 3\equiv(10-1)^{11}\cdot 3\equiv -1\cdot 3\equiv 7(\mathrm{mod}\ 10)$.

因此 23^{23} 的末位数字是 7.

习题 2-1

1. 证明：设 $d\geqslant 1$，$d\mid m$，$a\equiv b(\mathrm{mod}\ m)$，则 $a\equiv b(\mathrm{mod}\ d)$.

2. 证明：设 $d\neq 0$，$a\equiv b(\mathrm{mod}\ m)$，则 $ad\equiv bd(\mathrm{mod}\ |d|m)$.

3. 证明：设 d 为 a，b 及 m 的正的公约数，$a\equiv b(\mathrm{mod}\ m)$，则

$$\frac{a}{d}\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right).$$

4. 求 14^{14} 的末两位数.

5. 求 3^{406} 的个位数.

6. 求 13 除 6^{48} 的最小非负余数.

7. 求证：$168\mid(16^{6n}-1)$，其中 n 为任意自然数.

2.2 特殊数的整除特征

一个整数是否能被另一个整数整除，一般通过试除就可知，但有时这样做计算量较大. 那么有没有其他较简单的方法呢？本节就讨论这个问题.

定理 1 一个整数 a 能被 3(或 9)整除的充分必要条件是它的十进制数各位数字之和能被 3(或 9)整除.

证明：不妨设 $a>0$，把 a 写成十进位数的形式

$$a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_110+a_0,\ 0\leqslant a_i<10,\ 0\leqslant i\leqslant n,\ a_n\neq 0.$$

因为 $10\equiv 1(\mathrm{mod}\ 3)$，所以

$$a\equiv a_n+a_{n-1}+\cdots+a_1+a_0(\mathrm{mod}\ 3). \qquad ①$$

因为$10\equiv 1(\mathrm{mod}\ 9)$，所以①式对模 9 也成立.

例 1 判断 $a=10\ 293\ 762$ 是否是 3 和 9 的倍数.

解：由 $1+0+2+9+3+7+6+2=30$，$3\mid 30$，$9\nmid 30$，故 a 是 3 的倍数，但不是 9 的倍数.

定理 2 设正整数 a 写成 1 000 进制可表示为 $a=a_m\ 1\ 000^m+a_{m-1}\ 1\ 000^{m-1}+\cdots+a_1\ 1\ 000+a_0$，$0\leqslant a_i<1\ 000$，$0\leqslant i\leqslant m$，$a_m\neq 0$，则 7(或 11，或 13)整除 a 的充分必要条件是 7(或 11，或 13)整除 $\sum\limits_{i=0}^{m}(-1)^ia_i$.

证明：由 $1\ 000\equiv -1(\mathrm{mod}\ 7)$，故

$$\begin{aligned}a&\equiv a_m(-1)^m+a_{m-1}(-1)^{m-1}+\cdots-a_1+a_0\\&=\sum_{i=0}^{m}(-1)^ia_i(\mathrm{mod}\ 7). \qquad ②\end{aligned}$$

由$1\ 000\equiv -1(\mathrm{mod}\ 11)$，$1\ 000\equiv -1(\mathrm{mod}\ 13)$，故②式对模 11 和模 13 也分别成立.

例 2 判断 $a=75\ 312\ 289$ 是否是 7，11 和 13 的倍数.

解：由 $a=75\times 1\ 000^2+312\times 1\ 000+289$，$\sum_{i=0}^{2}(-1)^i a_i=289-312+75=52$，及 $13\mid 52$，$7\nmid 52$，$11\nmid 52$，故 a 是 13 的倍数，但不是 7 和 11 的倍数.

这个判断方法是将 a 从末位开始按 3 位数分段，如 $a=75,312,289$. 右起第一段取正号，以下各段负正交替. 求代数和，再看该代数和是否被 7(或 11，13)整除.

例 3 检查下列运算结果是否正确：

(1) $348\times 267=92\ 616$；

(2) $9\ 031\times 367=3\ 313\ 377$.

解：(1) 348 与 267 各位数字之和是 3 的倍数，因此积应是 9 的倍数. 而92 616各位数字之和为不是 9 的倍数. 因此，计算错误.

(2) $31-9=22$ 是 11 的倍数. $377-313+3=67$ 不是 11 的倍数. 可见计算有误.

习题 2-2

1. 设 $a>0$，证明：11 整除 a 的充分必要条件是：当 a 写成十进制表示，并由个位开始确定数位的奇偶时，它的奇数位数字和与偶数位数字和的差能被 11 整除.

2. 试判定 758 957 628 是否是 11 的倍数.

3. 设 $a>0$，证明：当 a 写成十进制表示时，7(或 11，或 13)整除 a 的充要条件是：a 的末三位数字所表示的数与末三位以前的数字所表示的数的差能被 7(或 11，或 13)整除.

4. 试判断 75 523，1 095 874，868 967 中，哪些是 7 的倍数？哪些是 11 的倍数？哪些是 13 的倍数？

2.3 剩余类及其运算

在同余式的运算中，两个同余数起的作用是一样的，可以把互相同余的这些数归于一类. 由此引进剩余类的概念.

定义 1 设 m 为正整数，所有对 m 同余的整数所组成的集合称为模 m 的一个剩余类.

由定义，全体整数对模 m 可分为 m 个互不相交的剩余类 K_0，K_1，…，K_{m-1}，其中

$$K_r=\{qm+r\},\ q=0,\ \pm 1,\ \pm 2,\ \cdots,\ 0\leqslant r<m.$$

例如，对模 3，其剩余类有如下三个：

$$K_0=\{3q\mid q\in\mathbf{Z}\},$$
$$K_1=\{3q+1\mid q\in\mathbf{Z}\},$$
$$K_2=\{3q+2\mid q\in\mathbf{Z}\}.$$

在数学中，不只是整数、实数或复数可以定义运算，向量、函数、矩阵等数学对象也可以定义运算. 本节对剩余类所组成的集合引入运算.

用 $\bar{a}$ 表示整数 a 所属的模 m 的剩余类，$\mathbf{Z}_m$ 表示模 m 的所有剩余类所组成的集合，设 a，$b\in\mathbf{Z}_m$，定义

$$\bar{a}+\bar{b}=\overline{a+b},$$

$$\bar{a}\,\bar{b}=\overline{ab}.$$

例如，对模 5，所有剩余数所组成的集合 $\mathbf{Z}_5=\{K_0, K_1, K_2, K_3, K_4\}$，其中

$$K_r=\{5q+r \mid q\in\mathbf{Z}\},\ r=0, 1, 2, 3, 4.$$

可以分别用其中一个元素作代表(代表元)，比如用 r 作代表，这样，$K_0=\bar{0}$，$K_1=\bar{1}$，$K_2=\bar{2}$，$K_3=\bar{3}$，$K_4=\bar{4}$.

由定义可知

$$\bar{0}+\bar{1}=\bar{1},\ \bar{2}+\bar{3}=\bar{0},\ \bar{3}+\bar{4}=\bar{2};$$

$$\bar{0}\cdot\bar{1}=\bar{0},\ \bar{2}\cdot\bar{3}=\bar{1},\ \bar{3}\cdot\bar{4}=\bar{2},\ \text{等等}.$$

模 m 的所有剩余类集合可表为

$$\mathbf{Z}_m=\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \cdots, \overline{m-1}\}.$$

注意这里的加法运算对象虽然是集合，但与集合的并集运算是不同的. 同样这里的乘法运算与集合的交集运算也是不同的.

下面介绍代数学中关于环的定义.

定义 2 设在非空集合 R 上定义了两个代数运算，一个叫加法，记为 $a+b$，一个叫乘法，记为 ab，它们适合

1. 关于加法的以下规则：

(1) $(a+b)+c=a+(b+c)$；(加法结合律)

(2) $a+b=b+a$；(加法交换律)

(3) 在 R 中有元素 0，使对任意的 $a\in R$，$a+0=a$；

(4) 若 $a\in R$，则存在 $b\in R$，使 $a+b=0$.

2. 关于乘法的结合律：

$$a(bc)=(ab)c.$$

3. 关于加法和乘法的分配律：

$$a(b+c)=ab+ac,$$

$$(b+c)a=ba+ca.$$

这样的非空集合 R 连同这两个运算称为环.

容易看出全体整数对于数的加法和乘法构成一个环，也不难验证，模 m 的全体剩余类 $\mathbf{Z}_m$ 对于以上定义的加法和乘法也构成一环. 人们可能认为剩余类环 $\mathbf{Z}_m$ 和整数环在运算性质上是完全相同的，但事实并非如此.

在代数中，如果 a，b 都非零，而 $ab=0$，则称 a 和 b 为零因子. 在整数环，实数环和复数环中都不存在零因子，但当$m>1$ 是合数时，$\mathbf{Z}_m$ 中却存在零因子. 事实上，当 m 是合数时，可设 $m=st$，$1<s<m$，$1<t<m$. 此时 $s\neq\bar{0}$，$t\neq\bar{0}$，但

$$s\bar{t}=\bar{s}\bar{t}=\bar{m}=\bar{0}.$$

因此，s 与 t 都是零因子. 例如，在 $\mathbf{Z}_6$ 中，因为 $\bar{2}\cdot\bar{3}=\bar{0}$，所以 $\bar{2}$ 与 $\bar{3}$ 是零因子，$\bar{4}$ 也是零因子❶，而 $\bar{0}$，$\bar{1}$，$\bar{5}$ 不是零因子.

注

❶ $\bar{4}$ 是 $\mathbf{Z}_6$ 中零因子，因为 $\bar{4}\cdot\bar{3}=\bar{0}$.

思考与讨论

当 m 是素数时，剩余类环 $\mathbf{Z}_m$ 中是否存在零因子？

例　列出 $\mathbf{Z}_7$ 的乘法表

解：

	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

表中数字 0，1，2，…，6 分别代表剩余数类 $\bar{0}$，$\bar{1}$，$\bar{2}$，…，$\bar{6}$. 这里的乘法与数的乘法是不同的. 例如表中第四行第五列表示 $\bar{3}\cdot\bar{4}=\bar{5}$，第五行与第六列表示 $\bar{4}\cdot\bar{5}=\bar{6}$.

习题 2-3

1. 列出 $\mathbf{Z}_8$ 的乘法表.
2. 找出 $\mathbf{Z}_{12}$ 中的零因子.
3. 从任意 101 个正整数中，总可以选出 11 个数，其和是 11 的倍数. 试证之.

2.4　剩余系和欧拉函数

为了在下一节能够证明数论中一个著名的定理——欧拉定理，我们需要有关剩余系和欧拉函数的知识.

定义 1　设 $\varphi(1)=1$，当 $n>1$，$\varphi(n)$ 表示 1，2，…，$n-1$ 中与 n 互素的数的个数，称 $\varphi(n)$ 为欧拉函数.

例如，当 p 为素数时，由定义即知 $\varphi(p)=p-1$. 又如 $\varphi(6)=2$，$\varphi(8)=4$，$\varphi(15)=8$.

定义 2 若模 m 的某个剩余类中的数与 m 是互素的，则称此剩余类为模 m 的互素剩余类❶.

例如，模 6 的互素剩余类有$\bar{1}$，$\bar{5}$.

对模 m，有 $\varphi(m)$个互素剩余类.

注

❶ 在模 m 的一个剩余类中，只要有一个数与 m 互素，则此剩余类中所有的数都与 m 互素.

思考与讨论

为什么在模 m 的一个剩余类中只要有一个数和模 m 互素，那么此剩余类的所有数都和 m 互素?

定义 3 从模 m 的每个剩余类中各取一个数，得到一个由 m 个数组成的集合，称为模 m 的一个完全剩余系. 从模 m 的每个互素剩余类中各取一个数，得到一个由 $\varphi(m)$个数组成的集合称为模 m 的一个简化剩余系.

例如，$\{0, 1, 2, 3, 4, 5\}$，$\{12, 7, 14, 21, 10, 47\}$ 是模 6 的完全剩余系. $\{1, 5\}$，$\{13, 41\}$是模 6 的简化剩余系.

显然，对固定的模 m，有无数多个完全剩余系和简化剩余系. 任意 m 个整数，只要它们对模 m 两两不同余，这 m 个数就是模 m 的一个完全剩余系. 任意 $\varphi(m)$个整数，只要它们对模 m 两两不同余并且都和 m 互素，这 $\varphi(m)$个数就是模 m 的一个简化剩余系.

定理 1 设 m 是正整数，k，l 是整数，且$(k, m)=1$，则：

(1) 当 x 遍历模❷m 的一个完全剩余系时，$kx+l$ 也遍历模 m 的一个完全剩余系；

(2) 当 x 遍历模 m 的一个简化剩余系时，kx 也遍历模 m 的一个简化剩余系.

注

❷ x 遍历某一个数集是指 x 能取到该数集的每一个数.

证明：(1) 只需证明当 x_0，x_1，…，x_{m-1}是模 m 的一个完全剩余系时，kx_0+l，kx_1+l，…，$kx_{m-1}+l$ 对模 m 两两不同余即可. 用反证法，设

$$kx_i+l\equiv kx_j+l \pmod m,\ 0\leqslant i<j\leqslant m-1,$$

则

$$x_i\equiv x_j \pmod m.$$

这与 x_0，x_1，…，x_{m-1}是模 m 的一个完全剩余系矛盾.

(2) 设 x_1，x_2，…，$x_{\varphi(m)}$是模 m 的一个简化剩余系. 由 (1) 知 kx_1，kx_2，…，$kx_{\varphi(m)}$对模 m 两两不同余，又当 $1\leqslant i\leqslant\varphi(m)$时，因$(k, m)=1$，$(x_i, m)=1$，故得$(kx_i, m)=1$.

定理 2 设$(m_1, m_2)=1$，则：

(1) 当 x，y 分别遍历模 m_1 和模 m_2 的一个完全剩余系时，m_2x+m_1y 也遍历模 m_1m_2 的一个完全剩余系；

(2) 当 x，y 分别遍历模 m_1 和模 m_2 的一个简化剩余系时，m_2x+m_1y 也遍历模 m_1m_2

的一个简化剩余系.

证明：(1) 若 $m_2x_1+m_1y_1\equiv m_2x_2+m_1y_2 \pmod{m_1m_2}$，则有

$$m_2x_1\equiv m_2x_2 \pmod{m_1}.$$

由于$(m_1, m_2)=1$，故

$$x_1\equiv x_2 \pmod{m_1}.$$

同理可得

$$y_1\equiv y_2 \pmod{m_2}.$$

因此当 x，y 分别遍历模 m_1 和模 m_2 的一个完全剩余系时，m_2x+m_1y 所取的 m_1m_2 个值对于模 m_1m_2 是互不同余的，从而是模 m_1m_2 的一个完全剩余系.

(2) 若$(x, m_1)=(y, m_2)=1$，则有

$$(m_2x+m_1y, m_1)=(m_2x, m_1)=(x, m_1)=1,$$

$$(m_2x+m_1y, m_2)=(m_1y, m_2)=(y, m_2)=1,$$

从而

$$(m_2x+m_1y, m_1m_2)=1.$$

于是，当 x，y 分别遍历模 m_1 和模 m_2 的一个简化剩余系时，m_2x+m_1y 所取的值和 m_1m_2 是互素的，且由 (1) 知这 $\varphi(m_1)\varphi(m_2)$ 个数对模 m_1m_2 是两两不同余的. 因此以下只需证明：

当$(n, m_1m_2)=1$ 时，存在整数 x_0，y_0，使

$$n\equiv m_2x_0+m_1y_0 \pmod{m_1m_2},\ (x_0, m_1)=1,\ (y_0, m_2)=1.$$

由(1)知，存在 x_0，y_0 使

$$n\equiv m_2x_0+m_1y_0 \pmod{m_1m_2}.$$

若$(x_0, m_1)>1$，则有素数 q，使 $q\mid x_0$，$q\mid m_1$，由上式即得 $q\mid n$，这与 n 和 m_1 互素矛盾.

同理可证$(y_0, m_2)=1$.

推论 若$(m_1, m_2)=1$，则 $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$.

由推论可得欧拉函数 $\varphi(n)$的计算公式.

定理 3 设 $n>1$，且 n 的标准分解式为 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

证明：由定理 2 推论可得

$$\varphi(n)=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k}).$$

以下证明 $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$.

因为 p 是素数，所以不与 p^α 互素的数都是 p 的倍数. 1，2，3，…，p^α 中是 p 的倍数的数是

$$p, 2p, 3p, \cdots, p^{\alpha-1}p.$$

这些数共有 $p^{\alpha-1}$个，其余的数都和 p 互素，而从 1 到 p^α 共有 p^α 个数. 于是，从 1 到 p^α 有 $(p^\alpha-p^{\alpha-1})$个数与 p^α 互素. 故从 1 到$(p^\alpha-1)$也有$(p^\alpha-p^{\alpha-1})$个数与 p^α 互素. 因此由欧拉函数的定义可得

$$\varphi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}.$$

由此

$$\begin{aligned}\varphi(n)&=(p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\cdots(p_k^{\alpha_k}-p_k^{\alpha_k-1})\\&=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\&=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

例 1 计算 $\varphi(36)$.

解：$36=2^2\cdot 3^2$，因此

$$\varphi(36)=36\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=12.$$

我们不妨验证一下：

从 1 到 35 共有 35 个数. 这 35 个数中，恰有 1，5，7，11，13，17，19，23，25，29，31，35 与 36 互素. 共有 12 个数与 36 互素. 可见 $\varphi(36)=12$.

例 2 设 p 是奇素数，且 $2^n\not\equiv 1 \pmod p$，证明：

$$1^n+2^n+\cdots+(p-1)^n\equiv 0 \pmod p.$$

证明：由 $(2,p)=1$，$\{1,2,\cdots,p-1\}$ 是模 p 的一个简化剩余系知，2×1，2×2，…，$2\times(p-1)$ 也是模 p 的一个简化剩余系. 这两个简化剩余系的数，两两对模 p 同余. 故有

$$1^n+2^n+\cdots+(p-1)^n\equiv(2\times 1)^n+(2\times 2)^n+\cdots+(2(p-1))^n \pmod p,$$

即

$$(2^n-1)(1^n+2^n+\cdots+(p-1)^n)\equiv 0 \pmod p.$$

由题设，$p\nmid(2^n-1)$，所以

$$p\mid(1^n+2^n+\cdots+(p-1)^n).$$

习题 2-4

1. 设 $2\mid m$，证明：在模 m 的任意一个完全剩余系中有一半是偶数，另一半是奇数.

2. 证明：$1^5+2^5+\cdots+10^5$ 是 11 的倍数. （提示：用例 2）

3. 求 $\varphi(10\,080)$ 的值.

4. 设 $n>2$，证明：$\varphi(n)$ 是偶数. （提示：用定理 3）

5. 设 p 为素数，求 $\varphi(p^{100})+\varphi(p^{99})+\cdots+\varphi(p^2)+\varphi(p)$.

2.5 欧拉定理

欧拉定理是数论中最重要的定理之一，有着广泛的应用.

欧拉定理 设 $m>1$，$(a, m)=1$，则

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

证明：设 x_1，x_2，…，$x_{\varphi(m)}$ 是模 m 的一个简化剩余系，由 $(a, m)=1$ 和上节定理 1 知 ax_1，ax_2，…，$ax_{\varphi(m)}$ 也是模 m 的一个简化剩余系. 因此有

$$(ax_1)(ax_2)\cdots(ax_{\varphi(m)})\equiv x_1x_2\cdots x_{\varphi(m)} \pmod m,$$

即

$$a^{\varphi(m)}(x_1x_2\cdots x_{\varphi(m)})\equiv x_1x_2\cdots x_{\varphi(m)} \pmod m.$$

又由 $(x_i, m)=1$，$1\leqslant i\leqslant\varphi(m)$ 即得

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

例如，$a=5$，$m=6$，$\varphi(6)=2$. $5^{\varphi(6)}=5^2\equiv 1 \pmod 6$.

推论 （费马小定理）设 p 为素数，$(a, p)=1$，则

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

例 1 证明 $15|(49^4-1)$.

证明：由 $\varphi(15)=\varphi(3)\varphi(5)=2\times 4=8$ 及欧拉定理即得

$$49^4\equiv 7^8\equiv 7^{\varphi(15)}\equiv 1 \pmod{15}.$$

所以 $15|(49^4-1)$.

例 2 7^{362} 的末两位数是什么？

解：由 $\varphi(100)=100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=40$ 及欧拉定理即得

$$7^{40}\equiv 1 \pmod{100}.$$

又由 $362=9\times 40+2$ 可得

$$7^{362}\equiv 7^2\equiv 49 \pmod{100},$$

所以 7^{362} 的末两位数是 49.

例 3 证明 $1\,777^{1\,885}\equiv 27 \pmod{41}$.

证明：由 $1\,777\equiv 14 \pmod{41}$ 得

$$1\,777^{1\,885}\equiv 14^{1\,885} \pmod{41}.$$

由费马小定理知

$$14^{40}\equiv 1 \pmod{41}.$$

又由 $1\,885=47\times 40+5$ 得

$$\begin{aligned}14^{1\,885}&\equiv 14^5\equiv 196\cdot 196\cdot 14\equiv(-9)\cdot(-9)\cdot 14\\&\equiv 81\cdot 14\equiv(-1)\cdot 14\equiv 27 \pmod{41}.\end{aligned}$$

例 4 今天是星期一，问这以后的第 47^{37} 天是星期几？

解：由费马小定理知

$$47^6 \equiv 1 \pmod 7.$$

又由 $37=6\times 6+1$ 可得

$$47^{37} \equiv 47 \equiv 5 \pmod 7.$$

所以是星期六.

习题 2-5

1. 求 7^{355} 的个位数.
2. 求 3^{400} 的末两位数.
3. 求 $8^{1\,964}$ 除以 13 的余数.
4. 今天是星期三，问今天以后的第 $10^{10^{10}}$ 天是星期几?
5. 证明：设 p 是素数，a 为任意整数，则 $a^p \equiv a \pmod p$.

2.6 不定方程与同余

对于某些较特殊的不定方程，可以利用同余知识来解决. 这种方法的要点是根据所给方程的特点选取某个大于 1 的正整数为模来导出矛盾，否定不定方程有解. 现举例说明.

例 1 证明方程 $x^2+y^2-4z^2=3$ 没有整数解.

证明：取 4 为模. 因对任意整数 x，有 $x^2 \equiv 0, 1 \pmod 4$，故对任意整数 x, y, z，有

$$\text{方程左边} \equiv 0, 1, 2 \pmod 4,$$

但

$$\text{方程右边} \equiv 3 \pmod 4,$$

所以方程无整数解.

例 2 证明方程 $x^2+2y^2=8y+5$ 没有整数解.

证明：取 8 为模. 因对任意整数 x，有 $x^2 \equiv 0, 1, 4 \pmod 8$，故对任意整数 x, y, z，

$$\text{方程左边} \equiv 0, 1, 2, 3, 4, 6 \pmod 8,$$

但

$$\text{方程右边} \equiv 5 \pmod 8,$$

所以方程无整数解.

例 3 证明方程 $x^3+2=7y$ 没有整数解.

证明：取 7 为模. 因对任意整数 x，有 $x^3 \equiv 0, \pm 1 \pmod 7$. 故对任意整数 x, y, z，

$$\text{方程左边} \equiv 1, 2, 3 \pmod 7,$$

但

$$\text{方程右边} \equiv 0 \pmod 7,$$

所以方程无整数解.

例 4 证明 $x^3+y^3+z^3=9w^3+4$ 没有整数解.

证明：取 9 为模. 因对任意整数 x，有 $x^3\equiv 0,\pm 1 \pmod 9$，故对任意整数 x，y，z，w，有

$$\text{方程左边}\not\equiv 4 \pmod 9,$$

但

$$\text{方程右边}\equiv 4 \pmod 9,$$

所以方程无整数解.

例 5 求方程 $(x-1)!=x^y-1$，$x>1$ 的正整数解.

解：设 (x,y)，$x>1$ 是方程的正整数解.

取 x 为模，因为 x 满足方程，所以有

$$(x-1)!\equiv -1 \pmod x,$$

故 x 是素数. 这是因为如果 x 不是素数，则 $x=kd$，$1<k$，$d<x$. 由 $(x-1)!\equiv -1 \pmod x$，可知 $x\mid[(x-1)!+1]$，因而 $d\mid[(x-1)!+1]$. 由此及 $d\mid(x-1)!$ 得 $d\mid 1$ 矛盾.

将 $x=2$，3，5 分别代入方程可得解

$$(x,y)=(2,1),(3,1),(5,2).$$

下设 x 为大于 5 的素数.

由

$$(x-1)!=1\cdot 2\cdot\cdots\cdot\frac{x-1}{2}\cdot\cdots\cdot(x-1)$$

知

$$(x-1)^2\mid(x-1)!. \qquad ①$$

由二项式定理可得

$$x^y-1=\{(x-1)+1\}^y-1=A(x-1)^2+y(x-1), \qquad ②$$

此处 A 是一个整数.

由原方程，①和②可得

$$(x-1)\mid y,$$

从而有

$$x^y-1\geqslant x^{x-1}-1>(x-1)!,$$

这个矛盾的结果说明当 $x>5$ 时方程没有正整数解，所以方程的全部正整数解为

$$(x,y)=(2,1),(3,1),(5,2).$$

习题 2-6

1. 证明方程 $x^2+y^2=4z+3$ 没有整数解.

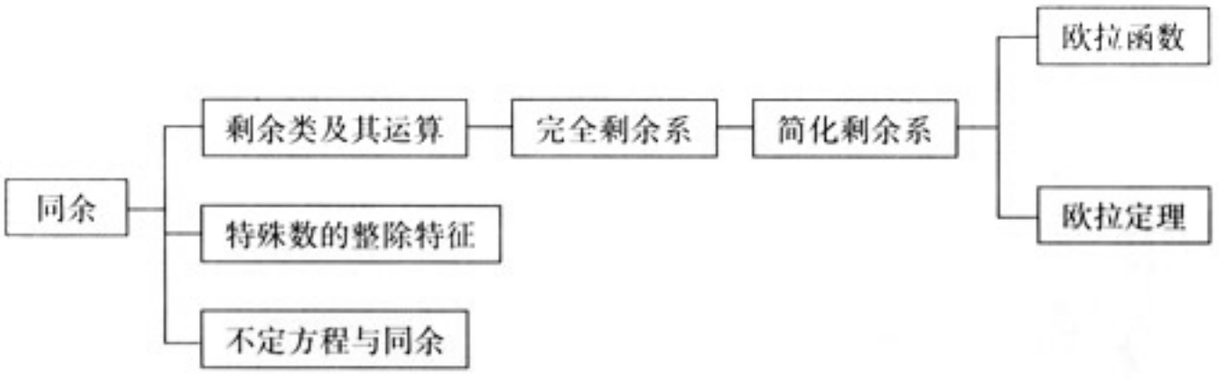
2. 证明方程 $x^3+y^3+z^3=9w^3-4$ 没有整数解.

3. 证明方程 $(3a+1)x^2+(3b+1)y^2=3z^2$ 仅有整数解 $x=y=z=0$.

4. 证明方程 $y^2=x^3+7$ 没有整数解.

本章小结

Ⅰ 知识结构



Ⅱ 思考与交流

1. 普通算式的等号“=”与同余的等号“≡”有什么区别？用同余等号时要特别注意什么？
2. 你能用欧拉函数计算公式证明素数的个数有无穷多个吗？
3. 费马小定理是欧拉定理当 m 是素数时的特例，你能用费马小定理推导出欧拉定理吗？

Ⅲ 巩固与提高

1. 证明：$70!\equiv 61!\pmod{71}$.（提示：$70!\equiv 61!\times 62\times 63\times\cdots\times 70\equiv 61!\times(-9)\times(-8)\times\cdots\times(-1)\pmod{71}$.）
2. 设素数 $p\geqslant 7$，证明：$240\mid(p^4-1)$.
3. 设 $(a,91)=(b,91)=1$，证明：$a^{12}-b^{12}\equiv 0\pmod{91}$.
4. 证明：对于任何整数 $k\geqslant 0$，$7\mid(2^{6k+1}+3^{6k+1}+5^{6k}+1)$.
5. 设 p 是奇素数，$m^p+n^p\equiv 0\pmod{p}$，证明：$m^p+n^p\equiv 0\pmod{p^2}$.
6. 设 $m>1$，$(a,m)=1$，d 是满足 $a^x\equiv 1\pmod{m}$ 的最小正整数，证明：$d\mid\varphi(m)$.（提示：用带余除法）

Ⅳ 自测与评估

1. 求 3^{406} 的个位数.

2. 证明：设 n 是任意整数，则 $n^9-n^3\equiv 0 \pmod{504}$.

3. 设 p 为素数，$a^p\equiv b^p \pmod{p}$，证明：$a^p\equiv b^p \pmod{p^2}$.（提示：用费马小定理）

4. 设 $l\geqslant 3$，证明：$5^{2^{l-2}}\equiv 1 \pmod{2^l}$.（提示：用数学归纳法）

5. 设 p 是一个奇素数，$(a,p)=1$，问对模 p，$a^{\frac{p-1}{2}}$ 可取哪些值？（提示：用费马小定理）

6. 设 m，n 为正整数，证明：$\varphi(mn)=(m,n)\varphi([m,n])$.（提示：$mn$ 和 $[m,n]$ 有相同的素数因子）

第三章 同余方程

大约在一千五百年前，我们的祖先创立的“孙子定理”在数学领域占有重要地位. 国际上称之为中国剩余定理. “孙子定理”的光辉之处在于，它把困难复杂的问题化解为几个易解的子问题，并将子问题标准化，然后用标准的、有效的算法，求得原问题的解. 这种思想方法对许多学科和实际工作都是适用的.

本章围绕“孙子定理”展开. 首先给出同余方程的概念和一些必要的结论，介绍解同余方程的方法；然后由“孙子定理”引出同余方程组，再由该定理给出标准的解法；最后用它解决数论中的一些经典问题，以及现代通讯技术中的编码问题.

3.1 同余方程的概念

解方程是代数的重要课题. 本章讨论和解代数方程类似的问题：解同余方程.

定义 1 设 $n\geqslant 0$，$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是整数系数多项式，m 是大于 1 的整数，则称

$$f(x)\equiv 0 \pmod m \qquad ①$$

为模 m 的一元同余方程，简称同余方程. 若 $m\nmid a_n$，则称同余方程①的次数为 n. 若整数 c 代入①式使①式成立，则称 c 为①式的解. 解同余方程①就是求出①式的全部解.

由同余的性质易知，若 c 是①式的解，则满足 $x\equiv c \pmod m$ 所有整数 x 都是①式的解，因此我们将所有对模 m 同余的①式的解看成是相同的，而把对模 m 不同余的解才看作是不同的.

定义 2 若 c 是①式的解，则称 $x\equiv c \pmod m$ 为①式的一个解.

例如同余方程

$$x^2-11x+18\equiv 0 \pmod 4$$

有解 $x=2$，那么

$$x=2+4p \quad (p \text{ 为整数})$$

都是方程的解. 但我们把这些解看作是相同的. 这个解表为

$$x\equiv 2 \pmod 4.$$

该方程还有解 $x\equiv 1 \pmod 4$，与 $x\equiv 2 \pmod 4$ 是不同的解.

方程①的解的个数不会超过 m，而且可以通过将 0，1，2，…，$m-1$ 逐个代入①而求出它的全部解.

例 1 解同余方程 $x^5+x+1\equiv 0 \pmod 7$.

解：将 0，1，2，3，4，5，6 逐个代入方程验算知 $x=2$，4 为其解，故此方程的全部解可表为

$$x\equiv 2 \pmod 7,$$
$$x\equiv 4 \pmod 7.$$

例 2 解同余方程 $x^2+1\equiv 0 \pmod 3$.

解：将 0，1，2 逐个代入方程知此方程无解.

例 3 解同余方程 $x^3-x\equiv 0 \pmod 6$.

解：因为相邻三整数之积为 6 的倍数，所以，对任何整数 x，有

$$x^3-x=(x-1)x(x+1)\equiv 0 \pmod 6,$$

故此方程有 6 个解：$x\equiv 0$，1，2，3，4，5(mod 6).

例 4 设 p 为素数，解同余方程 $(x+2)(x-p+2)\equiv 0 \pmod{p^2}$.

解：方程变为

$$(x+2)^2\equiv p(x+2) \pmod{p^2}.$$

因为 p 为素数，x 需满足 $p\mid(x+2)$. 反之，如果 $p\mid(x+2)$，则 x 也满足此方程. 因此方程的解为

$$x\equiv kp-2 \pmod{p^2},\ k \text{ 为整数}.$$

限制该同余方程的解在 0，1，2，…，p^2-1 之内，得 $k=1$，2，…，p. 这样该同余方程的解为 $x\equiv kp-2 \pmod{p^2}$，$k=1$，2，…，p 一共 p 个解.

从以上四例可以看出，同余方程①的解的个数是很不规则的.

习题 3-1

1. 解同余方程 $4x\equiv 2 \pmod 8$.
2. 设 p 为素数，解同余方程 $(x-1)(x-p-1)\equiv 0 \pmod{p^2}$.
3. 我们知道代数方程 $x^2+2x+2=0$ 无实数解，$x^2+2x+2\equiv 0 \pmod 5$ 是否有解？

3.2 一次同余方程

本节讨论最简单的模 m 的一次同余方程

$$ax\equiv b \pmod m. \qquad ①$$

先讨论判别①式有解的条件.

定理 1 设$(a, m)=1$，则①式有且仅有一解.

证明：由 1，2，…，m 是模 m 的一个完全剩余系，$(a, m)=1$ 知 a，$2a$，…，ma 也是模 m 的一个完全剩余系. 因此其中有且仅有一个整数 j，$1\leqslant j\leqslant m$ 满足

$$aj\equiv b \pmod m.$$

故 $x\equiv j \pmod m$就是①式的唯一解.

定理 2 若记 $d=(a, m)$，则①式有解的充分必要条件是 $d\mid b$. 若①式有解，则①式的解数是 d.

证明：易见①式有解的充分必要条件是二元一次不定方程

$$ax-my=b$$

有解. 由 1.7 节定理 1 即知①式有解的充分必要条件是$d\mid b$.

如①式有解，则 $d\mid b$，此时①式与同余方程

$$\frac{a}{d}x\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right) \qquad ②$$

的解是相同的.

由定理 1 知②式有唯一解，设为

$$x\equiv t_0\left(\mathrm{mod}\ \frac{m}{d}\right),\ 0\leqslant t_0<\frac{m}{d}.$$

因此①式的全部解可表示为 $t_0+k\frac{m}{d}$，$k=0$，±1，±2，….

考虑 d 个数 $t_0+i\frac{m}{d}$，$i=0$，1，2，…，$d-1$. ③

当 $0\leqslant i\leqslant d-1$ 时，有 $0\leqslant t_0+i\frac{m}{d}<m$，因此这 d 个数对模 m 是互不同余的. 另一方面，对于①式的任一解 $t_0+k_0\frac{m}{d}$，用 $k_0=qd+r$，$0\leqslant r<d$ 代入得

$$t_0+k_0\frac{m}{d}=t_0+(qd+r)\frac{m}{d}\equiv t_0+r\frac{m}{d} \pmod m,$$

因此①式的任一解必与③式中某一个数对模 m 同余.

故①式恰有 d 个解.

例 1 解同余方程 $40x\equiv6 \pmod{46}$.

解：由$(40, 46)=2$，且 $2\mid6$ 知方程有 2 个解.

先求同余方程

$$\frac{40}{2}x\equiv\frac{6}{2}\left(\mathrm{mod}\ \frac{46}{2}\right) \qquad ④$$

的唯一解.

由欧拉定理，$20^{\varphi(23)}\equiv1 \pmod{23}$，得出 $20\cdot2^{\varphi(23)-1}\times3\equiv3 \pmod{23}$.

由此可见④的解为

$$\begin{aligned}x&\equiv20^{\varphi(23)-1}\times3\\&\equiv20^{21}\times3\end{aligned}$$

$$\equiv -3^{22} \equiv -1 \equiv 22 \pmod{23}.$$

由定理 2 知原方程有两个解，且解为

$$x = 22 + i\frac{46}{2},\ i = 0,\ 1.$$

故原方程的解为

$$x \equiv 22 \pmod{46},$$

$$x \equiv 22 + 23 \equiv 45 \pmod{46}.$$

现在讨论①式的具体解法.

解一次同余方程有多种方法. 下面叙述的方法称为形式分数❶法，使用它解同余方程

$$ax \equiv b \pmod{m},\ (a,\ m) = 1 \qquad ⑤$$

常常是简便的. 此方法是基于同余式的恒等变形.

首先将⑤式形式上写成 $x \equiv \frac{b}{a} \pmod{m}$，然后在分数 $\frac{b}{a}$ 的分子，分母上进行变换. 变换有两种：（Ⅰ）用与 m 互素的数同时乘分子和分母，再将新的分子或分母换上它们对模 m 同余的数. （Ⅱ）在分子上加上 m 的倍数，使新分子和分母有公约数，再约去它.

适当地使用变换（Ⅰ）或（Ⅱ），经过若干次后，可使分母为 1，而求得解.

注

❶ 形式分数不是真正意义上的分数，只是具有分数的某些特征. 例如，分子，分母同乘一个数，将分子，分母模 m，不改变同余等式.

注

在运用变换（Ⅱ）时，必须要求 $(a,\ m) = 1$.

例 2 解同余方程 $8x \equiv 9 \pmod{11}$.

解：由 $(8,\ 11) = 1$，故可使用变换.

使用变换（Ⅰ），有

$$x \equiv \frac{9}{8} \equiv \frac{9\times 7}{8\times 7} \equiv \frac{63}{56} \equiv \frac{8}{1} \equiv 8 \pmod{11}.$$

故方程的解为

$$x \equiv 8 \pmod{11}.$$

也可使用变换（Ⅱ），我们有

$$x \equiv \frac{9}{8} \equiv \frac{9+11}{8} \equiv \frac{20}{8} \equiv \frac{5}{2} \equiv \frac{5+11}{2} \equiv \frac{8}{1} \equiv 8 \pmod{11}.$$

当然，变换（Ⅰ）和（Ⅱ）也可联合使用.

例 3 解同余方程 $78x \equiv 30 \pmod{198}$.

解：由 $(78,\ 198) = 6$，$6 \mid 30$ 知方程有 6 个解.

先解

$$\frac{78}{6}x \equiv \frac{30}{6} \left(\mathrm{mod}\ \frac{198}{6}\right),$$

即

$$13x \equiv 5 \pmod{33}.$$

$$x \equiv \frac{5}{13} \equiv \frac{5\times 7}{13\times 7} \equiv \frac{35}{91} \equiv \frac{35}{25} \equiv \frac{7}{5} \equiv \frac{7+33}{5} \equiv \frac{40}{5} \equiv 8 \pmod{33}.$$

故原方程 6 个解为

$$x\equiv 8,\ 41,\ 74,\ 107,\ 140,\ 173 \pmod{198}.$$

我国古代数学家秦九韶用“大衍求一术”求解一次同余方程，具体求法将在本章§3.3 节结合孙子定理讲述.

思考与讨论

你能证明威尔逊定理：设 p 为素数，则 $(p-1)!\equiv -1 \pmod p$ 吗？

（提示：由费马小定理，1，2，…，$p-1$ 是同余方程 $x^{p-1}-1\equiv 0 \pmod p$ 的解. 由因式定理，$x^{p-1}-1\equiv (x-1)(x-2)\cdots(x-p+1) \pmod p$，令 $x=0$.）

习题 3-2

1. 设 $(a,\ m)=1$，证明：$ax\equiv b \pmod m$ 的解为

$$x\equiv ba^{\varphi(m)-1} \pmod m.$$

2. 设 p 为奇素数，$1<a<p$，证明：

(1) $a!\mid (p-1)(p-2)\cdots(p-a+1)$；

(2) $ax\equiv b \pmod p$ 的解为

$$x\equiv b(-1)^{a-1}\frac{(p-1)(p-2)\cdots(p-a+1)}{a!} \pmod p.$$

3. 解同余方程 $111x\equiv 75 \pmod{321}$.

4. 解同余方程 $15x\equiv 9 \pmod 6$.

5. 解同余方程 $258x\equiv 131 \pmod{348}$.

6. 解同余方程 $20x\equiv 7 \pmod{53}$.

3.3 孙子定理

大约在公元 5～6 世纪，我国南北朝时期有一部著名算术著作《孙子算经》，其下卷第 26 题“物不知数”为：“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？”这个问题用同余式来表示，就是下面的一次同余方程组：

设物数为 x，依题意得

$$\begin{cases} x\equiv 2\ (\mathrm{mod}\ 3) \\ x\equiv 3\ (\mathrm{mod}\ 5) \\ x\equiv 2\ (\mathrm{mod}\ 7) \end{cases} \qquad ①$$

我们的祖先用歌诀形式给出了一种解法：

三人同行七十稀，
五树梅花廿一支，
七子团圆正月半，
除百零五便得之.

歌诀前三句给出了三组数：3，70；5，21；7，15. 这三组数有共同特征，从下表可以看出.

余数 / 除数 / 被除数	3	5	7
70	1	0	0
21	0	1	0
15	0	0	1

70，21，15 分别是满足表中第一、二、三行条件的最小正整数解. 容易看出

$$N=2\times 70+3\times 21+2\times 15=233,$$

满足原题所有三个余数条件. 歌诀最后一句“除百零五便得之”，意即 $N=233$ 模 3，5，7 的最小公倍数 105，所得 23 是原题的最小正整数解. 这样，

$$x\equiv 2\times\frac{105}{3}+3\times\frac{105}{5}+2\times\frac{105}{7}\equiv 23\ (\mathrm{mod}\ 105)$$

是同余方程①的唯一解.

这个解法的精妙之处在于，它把余数条件标准化，然后将较难的原问题分解为三个易解的子问题，并给出了通用的解法. 以下我们把《孙子算经》所述问题及其解法推广为下述定理.

定理 1 （孙子定理）设 m_1，m_2，…，m_n 是两两互素的正整数，记 $m=m_1m_2\cdots m_n$，$M_i=\dfrac{m}{m_i}$，$i=1$，2，…，n，则一次同余方程组

$$\begin{cases} x\equiv b_1(\mathrm{mod}\ m_1) \\ x\equiv b_2(\mathrm{mod}\ m_2) \\ \cdots, \\ x\equiv b_n(\mathrm{mod}\ m_n) \end{cases} \qquad ②$$

有唯一解

$$x\equiv b_1M'_1M_1+b_2M'_2M_2+\cdots+b_nM'_nM_n\ (\mathrm{mod}\ m),$$

其中 $M'_iM_i\equiv 1\ (\mathrm{mod}\ m_i)$，$i=1$，2，…，$n$.

证明：首先求出整数 x_0，使对每个 i，$i=1$，2，…，n，有 $x_0\equiv b_i(\mathrm{mod}\ m_i)$. 如能找到 L_i，$i=1$，2，…，n，满足

$$L_i \equiv \begin{cases} 1,\ (\mathrm{mod}\ m_j),\ j=i \\ 0,\ (\mathrm{mod}\ m_j),\ j\neq i \end{cases} \text{ 其中 } j=1,\ 2,\ \cdots,\ n,$$

则可取 $x_0=b_1L_1+b_2L_2+\cdots+b_nL_n$.

令 $m=m_1m_2\cdots m_n$，$M_i=\dfrac{m}{m_i}$，$i=1,\ 2,\ \cdots,\ n$. 显然 M_i 满足：(Ⅰ) $(M_i,\ m_i)=1$，(Ⅱ) $M_i\equiv 0\ (\mathrm{mod}\ m_j)$，$1\leqslant j\leqslant n$，$j\neq i$. 由(Ⅰ)知存在整数 M'_i，使 $M'_iM_i\equiv 1\ (\mathrm{mod}\ m_i)$. 不难看出可取 $L_i=M'_iM_i$，$i=1,\ 2,\ \cdots,\ n$. 因此可取

$$x_0=b_1M'_1M_1+b_2M'_2M_2+\cdots+b_nM'_nM_n.$$

易见满足 $x\equiv x_0(\mathrm{mod}\ m)$的整数 x 都是②式的解.

另一方面，如 x_1 是②式的解，则

$$\begin{cases} x_1\equiv x_0(\mathrm{mod}\ m_1) \\ x_1\equiv x_0(\mathrm{mod}\ m_2) \\ \cdots, \\ x_1\equiv x_0(\mathrm{mod}\ m_n) \end{cases}$$

因为$(m_i,\ m_j)=1$，$1\leqslant i<j\leqslant n$，所以

$$x_1\equiv x_0(\mathrm{mod}\ m).$$

于是②式的全部解为

$$x\equiv x_0(\mathrm{mod}\ m).$$

国际上称孙子定理为中国剩余定理.

从孙子定理可以看出解一次同余方程组②的难点在于对每个 M_i，求 M'_i，即求解一次同余方程 $M_iM'_i\equiv 1\ (\mathrm{mod}\ m_i)$，其中 M'_i 是未知数.

我国宋代大数学家秦九韶在他的杰作《数书九章》(1247 年) 中提出了求解同余方程

$$ax\equiv b\ (\mathrm{mod}\ m),\ (a,\ m)=1 \qquad ③$$

的方法——“大衍求一术”，用现代的数学语言来叙述大致就是：由已知互素的整数 a，$m(>0)$，去求整数 k，使得

$$ak\equiv 1\ (\mathrm{mod}\ m)$$

成立的一种算法.

具体做法是：(不妨设 $a>0$)

对 a，m 使用辗转相除得到

$$\begin{aligned} &a=mq_1+r_1,\ 0<r_1<m, \\ &m=r_1q_2+r_2,\ 0<r_2<r_1, \\ &\cdots, \\ &r_{n-2}=r_{n-1}q_n+r_n,\ 0<r_n<r_{n-1}, \\ &r_{n-1}=r_nq_{n+1}. \end{aligned}$$

由 1.4 节定理 3 知

$$1=(a,\ m)=[(-1)^{n-1}Q_n]a+[(-1)^nP_n]m,$$

即得

$$a[(-1)^{n-1}Q_n]\equiv 1 \pmod m.$$

于是求得

$$k=(-1)^{n-1}Q_n. \tag{4}$$

由④式即得③式的解为

$$x\equiv(-1)^{n-1}Q_n b \pmod m,$$

其中 Q_n 可按 $Q_0=0$，$Q_1=1$，$Q_k=q_kQ_{k-1}+Q_{k-2}$，$k\geqslant 2$，求出.

例 1 解“物不知数”问题中的同余方程组

$$\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 3 \pmod 5 \\ x\equiv 2 \pmod 7 \end{cases}$$

解：由 3，5，7 两两互素知可应用孙子定理. 此时

$$3\times 5\times 7=105=3\times 35=5\times 21=7\times 15.$$

解辅助方程

$$35x\equiv 1 \pmod 3, \tag{5}$$

$$21x\equiv 1 \pmod 5, \tag{6}$$

$$15x\equiv 1 \pmod 7. \tag{7}$$

由⑤式得

$$x\equiv\frac{1}{35}\equiv\frac{1}{2}\equiv\frac{4}{2}\equiv 2 \pmod 3,$$

由⑥式得

$$x\equiv\frac{1}{21}\equiv\frac{1}{1}\equiv 1 \pmod 5,$$

由⑦式得

$$x\equiv\frac{1}{15}\equiv\frac{1}{1}\equiv 1 \pmod 7.$$

故解为

$$\begin{aligned} x &\equiv b_1M_1'M_1+b_2M_2'M_2+b_3M_3'M_3 \\ &\equiv 2\times 2\times 35+3\times 1\times 21+2\times 1\times 15 \\ &\equiv 23 \pmod{105}. \end{aligned}$$

例 2 （韩信点兵）有兵四千多，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：设兵数为 x，则依题意知

$$\begin{cases} x\equiv 1 \pmod 5 \\ x\equiv 5 \pmod 6 \\ x\equiv 4 \pmod 7 \\ x\equiv 10 \pmod{11} \end{cases}$$

$$4\,000<x<5\,000.$$

由 5，6，7，11 两两互素知可应用孙子定理. 此时 $5\times6\times7\times11=2\,310=5\times462=6\times385=7\times330=11\times210$.

解辅助方程

$$462x\equiv1\pmod 5,\tag{8}$$

$$385x\equiv1\pmod 6,\tag{9}$$

$$330x\equiv1\pmod 7,\tag{10}$$

$$210x\equiv1\pmod{11}.\tag{11}$$

由⑧式得

$$x\equiv\frac{1}{462}\equiv\frac{1}{2}\equiv\frac{6}{2}\equiv3\pmod 5,$$

由⑨式得

$$x\equiv\frac{1}{385}\equiv\frac{1}{1}\equiv1\pmod 6,$$

由⑩式得

$$x\equiv\frac{1}{330}\equiv\frac{1}{1}\equiv1\pmod 7,$$

由⑪式得

$$x\equiv\frac{1}{210}\equiv\frac{1}{1}\equiv1\pmod{11}.$$

故解为

$$\begin{aligned}x&\equiv1\times3\times462+5\times1\times385+4\times1\times330+10\times1\times210\\&\equiv6\,731\equiv2\,111\pmod{2\,310},\end{aligned}$$

即为 $x=2\,111+2\,310k$，$k=0$，1，2，….

故所求兵数为 4 421.

习题 3-3

1. 解我国古代数学家杨辉在 1275 年所写的《续古摘奇算法》中的三个问题：

(1) 七数剩一，八数剩一，九数剩三，问本数；

(2) 十一数余三，十二数余二，十三数余一，问本数；

(3) 二数余一，五数余二，七数余三，九数余四，问本数.

2. 解一次同余方程组

$$\begin{cases}x\equiv1\pmod 3\\x\equiv-1\pmod 5\\x\equiv2\pmod 7\\x\equiv-2\pmod{11}\end{cases}$$

3.4 拉格朗日插值公式

本节我们用孙子定理的思想与方法研究插值问题.

设想某气象站在时刻 x_1，x_2，…，$x_n(x_1<x_2<\cdots<x_n)$上记录下来的温度分别是 y_1，y_2，…，y_n. 我们希望找到一个多项式函数 $f(x)$，使其满足 $f(x_i)=y_i$，$i=1$，2，…，n. 我们就用 $f(x)$来作温度函数的某种近似，这就是所谓插值问题.

先看一个例子.

例 1 已知三组数值 (1，7)，(2，3)，(3，−2). 找出一个二次多项式 $f(x)$，满足 $f(1)=7$，$f(2)=3$，$f(3)=-2$.

解：由余式定理，我们知道 $f(x)$除以 $(x-a)$ 的余数是 $f(a)$.

$f(1)=7$，$f(2)=3$，$f(3)=-2$分别意味着 $f(x)$除以$(x-1)$余 7，除以$(x-2)$余 3，除以$(x-3)$余-2. 一下子求出这样的 $f(x)$比较困难. 我们运用孙子定理的方法把条件标准化，并将问题分解，先求 $f_1(x)$，$f_2(x)$，$f_3(x)$，分别满足条件：

(1) $f_1(x)$除以$(x-1)$余 1，并被$(x-2)$，$(x-3)$整除. 这样，

$$f_1(x)=\lambda(x-2)(x-3).$$

由 $f_1(1)=1$，知

$$\lambda=\frac{1}{(1-2)(1-3)},$$

于是

$$f_1(x)=\frac{(x-2)(x-3)}{(1-2)(1-3)}.$$

(2) $f_2(x)$除以$(x-2)$余 1，并被$(x-1)$，$(x-3)$整除，同理可得

$$f_2(x)=\frac{(x-1)(x-3)}{(2-1)(2-3)}.$$

(3) $f_3(x)$除以$(x-3)$余 1，并被$(x-1)$，$(x-2)$整除，所以

$$f_3(x)=\frac{(x-1)(x-2)}{(3-1)(3-2)}.$$

不难验证

$$\begin{aligned}f(x)&=7f_1(x)+3f_2(x)-2f_3(x)\\&=-\frac{1}{2}x^2-\frac{5}{2}x+10\end{aligned}$$

是满足已知条件的二次多项式.

一般地，给定 n 组值(x_i, y_i)，$i=1$，2，…，n，其中 x_i 互不相等. 为求多项式 $f(x)$，使 $f(x_i)=y_i$，$i=1$，2，…，n，可先求出 $L_i(x)$满足

$$L_i(x_j)=\begin{cases}1, & j=i\\0, & j\neq i\end{cases}\text{ 其中 }j=1,2,\cdots,n. \qquad ①$$

那么不难看出 $f(x)=y_1L_1(x)+y_2L_2(x)+\cdots+y_nL_n(x)$ 就是满足 $f(x_i)=y_i$，$i=1,2,\cdots,n$ 的插值多项式.

由①式不难求出 $L_i(x)$，$i=1,2,\cdots,n$.

由①式知 $L_i(x)$ 以 $x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n$ 为其 $(n-1)$ 个不同零点，故 $L_i(x)=k_i(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)$，其中 k_i 是一个待定系数.

由 $L_i(x_i)=1$ 即得

$$k_i=\frac{1}{(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)},$$

于是，

$$L_i(x)=\frac{(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)},\quad i=1,2,\cdots,n.$$

这样，

$$f(x)=y_1L_1(x)+y_2L_2(x)+\cdots+y_nL_n(x)$$

为所求之多项式函数. 这个公式叫做拉格朗日插值公式.

例 2　已知 $f(n)=0^2+1^2+2^2+\cdots+(n-1)^2$ 是 n 的三次多项式，求 $f(n)$.

解：由已知条件知

$f(0)=0$❶，$f(1)=0$，$f(2)=1$，$f(3)=5$.

由插值公式可知

$$\begin{aligned}f(n)&=L_3(n)+5L_1(n)\\&=\frac{(n-0)(n-1)(n-3)}{(2-0)(2-1)(2-3)}+5\frac{(n-0)(n-1)(n-2)}{(3-0)(3-1)(3-2)}\\&=\frac{1}{6}n(n-1)(2n-1).\end{aligned}$$

注

❶ 当 $n=0$ 时，$f(n)$ 定义中等号右边没有加数，此时和为 0. 这里 n 表示项数.

习题 3-4

1. 已知三次函数 $y=f(x)$ 的图象经过点 $(1,0)$，$(2,0)$，$(3,2)$，$(4,12)$，求 $f(x)$.
2. 已知 $s(n)=0^3+1^3+2^3+\cdots+(n-1)^3$ 是四次多项式，求 $s(n)$.

3.5　公开密钥码

密钥是通讯双方的一种秘密约定，以防密码被第三者破译. 例如，双方约定，按英文字母表的顺序，把明文（要发出的真实信息）中的字母后移三格，即用它后面的第三个字母代替，得到密文（直接发出的码）. “后移三格”就是密钥. 接收者只需把密文中的字母向前移三格就得到真实信息. 这是最原始的编码方法，很容易被人破译. 二战时期所用的一种编码方法是用 0，1 两个数字编码，双方约定一个数，明文加上这个数（模 2 加法）便

得到密文. 比如：

明文　10101101110

密钥　00100110111（约定数）

密文　10001011001

接收者收到密文后，加上约定数便得明文. 破译这种密码虽然有一定难度，但还是常常被第三方破译. 本节给出一种编码方法，使所发密码不仅难以被别人破译，而且密钥可以公开. 设计者可以收到任何人按照指定方法发送的秘密信息.

同学们知道，求两个素数之积只是举手之劳，但是相反，分解一个大的正整数为两数之积会遇到难以想象的困难. 利用这个道理，可以找到如下的一种编码方法.

设张明同学学得一种编码方法. 他选择两个大素数 p 与 q，并求得乘积 $N=pq$. 然后按如下要求选取正整数 e 与 d：

(1) $(e,(p-1)(q-1))=1$；

(2) $d=\dfrac{k(p-1)(q-1)+1}{e}$，$k$ 为整数.

这里，条件(1)保证可以找到整数 k 使 d 为正整数.

此时，张明可以像公布自己的电话号码一样公开数字 N 和 e（密钥），但数字 d(解钥)保密. 李强同学事先没有和张明约定，想向张明发送秘密信息. 设李强要发的明文(真实信息)是 M（正整数，信息代码，$(M,N)=1$，$1\leqslant M\leqslant N$). 首先他可以像翻电话本一样，查到张明的密钥(N,e)，接着他不直接发 M，而发密文 C，C 由下式给出：

$$M^e\equiv C(\mathrm{mod}\ N),\quad 1\leqslant C\leqslant N.$$

张明接收到密文 C 后，作运算 $C^d(\mathrm{mod}\ N)$，具体为

$$C^d\equiv(M^e)^d\equiv M^{k(p-1)(q-1)+1}\equiv M\cdot M^{k(p-1)(q-1)}(\mathrm{mod}\ N).$$

由费马小定理可得

$$M^{k(p-1)(q-1)}\equiv(M^{k(q-1)})^{p-1}\equiv 1(\mathrm{mod}\ p),$$

$$M^{k(p-1)(q-1)}\equiv(M^{k(p-1)})^{q-1}\equiv 1(\mathrm{mod}\ q).$$

由孙子定理知，同余方程组

$$\begin{cases}x\equiv 1(\mathrm{mod}\ p)\\ x\equiv 1(\mathrm{mod}\ q)\end{cases}$$

有唯一解(mod N). 因为 $M^{k(p-1)(q-1)}$ 和 1 都是其解，所以有

$$M^{k(p-1)(q-1)}\equiv 1(\mathrm{mod}\ N),$$

于是

$$C^d\equiv M\cdot M^{k(p-1)(q-1)}\equiv M(\mathrm{mod}\ N),$$

这样张明同学便得到了李强同学的真实信息 M.

为什么除张明外，别人很难破译李强发给他的密码呢？原因就是张明没有公开解钥 d. 由公开密钥(N,e)是很难求得解钥 d 的. 因为由 d 的定义可知，要求 d 必须要知道素数 p 和 q，但当 N 很大时，把它分解成素数乘积是极其困难的❶.

注

❶ 分解一个上百位数字的数，即使采用最高速的电子计算机，所需时间（以年计）为天文数字.

为理解这种通讯模式，以下仅以较小的数字为例，说明本节的编码、译码过程.

你选择 $p=5$，$q=11$，$e=3$. 取 $k=2$，由(2)得 $d=27$. 将密钥$(N, e)=(55, 3)$公开，解钥 $d=27$ 保密.

设有某人向你发送明文 $M=23$，他可换成密文 C，即

$$M^e \equiv 23^3 \equiv 12 \pmod{55},\quad C=12.$$

你收到密文 $C=12$ 后，作运算

$$\begin{aligned} C^d &\equiv (12)^{27} \equiv (12^3)^9 \equiv (1728)^9 \equiv (23)^9 \equiv (23^3)^3 \\ &\equiv (12)^3 \equiv 23 \pmod{55}. \end{aligned}$$

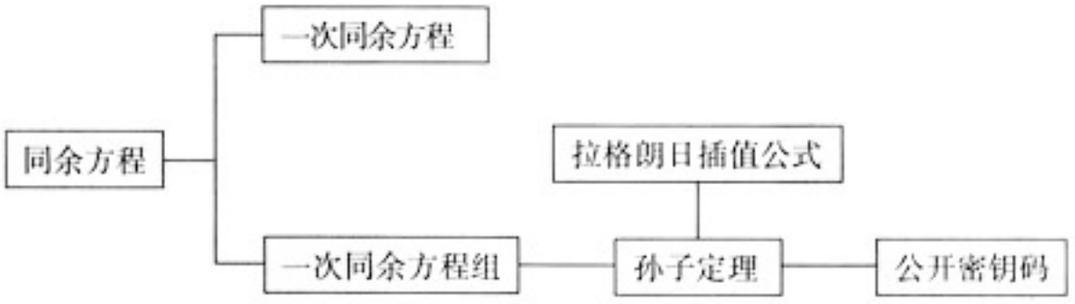
于是，你得到了他发给你的真实信息 $M=23$.

习题 3-5

选择两个素数 p，q 制作密码，并说明发码与译码过程.

本章小结

Ⅰ 知识结构



Ⅱ 思考与交流

1. 利用孙子定理解一次同余方程组时，要求各个模 m_1，m_2，…，m_n 必须是两两互素的. 如果不满足此条件，你能想出方法使原方程组转化成新的一次同余方程组，新方程组既和原方程组有相同的解，又满足各个模两两互素吗？本章小结第三栏中的第 3，4，5 题能帮助你做到这一点，仔细想想为什么？
2. 解同余方程时，能不能消去等式两边相同的因式？为什么？

Ⅲ 巩固与提高

1. 解同余方程 $x^3+25x^2+11x+25\equiv 0 \pmod{31}$.
2. 用七数剩二，用八数剩三，用九数剩一，问本数.
3. 设 $d=(m_1, m_2)$，则一次同余方程组 $\begin{cases} x\equiv b_1 \pmod{m_1} \\ x\equiv b_2 \pmod{m_2} \end{cases}$ 有解的充分必要条件是 $d\mid(b_1-b_2)$.
4. 设 m 的标准分解式为 $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$，则同余方程

$$x\equiv a \pmod{m}$$

与同余方程组

$$\begin{cases} x\equiv a\ (\mathrm{mod}\ p_1^{\alpha_1}) \\ x\equiv a\ (\mathrm{mod}\ p_2^{\alpha_2}) \\ \cdots, \\ x\equiv a\ (\mathrm{mod}\ p_s^{\alpha_s}) \end{cases}$$

具有相同的解.

5. 设 $\alpha\geqslant\beta$，且同余方程组 $\begin{cases} x\equiv a_1(\mathrm{mod}\ p^{\alpha}) \\ x\equiv a_2(\mathrm{mod}\ p^{\beta}) \end{cases}$ 有解，则解就是同余方程 $x\equiv a_1(\mathrm{mod}\ p^{\alpha})$ 的解，其中 p 是素数.（提示：用习题 3）

6. 解一次同余方程组 $\begin{cases} x\equiv 2\ (\mathrm{mod}\ 35) \\ x\equiv 9\ (\mathrm{mod}\ 14) \\ x\equiv 7\ (\mathrm{mod}\ 20) \end{cases}$

Ⅳ 自测与评估

1. 解同余方程 $5x\equiv 13\ (\mathrm{mod}\ 43)$.

2. 求整数 n，它被 3，5，7 除的余数分别是 1，2，3.

3. 解一次同余方程组

$$\begin{cases} 3x\equiv 2\ (\mathrm{mod}\ 5) \\ 7x\equiv 3\ (\mathrm{mod}\ 8) \\ 4x\equiv 7\ (\mathrm{mod}\ 11) \end{cases}$$

4. 求 7 的倍数，使它分别被 2，3，4，5，6 除时，余数都是 1.

5. 设 n 为正整数，证明：必有 n 个连续的整数，其中每一个都具有平方因子（即被某个素数的平方整除）.（提示：用孙子定理）

陈景润

陈景润（1933—1996），中国现代数学家，1953年毕业于厦门大学数学系，同年分配到北京当中学教师，1954年回厦门大学任图书管理员，期间，从事解析数论研究．1956年，23岁的陈景润，写出一篇论文，改进了华罗庚的工作，引起了数学大师华罗庚的注意，1957年经华罗庚推荐进入中国科学院数学研究所工作，曾对圆内格点问题、球内格点问题、华林问题作过重要推进．

1966年，陈景润发表论文摘要“每一个充分大的偶数都能够表示为一个素数及一个不超过两个素数的乘积之和”，1973年在《中国科学》上发表了论文全文，对推进哥德巴赫猜想的证明作出重大贡献．陈景润的这个结果被国际数学界誉为“陈氏定理”．

陈景润曾任中国科学院数学研究所研究员，中国科学院院士．1996年因病逝世．

陈景润历经磨难，但他对数学的热爱与执着始终不改．他以超乎常人的毅力与刻苦精神，攻克了数论中一道又一道难题．他的光辉业绩和科学精神值得我们学习．

附 录

部分中英文词汇对照表

整除	divide exactly
素数	prime number
合数	composite number
带余除法	division algorithm
辗转相除	mutual division
公约数	common divisor
公倍数	common multiple
算术基本定理	fundamental theorem of arithmetic
同余	congruence
威尔逊定理	Wilson theorem
剩余类	residue class
欧拉函数	Euler's function
欧拉定理	Euler's theorem
不定方程	Diophantine equation
同余方程	congruence equation
模	module
插值	interpolation
公开密钥	public key

后记

根据教育部制订的普通高中各学科课程标准（实验），人民教育出版社课程教材研究所编写的各学科普通高中课程标准实验教科书，得到了诸多教育界前辈和各学科专家学者的热情帮助和大力支持. 在各学科教科书终于同课程改革实验区的师生见面时，我们特别感谢担任教科书总顾问的丁石孙、许嘉璐、叶至善、顾明远、吕型伟、王梓坤、梁衡、金冲及、白春礼、陶西平同志，感谢担任教科书编写指导委员会主任委员的柳斌同志和编写指导委员会委员的江蓝生、李吉林、杨焕明、顾泠沅、袁行霈等同志.

本套高中数学实验教科书（B版）的总指导为丁尔陞教授. 从教材立项、编写、送审到进入实验区实验的过程中，在丁尔陞、孙瑞清、江守礼、房艮孙、王殿军等专家教授的指导下，经过实验研究组全体成员的努力，基本上完成了“课标”中各模块的编写任务，并通过了教育部的审查.

山东、辽宁等实验区的教研员和教师在实验过程中，对教材编写的指导思想、教材内容的科学性、基础性、选择性以及是否易教、易学等诸方面，进行了审视和检验，提出了许多的宝贵意见，并针对教材和教学写出了大量的论文. 我们在总结实验的基础上，逐年对教材进行认真的修改，使教材不断的完善. 现在所取得的成果，是实验研究组全体成员、编者，实验区的省、市、县各级教学研究员及广大数学教师集体智慧的结晶.

各实验区参加教材审读、研讨及修改的主要成员有：

韩继清、常传洪、尹玉柱、秦玉波、祝广文、尚凡青、杨长智、田明泉、邵丽云、于世章、李明照、胡廷国、张颉、张成钢、李学生、朱强、窦同明、姜传祯、韩淑勤、王宗武、黄武昌.

刘莉、宋明新、高锦、赵文莲、王孝宇、周善富、胡文亮、孙家逊、舒凤杰、齐力、林文波、教丽、刘鑫、李凤、金盈、潘戈、高钧、魏明智、刘波、崔贺、李忠、关玲、郝军、郭艳霞、董晖、赵光千、王晓声、王文、姚琳.

在此，特向参与、帮助、支持这套教科书编写的专家、学者和教师深表谢意.

我们还要感谢实验区的教育行政和教研部门，以及使用本套教材的学校领导和师生们.

让我们与一切关心这套教材建设的朋友们，共同携起手来，为建设一套具有中国特色的高中数学教材而努力.

我们的联系方式如下：

电话：010-58758523　010-58758532

电子邮件：longzw@pep.com.cn

人民教育出版社　课程教材研究所

中学数学教材实验研究组