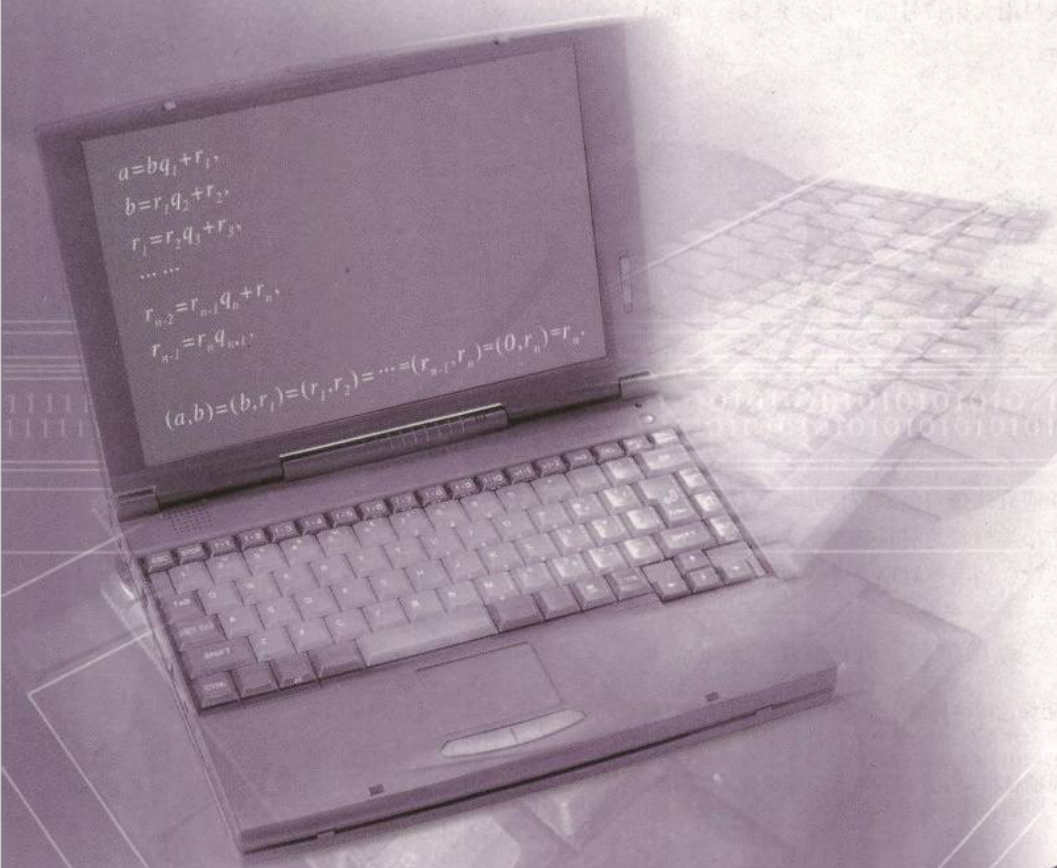
普通高中课程标准实验教科书

# 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
中学数学课程教材研究开发中心　编著




人民教育出版社
A版

普通高中课程标准实验教科书　数学　选修4-6　A版　初等数论初步

人民教育出版社　课程教材研究所
中学数学课程教材研究开发中心　编著

出版发行　人民教育出版社
（北京市海淀区中关村南大街17号院1号楼　邮编：100081）
网　　址　http://www.pep.com.cn
经　　销　全国新华书店
印　　刷　北京天宇星印刷厂
版　　次　2007年2月第2版
印　　次　2019年8月第30次印刷
开　　本　787毫米×1092毫米　1/16
印　　张　3.75
字　　数　77千字
书　　号　ISBN 978-7-107-18686-8
定　　价　3.85元
价格依据文件号：京发改规［2016］13号



绿色印刷　保护环境　爱护健康

亲爱的同学们：

你们手中的这本教科书采用绿色印刷标准印制，在它的封底印有“绿色印刷产品”标志。从2013年秋季学期起，北京地区出版并使用的义务教育阶段中小学教科书全部采用绿色印刷。

按照国家环境标准（HJ2503-2011）《环境标志产品技术要求　印刷　第一部分：平版印刷》，绿色印刷选用环保型纸张、油墨、胶水等原辅材料，生产过程注重节能减排，印刷产品符合人体健康要求。

让我们携起手来，支持绿色印刷，选择绿色印刷产品，共同关爱环境，一起健康成长！

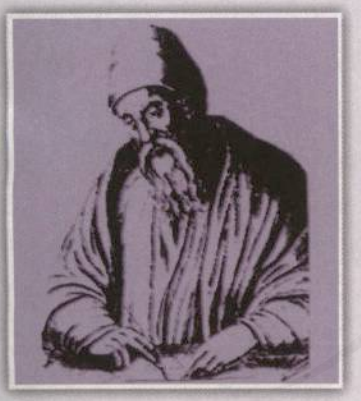
北京市绿色印刷工程

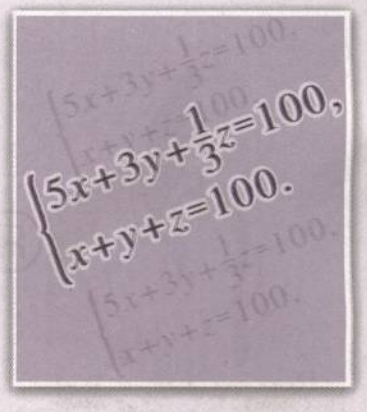
主　　编：刘绍学
副 主 编：钱珮玲　章建跃

主要编者：胡永建
责任编辑：张劲松
美术编辑：王俊宏　王　艾
封面设计：林荣桓　吴　敬

# 目 录








# 引言

| 九　月 | | | | | | |
|---|---|---|---|---|---|---|
| 日 | 一 | 二 | 三 | 四 | 五 | 六 |
| | 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 | | | | |

数论是研究整数的性质和方程的整数解的一门学科. 它起源于古代的东方，距今大约有3000年的历史.

我国古代数学家在数论方面取得了一些重要成就. 《周髀算经》记载有西周人商高提出的“勾广三，股修四，径隅五”的论断，它实际上给出了方程 $x^2+y^2=z^2$ 有一组正整数解 (3，4，5). 《九章算术》记载有另外的四组正整数解：(5，12，13)，(8，15，17)，(7，24，25)，(20，21，29). 我国另一部重要数学著作《孙子算经》中记载有“物不知数”问题：“今有物不知其数，三三数之余二，五五数之余三，七七数之余二，问物几何?”答曰：“二十三.”这一问题和它的解法一起被后人称为孙子定理（国外文献称之为中国剩余定理).

我国古代的数论研究具有鲜明的直观、实用和算法特性. 古希腊的数论研究则具有理性的特点，其成就集中反映在两部数学著作中，一部是欧几里得的《几何原本》，它给出了算术基本定理、素数有无限多个、辗转相除法等初等数论的重要结果；另一部是丢番图的《算术》，这是历史上第一部脱离几何，完全讲述数论的著作，书中讨论了300多个数论问题，列举了一些一次方程和二次方程的整数解的解法.

数论是一门古老而又基础的数学分支，至今仍有许多没有解决的问题. 这些数论问题对人类智慧产生极大的挑战，人们为解决这些数论问题所作的贡献，对数论乃至整个数学的发展起了重要的推动作用. 一个典型的例子就是费马猜想的解决.

1637年，法国数学家费马提出猜想：方程 $x^n+y^n=z^n$ 没有正整数解，其中 $n$ 为大于2的整数. 300多年来，许多专业数学家和业余数学爱好者为解决此猜想作了不懈的努力，最终于1994年被英国数学家威尔斯（Wiles）解决. 在费马猜想的研究过程中，人们创造了研究数论的许多新方法，建立了数论的一些新分支，发现了它与数学其他领域的奇妙而深刻的联系.

当今的数论已经发展成为一门艰深的学问. 而且，随着计算机技术和数字通信技术的飞速发展，数论已经成为计算机科学和通信工程的重要数学工具之一.

本专题中，同学们将通过具体的问题，学习有关整数和整除的知识，探索用辗转相除法求解一次同余方程、一次同余方程组、简单的一次不定方程等，从中体会数论的基本思想方法，同时了解我国古代数学的一些重要成就.

# 第一讲 整数的整除

我们知道，两个整数进行加法、减法、乘法运算，结果仍为整数. 但是，两个整数相除，不一定能除尽，也就是说，所得结果不一定为整数.

给定非零整数 $n$，如何找出所有除尽 $n$ 的整数和被 $n$ 除尽的整数；给定两个非零整数 $a$ 和 $b$，如何找出所有同时除尽 $a$，$b$ 的整数和同时被 $a$，$b$ 除尽的整数. 如果给定的是多个非零整数，又该如何?

这些问题不仅有理论意义，而且还是后面解同余方程和不定方程的基础. 要完整地回答这些问题，我们需要学习整数的一些基本知识.

## 一 整除

### 1. 整除的概念和性质

**思考**

如何从乘法角度判断一个整数能除尽另一个整数?

我们知道，乘法与除法是互逆的两种运算. 要判断一个整数能否除尽另一个整数，只需考察被除数能否写成除数和某个整数的乘积. 只有当被除数可以表示为除数和某个整数的乘积时，除数恰好能除尽被除数. 此时，我们就说除数整除被除数，或者说被除数能被除数整除.

**一般地，设 $a$，$b$ 为整数，且 $b\neq 0$. 如果存在整数 $q$，使得 $a=bq$，那么称 $b$ 整除 $a$，或者 $a$ 能被 $b$ 整除，记作 $b\mid a$. 并且称 $b$ 是 $a$ 的因数，$a$ 是 $b$ 的倍数. 如果这样的整数 $q$ 不存在，就称 $b$ 不整除 $a$，记作 $b\nmid a$.**

例如，$6\mid -24$，$-4\mid 56$，$-4\nmid 14$，$8\mid 0$.

由此可知，能被非零整数 $n$ 整除的整数是 $n$ 的倍数，其一般形式为 $nq$，这里 $q$ 为任意整数. 能除尽 $n$ 的整数是 $n$ 的因数，例如，能除尽 6 的整数为 1，$-1$，2，$-2$，3，$-3$，6，$-6$.

## 探究

由整除的概念，你能否推出下列整除的基本性质？

(1) 若 $a \mid b$，$b \mid a$，则 $a=b$，或 $a=-b$.

(2) 若 $a \mid b$，$b \mid c$，则 $a \mid c$.

(3) 若 $a \mid b$，$a \mid c$，则对任意整数 $x$，$y$，恒有 $a \mid bx+cy$.

如何判断一个非零整数整除给定的正整数？对某些特殊的非零整数，我们可以通过观察发现一些简单的判别方法.

## 观察

给定两组正整数：

第一组　6，　18，　21，　54，　81，　96，　108，　243

第二组　5，　17，　43，　80，　85，　98，　121，　212

第一组数有什么规律？它们能被什么整数整除？第二组数呢？计算每组数的各位数字之和，你能发现什么特征？

观察发现，第一组数能被 3 整除，并且其中每一个数的各位数字之和都能被 3 整除；第二组数不能被 3 整除，并且其中每一个数的各位数字之和也不能被 3 整除.

由此，我们猜想：

(1) **一个正整数的各位数字之和能被 3 整除，那么这个正整数能被 3 整除.**

这个命题是否正确？我们证明一下.

下面仅对 4 位正整数情形给出证明，同学们可以类比证明一般的情形.

证明：设 $N$ 为 4 位正整数，且它的个、十、百和千位数字依次为 $a$，$b$，$c$，$d$，则

$$\begin{aligned} N &= d\times 10^3+c\times 10^2+b\times 10+a \\ &= d\times(999+1)+c\times(99+1)+b\times(9+1)+a \\ &= 999d+99c+9b+d+c+b+a. \end{aligned}$$

因为 $3 \mid 999d+99c+9b$，所以，当 $3 \mid d+c+b+a$ 时，$3 \mid N$.

## 探究

请用类似的方法证明能被 9，11，7 整除的正整数的下列特征：

(2) 一个正整数的各位数字之和能被 9 整除，那么这个正整数能被 9 整除；

(3) 一个正整数的奇数位数字之和与偶数位数字之和的差能被 11 整除，那么这个正整数能被 11 整除；

(4) 一个正整数的末三位数字组成的数与末三位数字之前的数字组成的数之差能被 7（或 11）整除，那么这个正整数能被 7（或 11）整除.

例 1 判断 710316 能否被 9，11 整除.

解：因为 7+1+0+3+1+6=18 能被 9 整除，所以 710316 能被 9 整除.

又因为 710316 的奇数位数字之和为 6+3+1=10，偶数位数字之和为 1+0+7=8，而 10−8=2 不能被 11 整除，所以 710316 不能被 11 整除.

## 2. 带余除法

我们知道，14÷3 的商为 4，余数为 2，即 14=3×4+2，这种表示法在整数集中仍然成立，我们把它叫做带余除法（或欧氏除法算式）.

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

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

欧几里得（Euclid，生卒年不详，约活动于公元前 300 年前后），古希腊数学家.

古希腊的数论成就集中反映在欧几里得的几何《原本》一书中，全书共 13 卷，其中 5 卷讲数论，主要包括欧氏除法算式、算术基本定理、素数有无限多个等.

事实上，对任意整数 $a$ 和非零整数 $b$，如果 $a$ 是 $b$ 的倍数，那么存在整数 $q$，使得 $a=bq$，此时 $r=0$. 如果 $a$ 不是 $b$ 的倍数，如图 1-1 所示（$b>0$ 的情形），由于 $b$ 的倍数在数轴上是等距分布的，而且相邻两个倍数之间的距离为 $|b|$，而 $a$ 是数轴上的一点，那么它一定落在 $b$ 的两个相邻倍数之间. 此时，将紧邻 $a$ 的左侧 $b$ 的倍数记作 $bq$，选取 $r$ 为 $a$ 与 $bq$ 的距离，此时 $a=bq+r$（从数轴上可以直观地看出）. 这就说明了满足上述等式的整数 $q$ 和 $r$ 是存在的.

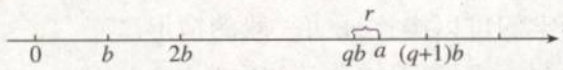



图 1-1

下面说明 $q$ 和 $r$ 是惟一的，如果整数对 $q'$ 和 $r'$ 也满足

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

那么 $a=bq+r=bq'+r'$，即 $r-r'=b(q'-q)$，

于是 $b\mid(r-r')$，而 $-|b|<r-r'<|b|$，

因此，$r-r'=0$，即 $r=r'$，从而 $q=q'$.

所以，$q$ 和 $r$ 是惟一的.

我们把带余除法中惟一的 $q$ 和 $r$ 分别叫做 $a$ 除以 $b$ 的商和余数. 显然，$a$ 能被 $b$ 整除当且仅当余数 $r=0$.

例 2 2004 除以某个整数，其商为 74，求除数和余数.

解：设除数为 $b$，余数为 $r$，则

$$2004=74b+r,\ 0\leqslant r<b.$$

由此可得

$$74b\leqslant 2004<74b+b=75b,$$

从而有

$$74\leqslant\frac{2004}{b}<75,$$

所以

$$\frac{2004}{75}<b\leqslant\frac{2004}{74},$$

即

$$26\frac{18}{25}<b\leqslant 27\frac{3}{37}.$$

因此，$b=27$，$r=2004-27\times 74=6$.

**探究**

我们用符号$[x]$❶表示不超过实数$x$的最大整数，试用$a$，$b$表示$a$除以正整数$b$的商$q$和余数$r$.

### 3. 素数及其判别法

考察正整数的正因数，我们发现，有的正整数仅有一个正因数（如1），有的正整数仅有两个正因数（如3，13，31），而有的正整数至少有三个正因数（如12，14，81）.

我们把仅有两个正因数的正整数叫做**素数**，不是素数又不是1的正整数叫做**合数**.

由定义知，3，13，31是素数，12，14，81是合数，1既不是素数，也不是合数.

显然，2是惟一的偶素数，也是最小的素数. 每个合数总可以表示成两个大于1的正整数的乘积，而素数则不能.

**观察**

找出下列每个正整数的正因数：

6，7，9，21，65，77，121.

观察每个正整数除1外的最小的一个正因数，从中你能发现什么规律？

我们发现，每个正整数$n$除1外的最小正因数$p$是一个素数. 事实上，假设$p$不是素数，因为$p>1$，所以$p$为合数，那么$p$必然有1，$p$以外的正因数$q$，使得$q\mid p$. 因为

❶ $[x]$通常叫做取整函数（或高斯函数），它是数论中一个常见的函数，具有许多有趣的性质.

$p \mid n$，所以 $q \mid n$，于是 $q$ 是 $n$ 的除 1，$p$ 以外且小于 $p$ 的正因数，这与已知矛盾，故最小正因数 $p$ 是一个素数. 一般地，任何大于 1 的整数，总存在一个素数因数. 通常，把一个正整数的素数因数叫做它的素因数.

**思考**

是否总可将任何大于 1 的整数 $n$ 分解为一些素数的乘积?

对大于 1 的整数 $n$，如果 $n$ 不是素数，我们可以将 $n$ 分解为一个素数和某个大于 1 的整数 $a$ 的乘积，如果 $a$ 是一个素数，则过程停止. 否则，又可将 $a$ 分解为一个素数和某个大于 1 的整数 $b$ 的乘积. 对 $b$ 又分两种情形：若 $b$ 为素数，则过程停止；若 $b$ 不是素数，则将 $b$ 继续分解为一个素数和某个大于 1 的整数 $c$ 的乘积. 如此进行下去，直到过程停止，最后总可将 $n$ 分解为一些素数的乘积. 例如，$12=2\times2\times3$，$78=2\times3\times13$.

既然任何大于 1 的整数 $n$ 总可分解为一些素数的乘积，那么素数有多少个？有限还是无限？为什么？

我们不妨假设素数有有限个，即 $m_1$，$m_2$，$m_3$，…，$m_k$，记这 $k$ 个素数的乘积为 $N$，即

$$N=m_1m_2m_3\cdots m_k.$$

由此可知，任意一个素数 $m_i(i=1, 2, \cdots k)$ 都整除 $N$，但不能整除 $N+1$. 又由于 $N+1$ 为大于 1 的正整数，所以它一定能被某个素数整除，这就产生了矛盾. 因此，假设素数有有限个是错误的，**素数有无穷多个**

欧几里得证明素数有无穷多个这个命题时使用了反证法，这是数学上第一批使用反证法的命题.

**思考**

对给定的大于 1 的正整数，如何判断它是不是素数呢？例如，要判断 61 是不是素数，是否需要用 2～60 之间的数一一试除 61 呢?

没有必要. 因为 2 不是 61 的因数，那么 2 的倍数也不是 61 的因数. 同样地，若 3 不是 61 的因数，那么 3 的倍数也不是 61 的因数. 这就是说只需用 2～60 之间的素数试除 61 即可.

另一方面，如果 61 是合数，那么它一定可以表示成两个大于 1 的正因数的乘积，其中较小的一个正因数一定不超过 $\sqrt{61}$，并且它的素因数也是 61 的素因数. 这就是说，如果 61 是合数，那么它一定存在不超过 $\sqrt{61}$ 的素因数.

因此只需用 2～60 之间不超过 $\sqrt{61}$ 的素数试除 61 即可.

不超过 $\sqrt{61}$ 的素数为 2，3，5，7，由于它们都不整除 61，所以 61 是素数.

一般地，我们有下面的判别法：

> **如果大于 1 的整数 $a$ 不能被所有不超过$\sqrt{a}$的素数整除，那么 $a$ 一定是素数.**

这个判别法实际上给出了一种寻找素数的有效方法.

**例 3**　找出 1～100 中的全部素数.

**解**：只需把 1 与 1～100 之间的合数去掉即可. 而对于 1～100 之间的每个合数 $a$，它一定能被某个不超过$\sqrt{a}$的素数整除，从而能被不超过 $\sqrt{100}=10$ 的素数整除. 我们知道，不超过 10 的素数为 2，3，5，7. 在 1～100 中首先去掉 1，然后分别去掉 2，3，5，7 除自身以外的倍数，最后剩下的数就是不超过 100 的全部素数. 具体做法如下表：

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| ~~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~~ |

因此不超过 100 的素数为 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，共 25 个. 这种寻找素数的方法叫做**埃拉托斯特尼（Eratosthenes）筛法**.


1. 判断下列整数中哪些能分别被 3，7，9，11 整除：
   45，98，120，189，1001，1331，56382.
2. 探究并证明能被 11 整除的 5 位正整数的特征.
3. 已知 1626 除以某个整数，其商为 81，求除数与余数.
4. 判断 343，2027 是素数还是合数.

## 二 最大公因数与最小公倍数

### 1. 最大公因数

给定两个整数 $a$，$b$，必有公共的因数，叫做它们的**公因数**. 当 $a$，$b$ 不全为零时，在有限个公因数中最大的一个叫做 $a$，$b$ 的**最大公因数**，记作$(a, b)$.

例如，$-8$ 和 14 的全部公因数为 1，$-1$，2，$-2$，最大的公因数为 2，所以

$$(-8, 14)=2.$$

如果 $a$，$b$ 的最大公因数为 1，那么称 $a$，$b$ 是**互素**的.

类似地，我们可以定义三个或更多个整数的最大公因数和互素的概念. 将整数 $a$，$b$，$c$ 的最大公因数记作$(a, b, c)$，依此类推.

如何计算一组非零整数的最大公因数呢？我们已经学习过一种算法——短除法.

**思考**

试用短除法计算下列两组数的最大公因数：

(1) 375，105； (2) 1840，667.

从中你能感受到什么？

我们发现，用短除法求最大公因数有一定的局限性，因为用它每进行一次操作必须事先观察到一个大于 1 的公因数，而这一点有时难以做到. 特别是求两个较大整数的公因数时，这一点显得更为突出.

如何求 (1840，667)？一个自然的考虑是把 1840，667 通过适当的方式都变小，变小后，公因数就容易求出了. 如何变小呢？看下面的问题.

**思考**

如果 $b$ 除 $a$ 的余数为 $r$，那么$(a, b)$是否等于$(b, r)$？

事实上，若 $d$ 为 $a$，$b$ 的公因数，即 $d \mid a$，$d \mid b$，则 $d \mid a-bq=r$，从而 $d$ 为 $b$，$r$ 的公因数. 同理可证，$r$，$b$ 的公因数也是 $a$，$b$ 的公因数. 因此，$a$，$b$ 公因数的集合与 $r$，$b$ 公因数的集合相同，从而它们的最大公因数相等，即$(a, b)=(b, r)$.

按照这种思路，我们来求$(1840, 667)$.

因为 $1840=667\times2+506$，所以$(1840, 667)=(667, 506)$；又因为 $667=506\times1+$

161，所以(667，506)=(506，161)；又因为506=161×3+23，所以(506，161)=(161，23)，而(161，23)=23. 因此

$$(1840，667)=23.$$

这种求最大公因数的方法，叫做**辗转相除法**❶. 它是一种古老而有效的算法. 下面，我们给出辗转相除法的一般形式.

设$a$和$b$为任意两个整数，且$b\neq0$. 应用带余除法，以$b$除$a$，得商$q_1$和余数$r_1$. 如果$r_1\neq0$，那么再以$r_1$除$b$，得商$q_2$和余数$r_2$. 如果$r_2\neq0$，再以$r_2$除$r_1$，如此继续下去，$r_i(i=1，2，\cdots)$越来越小，有限次这种除法后，必然得到一个余数$r_n\neq0$，它整除前一个余数$r_{n-1}$. 于是，我们有：

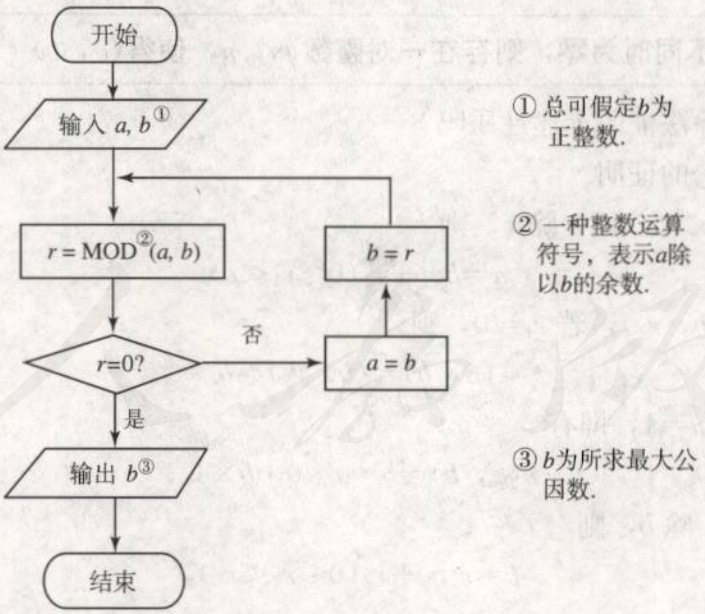
$$\begin{aligned}
&a=bq_1+r_1，\\
&b=r_1q_2+r_2，\\
&r_1=r_2q_3+r_3，\\
&\cdots\cdots\\
&r_{n-2}=r_{n-1}q_n+r_n，\\
&r_{n-1}=r_nq_{n+1}.
\end{aligned}$$

即

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

也就是说，$r_n$是$a$，$b$的最大公因数.

上述辗转相除法的过程可用下面的程序框图表示：




❶ 这种算法是欧几里得在公元前300年左右提出的，因此又叫欧几里得算法.

**探究**

你能根据上面的程序框图，编写一个计算机程序，求两个整数的最大公因数吗？

下面探讨三个整数的最大公因数的求法.

**探究**

1. 自己列举几组整数 $a$，$b$，$c$，计算并比较$(a, b, c)$，$((a, b), c)$，从中你能发现什么规律？

2. 求三个整数的最大公因数与求两个整数的最大公因数之间有什么联系？

我们发现，无论怎样选取 $a$，$b$，$c$，恒有

$$(a, b, c)=((a, b), c).$$

这表明，求三个整数的最大公因数，总可以转化为求两次两个整数的最大公因数.

对于多于三个整数的最大公因数，我们也有类似的结论.

关于最大公因数，有一条重要的性质. 这条性质在求解一次同余方程和不定方程时经常要用到.

**设整数 $a$，$b$ 不同时为零，则存在一对整数 $m$，$n$，使得$(a, b)=am+bn$.**

你能用辗转相除法证明上述性质吗？

下面我们给出它的证明.

证明：不妨设 $b>0$，用 $b$ 除 $a$，则

$$a=bq_1+r_1(0\leqslant r_1<b).$$

因为$(a, b)=(b, r_1)$，若 $r_1=0$，则

$$(a, b)=(b, r_1)=b.$$

此时取 $m=0$，$n=1$，即有

$$(a, b)=b=a\times 0+b\times 1.$$

若 $r_1\neq 0$，用 $r_1$ 除 $b$，则

$$b=r_1q_2+r_2(0\leqslant r_2<r_1),$$

且

$$(b, r_1)=(r_1, r_2).$$

若 $r_2=0$，则

$$(a, b)=(r_1, r_2)=r_1=a-bq_1.$$

此时取 $m=1$，$n=-q_1$，即有

$$(a, b)=r_1=a\times 1+b\times(-q_1).$$

若 $r_2\neq 0$，用 $r_2$ 除 $r_1$，则

$$r_1=r_2q_3+r_3\ (0\leqslant r_3<r_2),$$

且
$$(r_1,\ r_2)=(r_2,\ r_3).$$

若 $r_3=0$，则

$$(a,\ b)=(r_2,\ r_3)=r_2=b-r_1q_2=b-(a-bq_1)q_2$$
$$=a\times(-q_2)+b\times(1+q_1q_2).$$

此时取 $m=-q_2$，$n=1+q_1q_2$，即有

$$(a,\ b)=a\times(-q_2)+b\times(1+q_1q_2).$$

若 $r_3\neq0$，再用 $r_3$ 除 $r_2$，依次类推.

由上可知，这样的 $m$ 和 $n$ 是存在的.

这个性质对多于两个整数情形仍然成立，由它还可以推出整除的一条重要性质.

**若 $a\mid bc$，且$(a,\ b)=1$，则 $a\mid c$.**

下面我们给出它的证明.

**证明**：因为$(a,\ b)=1$，

所以存在一对整数 $m$，$n$，使得 $am+bn=1$.

于是　$(ac)m+(bc)n=c$.

又因为　$a\mid ac$，$a\mid bc$，

所以　$a\mid(ac)m+(bc)n$，即　$a\mid c$.

由整除的上述性质，我们可以得出素数的一条重要性质.

**设 $p$ 为素数，若 $p\mid ab$，则 $p\mid a$，或 $p\mid b$.**

下面我们给出它的证明.

**证明**：因为 $p$ 为素数，其正因数只有 1，$p$，所以

$$(p,\ a)=1，或(p,\ a)=p.$$

若$(p,\ a)=1$，则由上面整除的性质知

$$p\mid b.$$

若$(p,\ a)=p$，则 $p\mid a$.

素数的这条性质可以推广到一般情形：设 $p$ 为素数，若 $p\mid a_1a_2\cdots a_k$，则存在 $a_i(1\leqslant i\leqslant k)$，使得 $p\mid a_i$.

你能给出它的证明吗?

## 2. 最小公倍数

**思考**

甲、乙两个齿轮互相啮合，齿数分别为 84，36，在转动过程中同时啮合的两齿到下次再同时啮合，甲、乙两个齿轮分别转过多少圈?

这个问题的实质是，求出一个最小正整数，它同时为 84，36 的倍数.

事实上，任给两个非零整数 $a$，$b$，一定存在一个整数，它同时为 $a$，$b$ 的倍数，这个倍数叫做 $a$，$b$ 的**公倍数**. 例如，$|ab|$ 就是 $a$，$b$ 的一个公倍数.

我们把 $a$，$b$ 的最小的正公倍数叫做 $a$，$b$ 的**最小公倍数**，记作 $[a, b]$.

例如，8，$-6$ 的公倍数为 24，$-24$，48，$-48$，72，$-72$，…其中最小的正公倍数为 24，因此 $[8, -6]=24$.

类似地，我们还可以定义三个非零整数或更多个非零整数的最小公倍数的概念，将非零整数 $a$，$b$ 和 $c$ 的最小公倍数记作 $[a, b, c]$，依此类推.

下面我们证明两个非零整数 $a$，$b$ 的最小公倍数 $[a, b]$ 一定整除 $a$，$b$ 的公倍数.

**证明**：设 $[a, b]=m$，$n$ 为 $a$，$b$ 的任意一个公倍数.

对 $n$，$m$ 用带余除法：$n=mq+r(0\leqslant r<m)$.

假设 $m$ 不能整除 $n$，则 $r>0$.

由 $a \mid m$，$b \mid m$，$a \mid n$，$b \mid n$，得

$$a \mid n-mq=r,\ b \mid n-mq=r,$$

所以 $r$ 也是 $a$，$b$ 的一个正公倍数，而 $r<m$，这与 $m=[a, b]$ 矛盾.

因此，$m \mid n$.

## 探究

对于非零整数 $a$，$b$，我们研究了 $(a, b)$，$[a, b]$ 的一些性质，那么 $a$，$b$，$(a, b)$，$[a, b]$ 这些数之间有什么关系呢？

选取几组非零整数 $a$，$b$，分别计算并观察 $(a, b)$，$[a, b]$ 和 $ab$，并观察这三个数之间的关系.

我们发现，$(a, b)$，$[a, b]$ 和 $ab$ 之间存在下面的关系：

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

上述关系的证明此处略.

由上述关系可知，可以由两个非零整数乘积的绝对值除以它们的最大公因数求得它们的最小公倍数.

**例 4** 求 $[375, 105]$ 的值.

**解**：因为 $375=105\times3+60$，

$105=60\times1+45$，

$60=45\times1+15$，

$45=15\times3$，

所以

$$(375, 105)=15.$$

于是

$$[375,\ 105]=\frac{375\times105}{(375,\ 105)}=2625.$$

类似地，求多个非零整数的最小公倍数，可以转化为求两个非零整数的最小公倍数. 例如，$[a,\ b,\ c]=[[a,\ b],\ c]$.


1. 用辗转相除法求下列各组整数的最大公因数和最小公倍数：
   (1) $-39$，52；(2) 161，46；(3) 76，$-144$，42；(4) $-56$，84，76.
2. 求一组整数 $m$，$n$，使得 $35m+46n=1$.
3. 证明：如果 $a\mid c$，$b\mid c$，且 $(a,\ b)=1$，那么 $ab\mid c$.
4. 计算 6，12，18，…，2004 中 334 的倍数的个数.

## 三 算术基本定理

我们已经知道，任何大于 1 的整数总可以表示成一些素因数的乘积. 例如，$12=2\times2\times3$，$60=2\times2\times3\times5$. 一般地，我们有下面的定理.

**任何大于 1 的整数总可以分解成素因数乘积的形式，并且，如果不计分解式中素因数的次序，这种分解式是惟一的.**

这就是**算术基本定理**，定理中的分解式叫做素因数分解式. 它是欧几里得在公元前 3 世纪建立的，是整个初等数论的基础. 下面给出它的证明.

**证明**：对大于 1 的整数 $n$，其素因数分解式的存在性前面已经指出. 余下只需证明素因数分解式的惟一性.

假定 $n$ 有如下两个素因数分解式：

$$n=p_1p_2\cdots p_r=q_1q_2\cdots q_s,$$

其中 $p_1$，$p_2$，…，$p_r$ 与 $q_1$，$q_2$，…，$q_s$ 都是 $n$ 的素因数.

由于 $p_1$ 为素数，且 $p_1\mid q_1q_2\cdots q_s$，故 $p_1$ 整除 $q_1$，$q_2$，…，$q_s$ 中的某个 $q_i$. 当不计素因数的次序时，总可假定 $p_1\mid q_1$，而 $p_1$，$q_1$ 均为素数，故 $p_1=q_1$. 于是，$p_2\cdots p_r=q_2\cdots q_s$. 再由 $p_2$ 为素数，且 $p_2\mid q_2\cdots q_s$ 知，$p_2$ 整除 $q_2$，…，$q_s$ 中的某个 $q_j$. 若不计素因数的次序，可假定 $p_2\mid q_2$，而 $p_2$，$q_2$ 均为素数，同样有 $p_2=q_2$. 如此进行下去，最后得 $r=s$，并且 $p_i=q_i$，$i=1,\ 2,\ \cdots,\ r$.

所以 $n$ 的素因数分解式是惟一的.

在实际应用中，我们常常将素因数分解式中相同的几个素因数的乘积写成幂的形式.

例如，$12=2^2\times3$，$60=2^2\times3\times5$.

需要说明的是，素因数分解式只是一个理论结果，实际得到一个大于 1 的正整数的素因数分解式是很不容易的.

算术基本定理描述的是大于 1 的整数的素因数的分解情况，定理中的素因数分解式有非常重要的应用. 我们看一个具体的例子.

**例 5** 分别将 720，152 进行素因数分解. 由素因数分解式，你能求出(720，152)以及[720，152]吗?

**解**：容易知道，720 的素因数只有 2，3，5，且

$$720=2^4\times3^2\times5;$$

152 的素因数只有 2，19，且

$$152=2^3\times19.$$

由此，我们不难得到

$$(720，152)=2^3=8,$$

$$[720，152]=2^4\times3^2\times5\times19=13680.$$

由例 5 不难看出，由两个大于 1 的整数的素因数分解式，可以求得这两个整数的最大公因数和最小公倍数.

一般地，对给定的两个大于 1 的整数 $a$，$b$，找出它们所有的互异素因数，然后将 $a$，$b$ 表示成这些素因数的幂的乘积，如果其中一个素因数在 $a$ 或 $b$ 中不出现，就将这个素因数的幂指数写作 0，那么$(a，b)$可以表示成这些素因数的幂的乘积，每个素因数的幂指数为其在 $a$ 与 $b$ 中的幂指数的最小者，而$[a，b]$也可以表示成这些素因数幂的乘积，每个素因数的幂指数为其在 $a$ 与 $b$ 的幂指数的最大者.


用素因数分解式计算：

(1) (152，216)；　　(2) [152，216].

与用辗转相除法求两个整数的最大公因数和最小公倍数相比，你有什么体会?

# 第二讲　同余与同余方程

上讲我们讨论了整数之间的整除关系. 本讲我们介绍整数之间一种更精细的关系：同余关系. 它的引入极大地丰富了数论的内容，简化了数论中的许多问题. 利用同余关系可以进一步讨论整除；对整数集合进行分类，将彼此同余的整数放在一起，得到一类整数，称为剩余类. 每个剩余类可看作一个特殊的“数”. 对于这些“数”，我们可以像普通的数一样引入加法、乘法运算. 在此基础上，我们讨论同余方程和同余方程组的解法. 同余在初等数论中占有极为重要的地位.

## 一　同余

### 1. 同余的概念

**观察**

观察下面的月历：

| 九　月 | | | | | | |
|---|---|---|---|---|---|---|
| 日 | 一 | 二 | 三 | 四 | 五 | 六 |
| | 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 | | | | |

在月历表中位于同一列的整数被 7 除后的余数有什么规律？在其他的月历中是否也有同样的规律？

在月历表中位于同一列的整数被 7 除后的余数是相同的，如 1，8，15，22，29 被 7 除后，余数都是 1. 在其他的月历中也有同样的规律.

我们把这些被 7 除后余数相同的整数称作是模 7 同余的.

**一般地，设 $n$ 为正整数，$a$ 和 $b$ 为整数．如果 $a$ 和 $b$ 被 $n$ 除后余数相同，那么称 $a$ 和 $b$ 模 $n$ 同余，记作 $a\equiv b(\mathrm{mod}\ n)$．若 $a$ 和 $b$ 被 $n$ 除后余数不同，则称 $a$ 和 $b$ 模 $n$ 不同余，记作 $a\not\equiv b(\mathrm{mod}\ n)$．**

例如，12 与 $-6$ 被 9 除后余数均为 3，所以 $12\equiv -6(\mathrm{mod}\ 9)$，而 $-15$ 与 21 被 7 除后余数分别为 6 和 0，所以 $-15\not\equiv 21(\mathrm{mod}\ 7)$．

由同余的概念，我们容易知道，同余与整除存在密切的关系．

高斯（Gauss，C. F.，1777—1855）德国数学家、天文学家、物理学家．

高斯被誉为历史上伟大的数学家之一，和阿基米德、牛顿并列，同享盛名．高斯的数学成就遍及各个领域，在数论、代数学、微分几何等方面均有一系列开创性贡献．

**思考**

模 $n$ 同余的两个整数 $a$，$b$，与 $n$ 有什么关系？

设 $a$，$b$ 被 $n$ 除后的商分别为 $q$，$q'$，余数分别为 $r$，$r'$，则

$$a=nq+r,\qquad b=nq'+r'.$$

若 $a\equiv b(\mathrm{mod}\ n)$，则 $r=r'$，并且 $a-b=n(q-q')$，于是 $n\mid a-b$．反过来，若 $n\mid a-b=n(q-q')+r-r'$，则 $n\mid r-r'$，而 $-n<r-r'<n$，故 $r-r'=0$，从而 $r=r'$，因此 $a\equiv b(\mathrm{mod}\ n)$．

因此，我们有

$$a\equiv b(\mathrm{mod}\ n)\Leftrightarrow n\mid a-b.$$

**探究**

根据 $a\equiv b(\mathrm{mod}\ n)\Leftrightarrow n\mid a-b$，探索同余满足下面同余的三条性质：

（1）$a\equiv a(\mathrm{mod}\ n)$；

（2）若 $a\equiv b(\mathrm{mod}\ n)$，则 $b\equiv a(\mathrm{mod}\ n)$；

（3）若 $a\equiv b(\mathrm{mod}\ n)$，且 $b\equiv c(\mathrm{mod}\ n)$，则 $a\equiv c(\mathrm{mod}\ n)$．

由上可知，模 $n$ 同余给出了整数之间的一种关系，这种关系我们称之为同余关系．利用同余关系，我们可以对整数集进行分类：将整数集中所有模 $n$ 同余的整数放在一起构成一个集合．例如，利用模 2 同余可将整数集分成两个集合：

（1）模 2 同余于 0 的整数构成偶数集；

❶ mod 这个记号是高斯发明的．

(2) 模 2 同余于 1 的整数构成奇数集.

## 2. 同余的性质

从同余的概念和上面的探究，我们不难发现，同余式 $a\equiv b(\mathrm{mod}\ n)$ 与等式 $a=b$ 有许多类似的性质.

**探究**

类比等式的性质，你能猜想同余式的一些性质吗？试根据同余的概念，探究同余的下列性质：

1. 若 $a\equiv b(\mathrm{mod}\ n)$，且 $c\equiv d(\mathrm{mod}\ n)$，则

(1) $a+c\equiv b+d(\mathrm{mod}\ n)$；

(2) $ac\equiv bd(\mathrm{mod}\ n)$；

(3) $ka\equiv kb(\mathrm{mod}\ n)$，$k$ 为任意整数；

(4) $a^m=b^m(\mathrm{mod}\ n)$，$m$ 为正整数.

2. 若 $ab\equiv ac(\mathrm{mod}\ n)$，且 $(a,\ n)=1$，则 $b\equiv c(\mathrm{mod}\ n)$.

我们给出性质 1(1)及性质 2 的证明，余下的请同学们自己证明：

1° 证明：因为 $a\equiv b(\mathrm{mod}\ n)$，$c\equiv d(\mathrm{mod}\ n)$，

所以　$n\mid a-b$，$n\mid c-d$，

因此　$n\mid c-d+a-b$，即　$n\mid (a+c)-(b+d)$.

所以　$a+c=b+d(\mathrm{mod}\ n)$.

性质 1 说明，类似整数集中两个等式两端对应加、减、乘仍得到等式，同余式两端对应加、减、乘仍然是同余的.

2° 证明：因为 $(a,\ n)=1$，

所以存在一对整数 $k$，$l$，使得

$$ak+nl=1.$$

因此　$n\mid nl=1-ak$，即

$$ak\equiv 1(\mathrm{mod}\ n).$$

又因为　$ab\equiv ac(\mathrm{mod}\ n)$，

所以　$kab\equiv kac(\mathrm{mod}\ n)$. 而 $ka\equiv 1(\mathrm{mod}\ n)$，

因此　$b\equiv c(\mathrm{mod}\ n)$.

性质 2 可以看作是同余意义下的消去律，消去律的前提是 $a$ 与 $n$ 必须互素，否则结论不一定成立.

利用同余的这些性质，我们可以简化数论中的许多问题.

先看星期几问题. 如果今天为星期天，过 $n$ 天后的今天是星期几？这个问题并不难回答，我们只需对 $n$ 和 7 用带余除法，由余数即可确定. 但是，有时直接应用带余除法求余

数是困难的，特别是当被除数较大时，如下例.

**例 1** 今天为星期日，过 $2004^{2004}$ 天后的今天是星期几?

**分析**：$2004^{2004}$ 这个数很大，我们很难直接判断 7 除 $2004^{2004}$ 的余数是几. 现在，我们想办法把 $2004^{2004}$ 变小. 一个自然的考虑是 7 除底数 2004 的余数是几，利用这个余数替换底数 2004，然后降次，反复进行这个过程，直至去掉指数.

**解**：因为 $2004=7\times286+2$，所以 $2004\equiv2\pmod 7$.

由同余的性质，有

$$2004^{2004}\equiv2^{2004}\pmod 7,$$

而 $2^{2004}=8^{668}$，所以 $2^{2004}\equiv8^{668}\pmod 7$.

又因为 $8\equiv1\pmod 7$，所以 $8^{668}\equiv1^{668}=1\pmod 7$.

因此 $2004^{2004}\equiv1\pmod 7$，即 7 除 $2004^{2004}$ 的余数为 1，所以过 $2004^{2004}$ 天后的今天是星期一.

再看一个整除问题的例子.

**例 2** 证明：$17\mid 19^{1000}-1$.

**分析**：类似例 1，我们想办法把 $19^{1000}$ 变小，用 17 除底数 19 的余数替换底数 19，然后降次，反复进行这个过程，直至去掉指数.

由例 2 你能体会同余方法在解决整除问题中的作用吗?

**证明**：要证 $17\mid 19^{1000}-1$，只需证 $19^{1000}\equiv1\pmod{17}$，

因为 $19\equiv2\pmod{17}$，所以

$$19^{1000}\equiv2^{1000}=16^{250}\pmod{17}.$$

又由于 $16\equiv-1\pmod{17}$，故 $16^{250}\equiv(-1)^{250}=1\pmod{17}$.

因此 $17\mid 19^{1000}-1$.


1. 试用同余的性质证明能被 3，9，7，11 整除的正整数的特征.
2. 已知今天是星期二，过 $2008^{2008}$ 天后的今天是星期几?
3. 证明：$7\nmid 2^n+1$，$n$ 为任意自然数.
4. 求 $3^{50}$ 的十进制表示中的末两位数字.
5. 证明：对任意自然数 $n$，$4n+3$ 不是两个整数的平方和.

## 二 剩余类及其运算

我们知道，一个整数被正整数 $n$ 除后，余数有 $n$ 种情形：0，1，2，3，…，$n-1$，它们彼此模 $n$ 不同余. 这表明，每个整数恰与这 $n$ 个整数中某一个模 $n$ 同余.

这样一来，按模 $n$ 是否同余对整数集进行分类，我们可以将整数集分成 $n$ 个两两不相交的子集. 例如，按模 6 是否同余可将整数集分成下面六个子集：

$$\{\cdots, -12, -6, 0, 6, 12, \cdots\},$$
$$\{\cdots, -11, -5, 1, 7, 13, \cdots\},$$
$$\{\cdots, -10, -4, 2, 8, 14, \cdots\},$$
$$\{\cdots, -9, -3, 3, 9, 15, \cdots\},$$
$$\{\cdots, -8, -2, 4, 10, 16, \cdots\},$$
$$\{\cdots, -7, -1, 5, 11, 17, \cdots\},$$

它们分别是由与 0，1，2，3，4，5 模 6 同余的整数构成的集合.

**我们把所有与整数 $a$ 模 $n$ 同余的整数构成的集合叫做模 $n$ 的一个剩余类，记作 $[a]$**[1]，并把 $a$ 叫做剩余类 $[a]$ 的一个**代表元**.

例如，模 6 的不同剩余类有 6 个，它们分别为 $[0]$，$[1]$，$[2]$，$[3]$，$[4]$，$[5]$；模 2 的剩余类有 2 个：$[0]$，$[1]$，它们分别代表偶数集和奇数集.

需要指出的是，对模 $n$ 的每个剩余类，我们可以用不同的代表元表示. 如在模 6 的剩余类中，$[5]=[-1]=[11]$.

一般地，我们有

$$a\equiv b(\bmod n)\Leftrightarrow [a]=[b].$$

事实上，对任意 $c\in[a]$，我们有 $a\equiv c(\bmod n)$. 若 $a\equiv b(\bmod n)$，则 $c\equiv b(\bmod n)$，从而 $c\in[b]$. 同理可证，对任意 $c\in[b]$，则 $c\in[a]$. 因此 $[a]=[b]$.

反过来的正确性是显而易见的.

**探究**

分别从模 6 的剩余类 $[2]$ 和 $[3]$ 中，选取一个元素进行加法和乘法运算：(1) 和与积分别位于哪个剩余类中？(2) 结果与代表元的选取有关吗？(3) 换其他剩余类是否也有类似的结果？

我们发现，每个模 $n$ 的剩余类可以看作一个特殊的“数”，如同整数. 我们可以在这 $n$ 个“数”构成的集合中引入两种运算，一种叫**剩余类加法**（仍用“+”表示），另一种叫**剩余类乘法**（仍用“·”表示，但通常省略不写）：

$$\text{剩余类加法：}[a]+[b]=[a+b],$$
$$\text{剩余类乘法：}[a][b]=[ab].$$

如果模 $n$ 的剩余类集合中定义了剩余类加法和剩余类乘法运算，就把它叫做**模 $n$ 的剩余类环**，并记作

[1] 今后我们总用 $[a]$ 表示剩余类，请不要与第一讲的取整函数 $[x]$ 混淆.

$\{[0], [1], \cdots, [n-1]; +, \cdot\}$.

## 探究

引进一种运算，自然要看它满足怎样的运算律. 我们知道，模 5 的剩余类环为

$\{[0], [1], [2], [3], [4]; +, \cdot\}$

根据剩余类加法运算和乘法运算的定义，填写下面的表格.

剩余类加法运算表

| + | [0] | [1] | [2] | [3] | [4] |
|---|---|---|---|---|---|
| [0] | [0] | [1] | [2] | [3] | [4] |
| [1] | [1] | | | | |
| [2] | [2] | | | | |
| [3] | [3] | | | | |
| [4] | [4] | | | | |

剩余类乘法运算表

| · | [0] | [1] | [2] | [3] | [4] |
|---|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | | | | |
| [2] | [0] | | | | |
| [3] | [0] | | | | |
| [4] | [0] | | | | |

每类运算中，你能举一个例子说明这种运算吗？从中你发现了哪些运算律？

我们知道，整数加法、乘法运算遵循交换律、结合律和分配律. 由上面的探究，你是否发现了剩余类加法、乘法运算也遵循交换律、结合律和分配律？

另外，在模 $n$ 的剩余类环中，对任意剩余类$[a]$，恒有

$$[a]+[0]=[0]+[a]=[a],$$
$$[a][0]=[0][a]=[0],$$
$$[a][1]=[1][a]=[a].$$

这样，$[0]$与$[1]$与整数集中的 0 与 1 具有同样的运算性质，我们把$[0]$与$[1]$分别叫做模 $n$ 的剩余类环的**零元**和**单位元**.

类比数集中的相反数和倒数，我们引入模 $n$ 的剩余类的负元和逆元的概念.

如果存在模 $n$ 的剩余类$[b]$，使得

$$[a]+[b]=[b]+[a]=[0],$$

那么称$[b]$为$[a]$的**负元**❶.

从模 5 的剩余类加法的运算表可以看出，模 5 的剩余类$[a]$均存在负元.

相应地，如果存在剩余类$[b]$，使得

$$[a][b]=[b][a]=[1],$$

那么称剩余类$[a]$可逆，并把$[b]$叫做$[a]$的**逆元**❷.

---

❶ 负元类似于数集中一个数的相反数的概念.

❷ 逆元类似于数集中一个数的倒数的概念.

从模 5 的剩余类乘法的运算表可以看出，模 5 的剩余类环中每个非零元$[a]$都存在逆元.

**思考**

是否模 $n$ 的剩余类中的每个非零元$[a]$都存在逆元呢?

我们不妨看一下模 6 的剩余类环. 由剩余类的乘法运算，填写下表：

剩余类乘法运算表

| · | [0] | [1] | [2] | [3] | [4] | [5] |
|---|---|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | | | | | |
| [2] | [0] | | | | | |
| [3] | [0] | | | | | |
| [4] | [0] | | | | | |
| [5] | [0] | | | | | |

从中你发现了什么?

从表中可以发现，[2]，[3]，[4]与模 6 的剩余类环中任何其他元进行乘法运算都不等于[1]，也就是说，模 6 的剩余类环中，[2]，[3]，[4]不存在逆元.

那么，什么情况下，一个模 $n$ 的剩余类环中非零元$[a]$都有逆元呢?

我们看下面的式子：

$[a][b]=[b][a]=[1]\Leftrightarrow[ab]=[ba]=[1]\Leftrightarrow ab=ba\equiv 1(\mathrm{mod}\ n)\Leftrightarrow$存在整数 $t$，使得 $ab+nt=1$.

上式表明，若非零元$[a]$有逆元，不妨设为$[b]$，则存在整数 $t$，使得 $ab+nt=1$. 而 $(a, n)\mid a$，$(a, n)\mid n$，故$(a, n)\mid 1$，所以$(a, n)=1$.

反过来，若$(a, n)=1$，由最大公因数的性质，存在一对整数 $b$，$t$，使得

$$ab+nt=1.$$

于是$[a][b]=[b][a]=1$，即$[b]$为非零元$[a]$的逆元.

因此，非零元$[a]$有逆元的充要条件是$(a, n)=1$.

需要说明的是，在整数集中，乘法运算有一个重要特征：任意两个非零整数的乘积不等于零，我们把这个特征叫做无零因子. 但是，对模 6 的剩余类乘法，不具备这个特征. 从模 6 的剩余类乘法的运算表可以发现，$[2]\neq[0]$，$[3]\neq[0]$，但是$[2][3]=[0]$. 这表明，模 6 的剩余类环是有零因子的.

这一点与数的乘法运算有很大的区别. 你有什么体会?

从模 5 的剩余类乘法的运算表可以发现，模 5 的剩余类环无零因子.


1. 证明：剩余类加法运算和乘法运算与代表元的选取无关.
2. 证明：在模 $n$ 的剩余类环中，若$[a]$存在逆元，则它的逆元仅有一个.
3. 给出模 $n$ 的剩余类环中每个非零元都存在逆元的条件，并说明理由.

## 三 费马小定理和欧拉定理

### 探究

在模 3 的剩余类环中，下列等式是否成立？为什么？

(1) $[0^3]=[0]$；

(2) $[1^3]=[1]$；

(3) $[2^3]=[2]$.

我们发现，探究中的三个等式都是成立的.

事实上，我们还可以进一步探究得知，在模 5 的剩余类环中，仍然存在这种规律. 即

$$[0^5]=[0],$$
$$[1^5]=[1],$$
$$[2^5]=[2],$$
$$[3^5]=[3],$$
$$[4^5]=[4].$$

不难验证，在模 7 的剩余类环中仍然存在这种规律.

由于 3，5，7 均为素数，我们大胆地猜想：当 $m$ 为素数时，对任意整数 $a$，总有

$$[a^m]=[a], \text{ 或 } a^m\equiv a(\mathrm{mod}\ m).$$

特别地，当$(a, m)=1$ 时，运用同余意义下的消去律，可得

$$a^m\equiv a(\mathrm{mod}\ m)\Leftrightarrow a^{m-1}\equiv 1(\mathrm{mod}\ m).$$

事实上，这个猜想是正确的. 这就是费马小定理.

**费马小定理** 设 $m$ 为素数，$a$ 为任意整数，且$(a, m)=1$，则 $a^{m-1}\equiv 1(\mathrm{mod}\ m)$.

费马（Fermat，P. de.，1601—1665）法国数学家.

费马在数论、解析几何、概率论等方面都有重大贡献. 费马特别爱好数论，他证明或提出许多命题，最有名的是费马大定理，即不可能有满足 $x^n+y^n=z^n$，$n>2$ 的正整数 $x$，$y$，$z$，$n$ 存在.

费马小定理是费马在 1640 年提出的，但当时没有给出证明.

下面我们给出它的证明.

**证明**：由$(a, m)=1$，可知$m$不是$a$的素因数，

又因为$m$不是1，2，3，…，$m-1$的素因数，所以$a$，$2a$，$3a$，…，$(m-1)a$均不能被$m$整除.

又因为$a$，$2a$，$3a$，…，$(m-1)a$模$m$两两不同余，所以它们分别属于模$m$的除[0]以外的$m-1$个不同的剩余类中. 由同余的性质1可知

$$a\times 2a\times 3a\times\cdots\times(m-1)a$$
$$\equiv 1\times 2\times 3\times\cdots\times(m-1)\pmod m.$$

因此$a^{m-1}(m-1)!\equiv(m-1)!\pmod m$.

又由于$(m-1)!$不含素因数$m$，所以

$$((m-1)!, m)=1.$$

由同余的性质2可知

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

例如，$a=8$，$m=5$，我们知道，

$$8\times 1\equiv 3\pmod 5,\quad 8\times 2\equiv 1\pmod 5,$$
$$8\times 3\equiv 4\pmod 5,\quad 8\times 4\equiv 2\pmod 5.$$

那么$8^4\times 4!\equiv 4!\pmod 5$. 而$(4!, 5)=1$，故

$$8^4\equiv 1\pmod 5.$$

用证明费马小定理的方法，我们还可以证明更一般的结论——欧拉定理.

欧拉(Euler, L., 1707—1783)，瑞士数学家.

欧拉是18世纪数学界杰出的人物之一，他不但在数学上作出伟大贡献，而且把数学用到了几乎整个物理领域. 在数学的许多分支中，我们常常见到以他的名字命名的重要常数、公式和定理.

1736年，欧拉第一次给出了费马小定理的证明，并于1760年证明了更一般的欧拉定理.

**欧拉定理**　**设$m$为正整数，$a$为任意整数，且$(a, m)=1$，则**

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

**其中$\varphi(m)$表示1，2，…，$m$中与$m$互素的正整数的个数.**

$\varphi(m)$称为欧拉函数. 当$m$为素数时，从1到$m$的整数中与$m$互素的整数为1，2，…，$m-1$，共有$m-1$个，所以$\varphi(m)=m-1$. 一般地，当$m$为大于1的整数时，有

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

其中$p_1$，$p_2$，…，$p_k$为$m$的所有互异的素因数.

一般情形$\varphi(m)$的表达式的证明，可参见附录一.

下面我们给出欧拉定理的证明.

**证明**：记$\varphi(m)=r$，并用$a_1$，$a_2$，…，$a_r$表示1，2，3，…，$m$中所有与$m$互素的整数.

因为$(a, m)=1$，且$a_1$，$a_2$，…，$a_r$与$m$均互素，所以$aa_1$，$aa_2$，…，$aa_r$与$m$均是互素的（为什么?）. 从而它们分属于模$m$的$r$个剩余类$[a_1]$，$[a_2]$，…，$[a_r]$. 由同余的性质1可得：

$$a^r a_1 a_2 \cdots a_r \equiv a_1 a_2 \cdots a_r \pmod{m}.$$

又因为 $a_1$，$a_2$，…，$a_r$ 均与 $m$ 互素，由同余的性质 2 可得 $a^r \equiv 1 \pmod{m}$，即

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

在欧拉定理中，如果 $m$ 为素数，此时 $\varphi(m)=m-1$，那么我们得到了费马小定理. 费马小定理是欧拉定理的特例.

欧拉定理和费马小定理有许多重要的应用，利用它们可以简化许多计算.

**例 3** 求 $13^{2004}$ 除以 17 的余数.

**分析**：遇到有关带指数的被除数的问题，我们首先考虑运用同余、互素以及欧拉定理或费马小定理，降次使被除数变小，进而求出余数.

**解**：容易知道 17 为素数，且(13，17)=1，由费马小定理可知

$$13^{17-1}=13^{16} \equiv 1 \pmod{17}.$$

又因为 $2004=16\times125+4$，且 13 为素数，所以

$$13^{2004}=(13^{16})^{125}\times13^4 \equiv 13^4 \pmod{17}.$$

而 $13^4=169^2=(170-1)^2 \equiv (-1)^2=1 \pmod{17}$，

因此 $13^{2004} \equiv 1 \pmod{17}$，即

$13^{2004}$ 除以 17 的余数为 1.

**例 4** 求使 $5^m \equiv 1 \pmod{21}$ 成立的最小正整数 $m$.

**分析**：$5^m \equiv 1 \pmod{21}$ 与欧拉定理的形式类似，而且(5，21)=1，$\varphi(21)$ 容易求出. 我们考虑使用欧拉定理.

**解**：因为(5，21)=1，且 $\varphi(21)=12$（即 1，2，…，20 中与 21 互素的数有 12 个），由欧拉定理有

$$5^{12} \equiv 1 \pmod{21}.$$

显然，$m \leqslant 12$. 令 $12=mq+r$，其中 $0 \leqslant r < m$，则有

$$5^{12}=5^{mq+r}=(5^m)^q\times5^r,$$

所以 $1 \equiv 5^r \pmod{21}$.

由 $m$ 是使同余式成立的最小正整数知 $r=0$，从而 $m \mid 12$. 检验 12 的正因数 1，2，3，4，6，12，我们发现

$$5^1 \equiv 5 \pmod{21},\ 5^2 \equiv 4 \pmod{21},$$
$$5^3=20 \pmod{21},\ 5^4 \equiv 16 \pmod{21},$$
$$5^6 \equiv 1 \pmod{21},$$

因此，最小正整数 $m$ 为 6.

由上面的例子不难看出，费马小定理和欧拉定理在解决较大数的整除或同余问题时具有重要的作用.


1. 求 $47^{7385}$ 除以 19 的余数.
2. 求使 $18^x \equiv 1 \pmod{25}$ 成立的最小正整数 $x$.
3. 证明：任何正整数的 12 次方要么是 13 的倍数，要么是 13 的倍数加 1.

## 四　一次同余方程

### 1. 一次同余方程

前面已经提到，剩余类可以看作特殊的“数”，剩余类环可以看作是定义了剩余类加法和剩余类乘法运算的“数集”. 类似于实数集情形，我们也可以在剩余类环中解方程或方程组.

例如，在模 6 的剩余类环中解方程 $[5][x]=[3]$，这里，$[x]$ 是模 6 的剩余类环中的未知剩余类. 注意到在模 6 的剩余类环中，有

$$[5][x]=[3]\Leftrightarrow[5x]=[3]\Leftrightarrow 6\mid 5x-3\Leftrightarrow 5x\equiv 3 \pmod 6,$$

因此，原方程可表示成下面含未知数的同余式：

$$5x\equiv 3 \pmod 6.$$

通常，我们把含有未知数的同余式叫做**同余方程**. 方程 $5x\equiv 3 \pmod 6$ 是一类形式最简单的同余方程，叫做**一次同余方程**. 一次同余方程的一般形式为

$$ax \equiv b \pmod n, \tag{1}$$

其中 $n$ 为正整数，$a$，$b$ 为整数，且 $a$ 不等于零.

若存在整数 $c$，使得同余式 $ac\equiv b \pmod n$ 成立，则把 $x\equiv c \pmod n$ 叫做**一次同余方程 $ax\equiv b \pmod n$ 的解**. 例如，$x\equiv 3 \pmod 6$ 是 $5x\equiv 3 \pmod 6$ 的解.

如果 $x\equiv d \pmod n$ 也是同余方程(1)的解，且 $c\equiv d \pmod n$，那么我们将这两个解视作一样的. 实际上，在这种意义下，一次同余方程的解可理解为模 $n$ 的一个剩余类，是一个集合，而不是一个整数. 因此，要判断一个模 $n$ 的剩余类是不是同余方程的解，只需选取剩余类中的一个代表元，看它是否使同余式成立即可.

由上面的分析可知，解剩余类环中的方程总可以转化为解某个同余方程. 与我们熟悉的解一元一次方程、一元二次方程等过程类似，对于一次同余方程，我们关心下面几个问题：

(1) 一次同余方程 $ax\equiv b \pmod n$ 什么情况下有解？

(2) 有多少解？

(3) 有解时如何描述所有的解？

1° 先讨论特殊情形，即当 $(a, n)=1$ 的情形.

我们知道，当 $(a, n)=1$ 时，存在整数 $k$，$l$，使得 $ak+nl=1$，于是 $n \mid nl=1-ak$，

即

$$ak\equiv 1(\bmod n).$$

因此，$ax\equiv b(\bmod n)\Leftrightarrow ax\equiv (ak)b=a(kb)(\bmod n)\Leftrightarrow x\equiv kb(\bmod n)$.

因此，同余方程(1)仅有一个解 $x\equiv kb(\bmod n)$.

2° 再讨论$(a, n)=d>1$ 的情形.

若同余方程(1)有解，不妨设 $x\equiv c(\bmod n)$为它的一个解，则 $ac\equiv b(\bmod n)$，从而 $n\mid ac-b$. 由于 $d\mid a$，$d\mid n$，故 $d\mid ac$，$d\mid ac-b$，从而 $d\mid ac-(ac-b)=b$. 这表明，同余方程(1)有解时，必有 $d\mid b$.

那么，当 $d\mid b$ 时，同余方程(1)是否一定有解呢?

记 $a=a'd$，$n=n'd$，$b=b'd$，则$(a', n')=1$. 注意到，

$$ax\equiv b(\bmod n)\Leftrightarrow n\mid ax-b\Leftrightarrow n'd\mid (a'x-b')d\Leftrightarrow n'\mid a'x-b',$$

于是同余方程(1)可化简为

$$a'x\equiv b'(\bmod n'). \tag{2}$$

由于$(a', n')=1$，由情形 1°的讨论知，同余方程(2)有惟一解 $x\equiv k'b'(\bmod n')$，此时 $x=k'b'+n'l$，其中 $l$ 为任意整数.

对 $l$，$d$ 用带余除法：$l=dq+r$，$0\leqslant r\leqslant d-1$，则

$$x=k'b'+n'(dq+r)=k'b'+nq+n'r,$$

其中 $0\leqslant r\leqslant d-1$，$q$ 为整数. 于是

$$x\equiv k'b'+n'r(\bmod n),\ r=0,\ 1,\ \cdots,\ d-1.$$

容易检验，它们都是同余方程(1)的解.

综上所述，我们得到下面的结论.

> **一次同余方程 $ax\equiv b(\bmod n)$有解，则$(a, n)\mid b$. 反过来，当$(a, n)\mid b$ 时，一次同余方程 $ax\equiv b(\bmod n)$恰有$(a, n)$个解.**

下面看一个解一次同余方程例子.

**例 5** 解一次同余方程 $9x\equiv 6(\bmod 15)$.

**解**：注意到$(9, 15)=3$，且 $3\mid 6$，故同余方程有三个解. 原同余方程可化简为 $3x\equiv 2(\bmod 5)$. 由于 $3\times 2\equiv 1(\bmod 5)$，故 $x\equiv 2\times 2=4(\bmod 5)$. 所以，原同余方程的三个解分别为 $x\equiv 4+5\times 0=4(\bmod 15)$，$x\equiv 4+5\times 1=9(\bmod 15)$，$x\equiv 4+5\times 2=14(\bmod 15)$.

### 2. 大衍求一术

对于一次同余方程的解法，我们古代一些数学家曾做出过巨大的贡献，其中比较有名的是——大衍求一术.

大衍求一术是解一次同余方程 $ax\equiv 1(\bmod n)$，其中 $a$ 为正整数，$a<n$，且$(a, n)=1$ 的一种算法程序. 我国宋代大数学家秦九韶（约 1202—约 1261）继承前人造历算法经验，在其所著的《数书九章》中给出了解法：

秦九韶称 $a$ 为衍母，$n$ 为定母，并称满足同余式的最小正整数为乘率. 大衍求一术的

法则是：

置衍右上，定居下．立天元一于左上．先以右上除右下，所得商数与左上一相生并入左下．然后乃以右行上下，以少除多，递互除之．所得商数，随即递互累乘．归左行上下……须使右上末后奇一而止．乃验左上所得，以为乘率．

用现代数学的语言，大衍求一术的算法步骤可表述为：

先规定 $k_1=1$，$r_1=a$，

对 $n$，$a$ 用带余除法：$n=aq_2+r_2$，记 $k_2=-q_2k_1$；

对 $a$，$r_2$ 用带余除法：$a=r_2q_3+r_3$，记 $k_3=k_1-q_3k_2$；

对 $r_2$，$r_3$ 用带余除法：$r_2=r_3q_4+r_4$，记 $k_4=k_2-q_4k_3$；

对 $r_3$，$r_4$ 用带余除法：$r_3=r_4q_5+r_5$，记 $k_5=k_3-q_5k_4$；

……

重复这种运算，直到余数 $r_n=1$，那么最后所得 $k_n=k_{n-2}-q_nk_{n-1}$ 满足 $ak_n\equiv1\pmod n$．于是 $x\equiv k_n\pmod n$ 就是一次同余方程 $ax\equiv1\pmod n$ 的解．

**探究**

试将大衍求一术算法步骤中的余数 $r_2$，$r_3$，$r_4$，$r_5$ 分别写成 $ax+ny$ 的形式，从中你能发现什么规律？

下面考察一下大衍求一术的算法原理．

我们发现，

$$r_1=a=ak_1\pmod n,$$
$$r_2=n-r_1q_2\equiv a(-q_2k_1)=ak_2\pmod n,$$
$$r_3=r_1-r_2q_3\equiv a(k_1-q_3k_2)=ak_3\pmod n,$$
$$r_4=r_2-r_3q_4\equiv a(k_2-q_4k_3)=ak_4\pmod n,$$
……

而 $r_n=1$，故 $ak_n\equiv1\pmod n$．这就是大衍求一术的算法原理．

下面看一个用大衍求一术解同余方程的例子．

**例 6**　解同余方程 $33x\equiv1\pmod{74}$．

**解**：显然 $(33,74)=1$．

由于 $74=33\times2+8$，$33=8\times4+1$，故 $q_2=2$，$q_3=4$，$r_3=1$．依次可计算出

$$k_2=-2\times1=-2,\ k_3=1-4\times(-2)=9.$$

因此原方程的解为

$$x\equiv9\pmod{74}.$$


解下列同余方程：

(1) $9x\equiv5\pmod 7$；　(2) $32x\equiv12\pmod 8$；

(3) $28x\equiv124\pmod{116}$；　(4) $5x\equiv44\pmod{81}$.

## 五　拉格朗日插值法和孙子定理

约在2000多年以前，我国古代数学著作《孙子算经》中提出了著名的“物不知其数”问题：“今有物不知其数，三三数之余二，五五数之余三，七七数之余二，问物几何.”答曰：“二十三.”

我国历史上还有很多人研究过这类问题，其名称也多种多样. 后来，人们将这类问题的解法进一步发展和推广，并称之为孙子定理，在国外文献和教科书中称为“中国剩余定理”.

我国明代程大位在“算法统宗”(1592)中以诗的语言写出了“物不知其数”问题的算法口诀：“三人同行七十稀，五树梅花廿一枝，七子团圆月正半，除百零五便得知.”

设物数为 $x$，那么“物不知其数”问题相当于解如下形式的方程组：

$$\begin{cases} x\equiv 2\pmod 3, \\ x\equiv 3\pmod 5, \\ x\equiv 2\pmod 7. \end{cases} \qquad (※)$$

这种方程组，我们称为同余方程组.

如果存在正整数 $k$，使得(※)中每个同余式成立，那么 $k$ 就是“物不知其数”问题的一个解.

容易检验，当 $k$ 使得(※)中每个同余式都成立时，所有模 $3\times5\times7=105$ 同余于 $k$ 的整数，也使得(※)中每个同余式成立. 反过来，如果还有整数 $l$ 使得(※)中每个同余式成立，那么

$$l\equiv k\pmod 3,\ l\equiv k\pmod 5,\ l\equiv k\pmod 7,$$

于是 $3\mid l-k$，$5\mid l-k$，$7\mid l-k$. 这表明 $l-k$ 含有素因数3，5，7，从而 $3\times5\times7\mid l-k$，即 $l\equiv k\pmod{105}$.

通常，我们把 $x\equiv k\pmod{105}$ 叫做同余方程组(※)的解. 在这个意义下，同余方程组(※)仅有一个解.

为了解同余方程组(※)，我们首先建立拉格朗日插值公式.


你能否求一个多项式 $f(x)$，使其满足 $f(1)=1$，$f(-1)=3$，$f(2)=3$?

由二次函数的知识知，在平面上一定存在一条抛物线通过(1，1)，(−1，3)，(2，3)这三个点．因此，我们先假定 $f(x)=ax^2+bx+c$，由题意，得

$$\begin{cases}1=a+b+c,\\3=a-b+c,\\3=4a+2b+c.\end{cases}$$

解得，$a=1$，$b=-1$，$c=1$.

因此多项式 $f(x)=x^2-x+1$ 满足上述条件．利用这个多项式，我们可以写出所有满足条件的多项式

$$f(x)=x^2-x+1+(x-1)(x+1)(x-2)h(x),$$

其中 $h(x)$为任意多项式.

下面介绍一种更为一般的方法——拉格朗日❶插值法．我们按如下步骤进行：

(1) 求多项式 $p(x)$，使 $p(1)=1$，$p(-1)=0$，$p(2)=0$；

(2) 求多项式 $q(x)$，使 $q(1)=0$，$q(-1)=1$，$q(2)=0$；

(3) 求多项式 $r(x)$，使 $r(1)=0$，$r(-1)=0$，$r(2)=1$；

(4) 作多项式 $f(x)=1\times p(x)+3\times q(x)+3\times r(x)$，它就是问题的一个解.

这里的多项式 $p(x)$，$q(x)$与 $r(x)$好求吗？

如选取 $p(x)=c(x+1)(x-2)$，其中 $c$ 为常数．显然 $p(-1)=0$，$p(2)=0$．再代入条件 $p(1)=1$，可求得 $c$ 为$(1+1)(1-2)$的倒数．于是

$$p(x)=\frac{(x+1)(x-2)}{(1+1)(1-2)}=-\frac{1}{2}(x^2-x-2).$$

同理可得

$$q(x)=\frac{(x-1)(x-2)}{(-1-1)(-1-2)}=\frac{1}{6}(x^2-3x+2),$$

$$r(x)=\frac{(x-1)(x+1)}{(2-1)(2+1)}=\frac{1}{3}(x^2-1).$$

一般地，设 $a$，$b$，$c$ 两两不同，那么满足 $f(a)=e$，$f(b)=f$，$f(c)=g$ 的一个多项式 $f(x)$可由下面的公式给出：

$$f(x)=e\cdot p(x)+f\cdot q(x)+g\cdot r(x),\qquad (\text{Ⅰ})$$

其中

$$p(x)=\frac{(x-b)(x-c)}{(a-b)(a-c)},\ q(x)=\frac{(x-a)(x-c)}{(b-a)(b-c)},\ r(x)=\frac{(x-a)(x-b)}{(c-a)(c-b)}.\qquad (\text{Ⅱ})$$

通常，我们把公式(Ⅰ)和(Ⅱ)叫做拉格朗日插值公式．运用类似的方法，同学们可将它推广到一般情形.

为了解同余方程组(※)．我们依照建立拉格朗日插值公式的想法，按如下两个步骤进行：

1° 求整数 $p$，使 $p\equiv1\pmod 3$，$p\equiv0\pmod 5$，$p\equiv0\pmod 7$.

求整数 $q$，使 $q\equiv0\pmod 3$，$q\equiv1\pmod 5$，$q\equiv0\pmod 7$.

求整数 $r$，使 $r\equiv0\pmod 3$，$r\equiv0\pmod 5$，$r\equiv1\pmod 7$.

---

❶ 拉格朗日(Lagrange，J. L；1736—1813)，法国数学家.

2° 作整数 $k=2\times p+3\times q+2\times r$，这个 $k$ 使得(※)中每个同余式都成立.

此时，$x\equiv k(\mathrm{mod}\ 3\times5\times7)$就是同余方程组(※)的解.

如何求出整数 $p$，$q$ 和 $r$ 呢？不妨以求整数 $p$ 为例.

由于 $p\equiv0(\mathrm{mod}\ 5)$，$p\equiv0(\mathrm{mod}\ 7)$，故 $5\mid p$，$7\mid p$，于是 $p=5\times7\times c$，其中 $c$ 为某个整数. 再由 $p\equiv1(\mathrm{mod}\ 3)$知，整数 $c$ 满足：$5\times7\times c\equiv1(\mathrm{mod}\ 3)$. 而 $5\times7\equiv-1(\mathrm{mod}\ 3)$，于是 $-c\equiv1(\mathrm{mod}\ 3)$，进而 $c\equiv-1(\mathrm{mod}\ 3)$. 若选取 $c=2$，则 $p=70$.

用类似的方法，我们计算得 $q=21$，$r=15$. 作整数 $k=2\times70+3\times21+2\times15=233$，于是同余方程组(※)的解为 $x\equiv233\equiv23(\mathrm{mod}\ 105)$.

**思考**

从前面 $p$ 的计算过程可以看出，步骤(1)中整数 $p$，$q$ 和 $r$ 的选取是不惟一的，那么 $p$，$q$ 和 $r$ 的不同选取方式会导致解的不同吗？为什么？你能根据上面的解答来解释程大位的算法口诀吗？

一般地，我们有下面的结论.

**孙子定理** **设 $a$，$b$，$c$ 为两两互素的正整数，$e$，$f$，$g$ 为任意整数，则同余方程组**

$$\begin{cases}x\equiv e(\mathrm{mod}\ a),\\ x\equiv f(\mathrm{mod}\ b),\\ x\equiv g(\mathrm{mod}\ c)\end{cases}$$

**仅有一解：$x\equiv ebcc_1+facc_2+gabc_3(\mathrm{mod}\ abc)$，其中 $c_1$，$c_2$，$c_3$ 分别为满足同余式：$bcc_1\equiv1(\mathrm{mod}\ a)$，$acc_2\equiv1(\mathrm{mod}\ b)$，$abc_3\equiv1(\mathrm{mod}\ c)$的整数.**

运用类似的方法，同学们可将孙子定理推广到更一般的情形.

**习题**

1. 求次数小于 3 的多项式 $f(x)$，使得 $f(-1)=2$，$f(0)=3$，$f(1)=6$.

2. 用孙子定理解同余方程组：

(1) $\begin{cases}x\equiv2(\mathrm{mod}\ 4),\\ x\equiv3(\mathrm{mod}\ 5),\\ x\equiv4(\mathrm{mod}\ 9);\end{cases}$ (2) $\begin{cases}x\equiv2(\mathrm{mod}\ 7),\\ x\equiv3(\mathrm{mod}\ 9),\\ x\equiv7(\mathrm{mod}\ 11).\end{cases}$

3. （韩信点兵问题）有兵 1 队，若排成 5 行，则末行 1 人；若排成 6 行，则末行 5 人；若排成 7 行，则末行 4 人；若排成 11 行，则末行 10 人. 求兵数.

## 六　弃九验算法

**思考**

观察下面的算式：

$$28947\times 34578=1001865676.$$

你能很快确定上面算式的正确性吗？

这里，我们介绍一种用来验算正整数计算结果是否正确的方法——弃九验算法. 弃九验算法是同余性质在算术里的一个应用.

下面仅以正整数的乘法为例说明弃九验算法及其原理.

考虑算式 $p=ab$，其中 $a$，$b$，$p$ 为正整数.

**探究**

设 $a$，$b$，$p$ 的各位数字之和分别为 $\bar{a}$，$\bar{b}$，$\bar{p}$. 由第一讲中能被 3 整除的正整数特征的证明过程，探究一个正整数与它的各位数字之和模 9 同余.

由上面的探究，我们知道

$$a\equiv\bar{a}\pmod 9,\quad b\equiv\bar{b}\pmod 9,\quad p\equiv\bar{p}\pmod 9.$$

从而有

$$\bar{a}\,\bar{b}\equiv\bar{p}\pmod 9.$$

如果上式不成立，那么算式 $p=ab$ 肯定是错的.

现在用弃九验算法判断本段开头给出的算式的正确性，由于

$$28947\equiv 2+8+9+4+7\equiv 3\pmod 9,$$

$$34578\equiv 3+4+5+7+8\equiv 0\pmod 9,$$

$$1001865676\equiv 1+0+0+1+8+6+5+6+7+6\equiv 4\pmod 9,$$

故 $3\times 0=0\not\equiv 4\pmod 9$，因此这个算式是错的.

利用类似的方法，同学们可以验算两个正整数加法、减法等算式的正确性.

弃九验算法的优点是验算比较方便，但是应该特别注意的是弃九验算法只能“检错”，不能“判正”. 也就是说，使用弃九验算法时，得出的结果如果是 $\bar{a}\,\bar{b}\equiv\bar{p}\pmod 9$，也不能判断算式 $p=ab$ 是正确的. 例如，通过直接计算，我们发现算式 $28\ 997\times 39\ 459=1\ 144\ 192\ 533$ 是错误的，但用弃九验算法发现不了这个错误，所以弃九验算法有它的缺点.


用弃九验算法验算下列算式是否正确：

(1) 1524＋3456＝4880；

(2) 2596－2346＝1340；

(3) 4328×3249＝14246432；

(4) 226380÷165＝1432.

# 第三讲　一次不定方程

不定方程是数论中最古老的一个分支. 我国古代对不定方程进行了大量研究，且研究内容极为丰富. 早在公元前 1100 多年，我国古代数学家商高就提出了直角三角形的“勾广三，股修四，径隅五”的著名论断，这实际上给出了方程 $x^2+y^2=z^2$ 的一组正整数解 $x=3$，$y=4$，$z=5$.

大约 1500 年以前，我国古代另一位数学家张丘建在他编写的《张丘建算经》里，提出并解决了下面的数学问题：“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?”这就是人们常说的“百钱买百鸡”问题. 如果用 $x$，$y$，$z$ 分别表示鸡翁、鸡母和鸡雏的个数，那么我们可以得到下面的方程组：

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

这两个问题最后都归结为求解一类方程或方程组的整数解. 由于其未知数个数多于方程的个数，所以我们把这样的方程或方程组叫做不定方程. 由于公元 200 多年，古希腊数学家丢番图（Diophantus）曾讨论了某些不定方程，因而也有人把不定方程叫做丢番图方程.

## 一　二元一次不定方程

二元一次不定方程是最简单的不定方程，它的一般形式为

$$ax+by=c, \tag{1}$$

其中 $a$，$b$，$c$ 为整数，且 $a$，$b$ 不等于零.

显然，这类不定方程不一定有整数解. 例如，$2x+4y=1$ 没有整数解，因为对任意整数 $x$，$y$，$2x+4y$ 恒为偶数，它不可能等于 1.

我们感兴趣的是，不定方程（1）何时有整数解? 有解时是否有无穷多个整数解? 这些整数解是否有统一的表达式? 当然，还有一个问题就是如何求出所有的整数解.

首先看不定方程（1）有解时，整数 $a$，$b$，$c$ 具有什么特征.

观察不定方程 $ax+by=c$ 的形式，自然联想到它与整除、同余之间的联系.

假定不定方程（1）有整数解 $x=x_0$，$y=y_0$. 因为 $(a,b)\mid a$，$(a,b)\mid b$，所以 $(a,b)\mid ax_0+by_0=c$. 也就是说，不定方程（1）有解时，整数 $a$，$b$，$c$ 必须满足：

$(a, b) \mid c$.


整数 $a$，$b$，$c$ 的这种特征能否保证不定方程（1）有整数解呢？

下面我们来检验一下. 设 $d=(a, b) \mid c$，令 $a=a'd$，$b=b'd$，$c=c'd$，则不定方程（1）简化为

$$a'x+b'y=c', \tag{2}$$

其中 $(a', b')=1$. 由最大公约数的性质，存在一对整数 $u$，$v$，使得 $a'u+b'v=1$. 于是 $a'(uc')+b'(vc')=c'$，从而有 $a(c'u)+b(c'v)=c$. 那么 $x=c'u$，$y=c'v$ 就是不定方程（1）的整数解.

综合上述，我们可以得到不定方程（1）有整数解的一个判别准则.

**如果不定方程（1）有整数解，那么 $(a, b) \mid c$. 反过来，当 $(a, b) \mid c$ 时，不定方程（1）一定有整数解.**

从前面的分析可以看出，当不定方程（1）有整数解时，它可以化简为 $x$，$y$ 的系数互素的不定方程（2）. 基于这个事实，对有整数解的不定方程（1），我们不妨假定 $(a, b)=1$.

设 $(a, b)=1$，且 $x=x_0$，$y=y_0$ 为不定方程（1）的整数解. 容易检验，对任意整数 $t$，

$$\begin{cases} x=x_0+bt, \\ y=y_0-at \end{cases} \tag{3}$$

均为不定方程（1）的整数解. 这意味着不定方程（1）有整数解时，必有无穷多个整数解，从而回答了第二个问题.


不定方程（1）的每个解是否都可以用表达式（3）表示呢？

任取不定方程（1）的整数解 $x=x'$，$y=y'$，则有 $ax'+by'=c$. 因为 $ax_0+by_0=c$，所以

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

从而 $b \mid a(x'-x_0)$. 因为 $(a, b)=1$，所以 $b \mid x'-x_0$. 于是存在整数 $t$，使得 $x'-x_0=bt$，即 $x'=x_0+bt$，代入上式得 $y'=y_0-at$. 这表明，不定方程（1）的每个解都可以表示成（3）式的形式. 至此，最后两个问题也得到了回答.

通常，我们把（3）式叫做不定方程（1）的整数通解，而把 $x=x_0$，$y=y_0$ 叫做不定方程（1）的一个特解.

综上所述，我们得到下面的结论.

**设$(a,\ b)=1$，则不定方程$ax+by=c$的整数通解为**

$$\begin{cases}x=x_0+bt,\\ y=y_0-at\end{cases}$$

**其中$t$为任意整数，$x=x_0$，$y=y_0$为不定方程$ax+by=c$的一个特解.**

从上述结论可以看出，要描述二元一次不定方程的所有整数解，只需知道它的一个特解即可.

对某些比较简单的不定方程，如当$a$，$b$的绝对值较小时，我们可以直接通过观察或试验得到它的一个特解.

看下面两个例子.

**例1**　求不定方程$5x+3y=10$的整数通解.

**解**：因为$(5,\ 3)=1$，而$1\mid 10$，所以原不定方程有整数解. 容易观察，$5x+3y=1$有一个特解$x=-1$，$y=2$. 因此，$x=-10$，$y=20$就是原不定方程的一个特解. 由上述结论，原不定方程的整数通解为

$$\begin{cases}x=-10+3t,\\ y=20-5t,\end{cases}$$

其中$t$为任意整数.

**例2**　（百钱买百鸡问题）求下列不定方程的非负整数解：

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

**解**：首先由原不定方程中第一个方程的3倍减去第二个方程，得$7x+4y=100$. 通过观察发现，不定方程$7x+4y=1$有一个特解$x=-1$，$y=2$. 因此$x=-100$，$y=200$是不定方程$7x+4y=100$的一个特解. 所以它的整数通解为

$$\begin{cases}x=-100+4t,\\ y=200-7t,\end{cases}$$

其中$t$为任意的整数.

注意到，$0\leqslant x\leqslant 100$，$0\leqslant y\leqslant 100$，因此有

$$25\leqslant t\leqslant 50,\ 14\frac{2}{7}\leqslant t\leqslant 28\frac{4}{7},$$

即$25\leqslant t\leqslant 28\dfrac{4}{7}$. 从而$t=25$，$26$，$27$，$28$. 再将$x$，$y$的值代入方程$x+y+z=100$，可求得原不定方程有四组非负整数解：

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


1. 求下列不定方程的整数通解：

（1）$5x+4y=11$；　　（2）$25x-13y=7$.

2.（百马问题）一百马，一百瓦，大马驮三，中马驮二，两小马驮一瓦，最后不剩马和瓦．大马、中马、小马各有多少？

## 二　二元一次不定方程的特解

对某些较复杂的二元一次不定方程 $ax+by=c$，其中$(a,b)=1$，我们很难直接观察出它的一个特解．这时候，我们可以通过辗转相除法求它的一个特解．其过程如下：

注意到，当$b=1$时，我们容易观察出不定方程 $ax+by=c$ 的一个特解 $x_0=1$，$y_0=c-a$.

下面假定 $b>1$，并且对 $a$，$b$ 用辗转相除法得

$$\begin{aligned}
a&=bq_1+r_1,\\
b&=r_1q_2+r_2,\\
r_1&=r_2q_3+r_3,\\
r_2&=r_3q_4+r_4,\\
&\cdots\cdots\cdots\cdots\\
r_{n-2}&=r_{n-1}q_n+r_n\ (r_n=1).
\end{aligned}$$

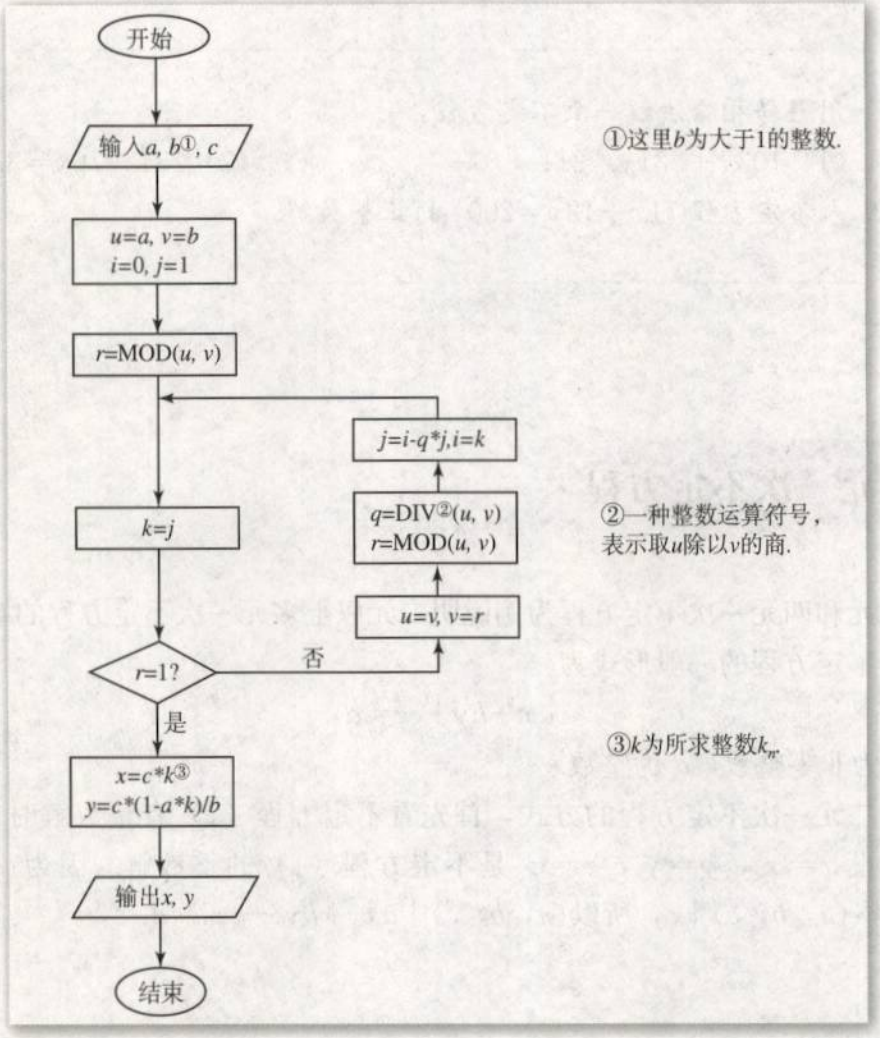
我们规定，$k_0=0$，$k_1=1$，然后由递推关系式 $k_i=k_{i-2}-q_ik_{i-1}$（$i=2$，…，$n$）依次计算出 $k_2$，…，$k_n$．根据大衍求一术的算法原理知，$r_i\equiv ak_i\pmod b$，于是 $b\mid r_i-ak_i$.

特别地，当 $i=n$ 时，$b\mid 1-ak_n$．我们选取

$$\begin{cases}x_0=k_nc,\\ y_0=\dfrac{c(1-ak_n)}{b}.\end{cases}$$

容易检验，$x=x_0$，$y=y_0$ 就是不定方程 $ax+by=c$ 的一个特解.

根据前面的过程，我们可以写出下面算法程序框图：




**例 3**　求不定方程 $13x+74y=2$ 的一个特解.

**解**：因为$(13, 74)=1$，我们对 13，74 用辗转相除法，得

$$13=74\times 0+13,$$
$$74=13\times 5+9,$$
$$13=9\times 1+4,$$
$$9=4\times 2+1,$$

因此 $q_2=5$，$q_3=1$，$q_4=2$. 再由递推关系式依次计算得

$$k_2=(-5)\times 1+0=-5,$$
$$k_3=(-1)\times(-5)+1=6,$$
$$k_4=(-5)+(-2)\times 6=-17.$$

因此

$$\begin{cases} x=(-17)\times 2=-34, \\ y=\dfrac{2(1-13\times(-17))}{74}=6 \end{cases}$$

是不定方程 $13x+74y=2$ 的一个特解.


1. 用辗转相除法解一次不定方程：

（1）$103x+231y=21$；　　（2）$23x-76y=3$.

2. 求不定方程 $71x+12y=2004$ 的正整数解.

## 三　多元一次不定方程

本节以三元和四元一次不定方程为例说明二元以上多元一次不定方程的解法.

三元一次不定方程的一般形式为

$$ax+by+cz=d, \tag{1}$$

其中 $a$，$b$，$c$ 为非零整数，$d$ 为整数.

仿照讨论二元一次不定方程的方式，首先看不定方程（1）有整数解时，$a$，$b$，$c$，$d$ 有什么特征. 设 $x=x_0$，$y=y_0$，$z=z_0$ 是不定方程（1）的整数解. 因为 $(a, b, c) \mid a$，$(a, b, c) \mid b$，$(a, b, c) \mid c$，所以 $(a, b, c) \mid ax_0+by_0+cz_0=d$.


当 $(a, b, c) \mid d$ 时，不定方程（1）是否一定有整数解呢？

我们记 $(a, b)=m$，由于 $(m, c)=(a, b, c) \mid d$，故二元一次不定方程

$$mt+cz=d \tag{2}$$

有整数解，不妨设 $t=t_0$，$z=z_0$. 考虑二元一次不定方程

$$ax+by=mt_0. \tag{3}$$

由于 $(a, b)=m \mid mt_0$，所以不定方程（3）有整数解 $x=x_0$，$y=y_0$. 注意到 $ax_0+by_0+cz_0=mt_0+cz_0=d$，所以 $x=x_0$，$y=y_0$，$z=z_0$ 是不定方程（1）的一组整数解.

综上所述，我们得到不定方程（1）有整数解的一个判断准则.

**不定方程（1）有整数解的充要条件为 $(a, b, c) \mid d$.**

从前面的分析可以看出，当 $(a, b, c) \mid d$ 时，要求不定方程（1）的全部整数解，我们可以先求不定方程（2）的整数通解，得到 $t$ 和 $z$ 的表达式. 然后用 $t$ 的表达式代替不定方程（3）中的 $t_0$，求出它的整数通解，得到 $x$ 和 $y$ 的表达式. 最后，联合 $x$，$y$ 和 $z$ 的表达式就给出了不定方程（1）的全部整数解.

然而，在实际解题时，我们常常将三元的问题转化为二元问题，即先分别解不定方程 $ax+by=mt$ 与 $mt+cz=d$，在解第一个不定方程时，把 $t$ 视为给定的整数，这样得到两个整数通解的表达式. 联立这两个表达式，消去 $t$ 后便得到 $x$，$y$ 和 $z$ 的表达式即为所求.

看一个具体的例子.

**例 4**　求不定方程 $5x-8y+3z=2$ 的全部整数解.

**解**：因为 $(5, -8)=1$，$(5, -8, 3)=(1, 3)=1 \mid 2$，所以不定方程有整数解. 分别解不定方程 $5x-8y=t$ 与 $t+3z=2$，得到它们的整数通解为

$$\begin{cases} x=5t+8k, \\ y=3t+5k; \end{cases} \quad \begin{cases} t=-1-3l, \\ z=1+l, \end{cases}$$

其中 $k$，$l$ 为任意整数. 联立上面的两个通解表示式，消去 $t$，便得到原不定方程的全部整数解

$$\begin{cases} x=-5+8k-15l, \\ y=-3+5k-9l, \\ z=1+l, \end{cases}$$

其中 $k$，$l$ 为任意整数.

**探究**

探究四元一次不定方程

$$ax+by+cz+dw=e, \tag{4}$$

其中 $a$，$b$，$c$，$d$ 为非零整数，$e$ 为整数，有整数解的充要条件为 $(a, b, c, d) \mid e$.

下面介绍不定方程（4）的解法. 同样地，我们可以将其化归为二元一次不定方程的情形.

记 $m=(a, b)$，$n=(m, c)$. 作三个二元一次不定方程

$$ax+by=mu, \quad mu+cz=nv \quad 与 \quad nv+dw=e.$$

先求不定方程 $nv+dw=e$ 的整数通解，得到 $v$ 和 $w$ 的表达式. 然后将 $v$ 代入不定方程 $mu+cz=nv$ 中，求出整数通解，得到 $u$ 和 $z$ 的表达式. 最后，将 $u$ 代入不定方程 $ax+by=mu$ 中，求出整数通解，得到 $x$ 和 $y$ 的表达式. 那么，联合 $x$，$y$，$z$ 和 $w$ 的表达式就给出了不定方程（4）的全部整数解.

在实际解题时，我们常常先分别求不定方程 $ax+by=mu$，$mu+cz=nv$ 与 $nv+dw=e$ 的整数通解，在求每个不定方程时，将等号右边的项视为整数常数，这样得到三个整数通解的表达式. 联立这三个表达式，消去 $u$，$v$ 后得到的 $x$，$y$，$z$ 和 $w$ 的表达式即为所求.

**例 5**　求不定方程 $2x+5y+7z+3w=10$ 的全部整数解.

**解**：因为 $(2, 5)=1$，$(1, 7)=1$，$(2, 5, 7, 3)=(1, 3)=1 \mid 10$，所以不定方程存

在整数解. 作不定方程

$$2x+5y=u,\ u+7z=v,\ v+3w=10,$$

分别求得上面三个二元一次不定方程的整数通解为

$$\begin{cases}x=3u+5t_1,\\ y=-u-2t_1;\end{cases}\quad\begin{cases}u=-6v+7t_2,\\ z=v-t_2;\end{cases}\quad\begin{cases}v=1+3t_3,\\ w=3-t_3,\end{cases}$$

其中 $t_1$，$t_2$，$t_3$ 为任意整数. 联合上述三个通解表达式，消去 $u$，$v$ 得

$$\begin{cases}x=-18-54t_3+21t_2+5t_1,\\ y=6+18t_3-7t_2-2t_1,\\ z=1+3t_3-t_2,\\ w=3-t_3,\end{cases}$$

其中 $t_1$，$t_2$，$t_3$ 为任意整数. 这就是不定方程 $2x+5y+7z+3w=10$ 的全部整数解.


1. 求下列一次不定方程的整数解：

（1）$5x-13y+6z=10$；　　（2）$4x-10y+21z=1$；

（3）$3x+2y+6z-5w=-4$；　　（4）$12x+8y-4z+14w=20$.

2. 试用解一次不定方程的方法解《孙子算经》中“物不知其数”问题.

# 第四讲 数论在密码中的应用

在现实生活中，人们常常需要从一方向另一方传送信息，如照片、一首歌曲、一封信、资料等. 有时由于某种原因，传送和接收双方都不希望传送的信息被第三方截取、篡改或伪造. 为保证信息安全，传送方常采用某种算法对原始信息进行加密，然后对加密后的信息进行传送，接收方收到信息后，再按照某种算法对信息进行去密，从而获知原始信息. 用于信息加密的算法和用于信息去密的算法共同组成了密码算法，也就是密码. 数论在密码中有重要应用.

## 一 信息的加密与去密

原始信息可以有很多种具体形式（如图像、声音和文字等）. 在无线电通信时代，原始信息在传送时通常都转换成数字信息 $x$（如十进制数字或计算机通用的二进制数字）. 信息传送的一个简单模型如图 1 所示：


图 1

即将数字信息 $x$ 直接通过信道传送给接收方.

下面看一个利用上述模型传送英文文字信息的例子.

首先传送和接收双方约定编码规则：将每个英文字母 $a$，$b$，$c$，…，$z$ 分别用十进制数字 01，02，03，…，26 代替，而英文中的空格、逗号、句号、感叹号、问号分别用数字 27 28 29 30 00 代替.

假定要传送信息 Good morning! 给接收方，传送方可以将十进制数字信息 $x$：07 15 15 04 27 13 15 18 14 09 14 07 30 直接通过信道发给接收方，接收方收到上面的数字信息 $x$ 后，根据上面的编码规则就可以识别原始信息.

信息的这种传送方式极不安全，在传送的过程中数字信息 $x$ 很容易被第三方截取、篡改或伪造.

现实生活中许多信息需要保密，如军事和外交机密、商业秘密、个人隐私等. 为此，传送方在发送之前需要将数字信息 $x$ 按某种方式进行变换（这个过程叫做加密），将变换

后的数字信息 $y$ 传送出去，然后合法的接收方收到数字信息 $y$ 后，再进行相反的变换（这个过程叫做去密），恢复成数字信息 $x$，而识别出原始信息.

历史上通过这种方式传送信息的事例并不鲜见. 例如，我国古代就不乏以藏头露尾诗的形式将信息隐藏在整个诗篇中，从而只让某些掌握了规律的人知晓的例子.

如用数学语言表示信息加密传送的机制，就是先对数字信息 $x$ 作一个变换 $E$，将变换后的信息 $y=E(x)$ 发出，接收方收到信息 $y$ 后，进行一个相反的变换 $D$（也就是 $E$ 的逆运算），恢复成数字信息 $x=D(y)$，从而识别原始信息.

信息加密传送的一个简单模型如图 2 所示：


图 2

通常把数字信息 $x$ 叫做明文，加密后得到的数字信息 $y$ 叫做密文，变换 $E$ 和 $D$ 分别叫做加密与去密的密钥. 一般来说，密钥对 $\{E, D\}$ 只能由传送方和接收方约定和保存，不被外人所知. 由于非法接收方不知道密钥，即使截取了密文 $y$，也无法恢复成明文 $x$.

要使外人很难从密文破译出明文，密钥的设计是关键. 密钥的设计方法多种多样，数论在这方面起着重要的作用.

我们简要介绍一下恺撒大帝的加密方法.

假定要把信息 Good morning! 加密传送给接收方，将每个英文字母或符号代表的十进制数作如下变换：

$$E:\ k\to\begin{cases}k+19, & \text{当 } k<12 \text{ 时;}\\ k-12, & \text{当 } k\geqslant 12 \text{ 时.}\end{cases}$$

若采用高斯的同余符号，则加密运算 $E$ 可表示为

$$E(k)=k+19(\mathrm{mod}\ 31)\text{❶},\ k=0,\ 1,\ 2,\ \cdots,\ 30.$$

这样一来，原始信息由明文：07 15 15 04 27 13 15 18 14 09 14 07 30 变成密文：26 03 03 23 15 01 03 06 02 28 02 26 18，其加密过程如表 1 所示：

**表 1**

| | g | o | o | d | 空格 | m | o | r | n | i | n | g | ! | 原始信息 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 07 | 15 | 15 | 04 | 27 | 13 | 15 | 18 | 14 | 09 | 14 | 07 | 30 | 明文 |
| + | 19 | 19 | 19 | 19 | 19 | 19 | 19 | 19 | 19 | 19 | 19 | 19 | 19 | (mod 31) 密钥 |
| | 26 | 03 | 03 | 23 | 15 | 01 | 03 | 06 | 02 | 28 | 02 | 26 | 18 | 密文 |
| | z | c | c | w | o | a | c | f | b | , | b | z | r | 伪装信息 |

传送方将密文 $y$ 通过信道发给接收方. 接收方收到密文 $y$ 之后，对 $y$ 中的每个十进制数（对应着伪装信息的字母或符号）进行相反的变换：

$$D:\ k\to\begin{cases}k-19, & \text{当 } k\geqslant 19 \text{ 时;}\\ k+12, & \text{当 } k<19 \text{ 时}\end{cases}$$

❶ 这个表达式的意义与第二讲中同余式的意义不同，它表示 $E(k)$ 的值等于 $k+19$ 被 31 除后的余数.

便得到明文 $x$，从而识别出原始信息，其去密过程如表 2 所示：

**表 2**

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | z | c | c | w | o | a | c | f | b | , | b | z | r | 伪装信息 |
| | 26 | 03 | 03 | 23 | 15 | 01 | 03 | 06 | 02 | 28 | 02 | 26 | 18 | 密文 |
| + | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | 12 | (mod 31)（密钥） |
| | 07 | 15 | 15 | 04 | 27 | 13 | 15 | 18 | 14 | 09 | 14 | 07 | 30 | 明文 |
| | g | o | o | d | 空格 | m | o | r | n | i | n | g | ! | 原始信息 |

同样地，如用高斯的同余符号，则去密运算 $D$ 可表示为

$$D(k)=k+12(\mathrm{mod}\ 31),\ k=0,\ 1,\ 2,\ \cdots,\ 30.$$

凯撒的加密方法的优点是加密和去密都是模 31 的加法或减法运算，很容易进行．但缺点是密钥个数太少，只有 30 个．第三方一旦知道了加密方法，就可以逐个试验这 30 个密钥，从而将 $y$ 恢复成明文．

另一方面，原始信息中某个字母或符号重复出现时，其对应的数字也重复出现，经加密后都变成同一个数字．那么，第三方在截取足够长的一段密文后，根据英文语言中某些字母出现的频率，用统计学的方法也可以发现加密密钥，进而得到去密密钥．

后来，人们对这种加密方法加以改进．例如，将加密密钥改为 $E(k)=k+i(\mathrm{mod}\ 31)$，其中 $i$ 是周期变化的．这样一来，密钥的个数大大增加了，并且原始信息中同一字母或符号，经加密后对应于不同的数字，从而增加了密钥破译的难度．

## 二　大数分解和公开密钥

随着信息时代的到来，一个人常常要和很多人进行信息传播．如果任意两个人彼此之间传递的信息需要保密的话，那么每个人需要保存大量的密钥对 $\{E,\ D\}$，而且这些密钥还要经常更换，否则容易被非法接收者破译．例如，若有 2 000 个人彼此之间进行信息传递，并且所有信息均需对第三方保密，那么共需要 $C_{2000}^{2}=1\ 999\ 000$ 对密钥，每个人需要保存 1 999 对密钥．这样一来，密钥的保存和保护就成了一个非常严重的问题．

1976 年，美国斯坦福大学年轻数学家狄菲（Diffe）和计算机专家海尔曼（Hellman）提出了一种新的加密方法，叫做公开密钥体制，并且在信息安全领域得到广泛的应用．在这种体制下，信息的加密与去密用两个不同的钥，加密用公钥（意指此钥可以公开，无需保密，任何人都可以得到），去密用私钥（意指此钥需严加管理，只有合法的去密者才有，并不能泄漏）．

在前面信息加密传送的例子中，发送与接收双方公用一对密钥：加密密钥 $E(k)=k+19(\mathrm{mod}\ 31)$和去密密钥 $D(k)=k+12(\mathrm{mod}\ 31)$，它们是一对互逆的运算

$$DE(k)=ED(k)=k.$$

不难发现，加密运算与去密运算都很简单，并且知道其中一个运算后很容易推出另一个运

算. 也就是说，由其中一个密钥可以得到另一个密钥. 与此不同的是，在公开密钥体制中，加密密钥 $E$ 采用所谓的“单向”作用. 具体地说，加密密钥 $E$ 虽然运算简单，并且是可逆的（即存在某个运算 $D$，使得 $DE(k)=ED(k)=k$，对所有 $k$ 都成立），但是即使知道了 $E$，要求它的逆运算 $D$ 也是极困难的，从而保证了第三方无法在保密期限内得到密文的真实信息.

在公开密钥体制下，每个人只需要自己的一对密钥 $\{E, D\}$，其中 $E$ 为单向作用，$D$ 为 $E$ 的逆运算. 每个人的加密密钥 $E$ 对外完全公开，甚至可以编制成册，供任何人查看，但去密密钥 $D$ 只有他自己知道，对其他人保密. 这样一来，每个人只需保存自己的去密密钥 $D$ 即可.

实现公开密钥体制的关键在于设计单向作用 $E$. 公开密钥体制自 1976 年提出后，立即引起人们的极大兴趣. 之后的数年里，人们提出了各种各样设计方案，但绝大多数方案提出不久便被否定了.

1977 年，美国麻省理工学院计算机科学实验室的列维斯特（Rivest）等人基于大数分解的复杂性给出了一个便于应用的设计方案，这就是著名的 RSA 方案. 下面简要介绍一下 RSA 方案.

我们知道，任意大于 1 的整数总可以分解成一些素因数的乘积形式，但这只不过是理论上的结果. 当整数很大时，这件事情具体做起来非常困难. 用现代最快速的分解算法，在大型计算机上分解一个大整数所需时间如表 3 所示：

**表 3**

| 整数的位数 | 必须操作数 | 所需时间 |
|---|---|---|
| 50 | $1.4\times10^{10}$ | 3.9 小时 |
| 75 | $9.0\times10^{12}$ | 104 天 |
| 100 | $2.3\times10^{15}$ | 74 年 |
| 200 | $1.2\times10^{23}$ | $3.8\times10^{9}$ 年 |
| 300 | $1.3\times10^{29}$ | $4.9\times10^{15}$ 年 |
| 500 | $1.3\times10^{39}$ | $4.2\times10^{17}$ 亿年 |

选取两个大约 100 位左右的不同素数 $p$ 和 $q$. 设 $n=pq$，我们不难计算出 $n$ 的欧拉函数值

$$\varphi(n)=(p-1)(q-1).$$

再取两个正整数 $e$ 和 $d$，使得 $ed\equiv1(\mathrm{mod}\ \varphi(n))$.

**一般地，对上述正整数 $e$，$d$ 和任意整数 $x$，恒有 $x^{ed}\equiv x(\mathrm{mod}\ n)$.**

**证明**：由 $ed\equiv1(\mathrm{mod}\ \varphi(n))$ 知 $ed=1+\varphi(n)k$，其中 $k$ 为某个整数. 如果 $p\nmid x$，那么由费马小定理知

$$x^{ed}=x^{1+\varphi(n)k}=x\cdot(x^{p-1})^{(q-1)k}\equiv x(\mathrm{mod}\ p).$$

如果 $p\mid x$，则 $x^{ed}$ 和 $x$ 模 $p$ 均同余于 0，所以对每个整数 $x$，均有 $x^{ed}\equiv x(\mathrm{mod}\ p)$. 类似可证 $x^{ed}\equiv x(\mathrm{mod}\ q)$，因此 $x^{ed}\equiv x(\mathrm{mod}\ n)$.

在 RSA 方案中，把信息 $x$ 用 0 至 $n-1$ 之间的数表示，分别选取加密密钥和去密密

钥为

$$E(x)\equiv x^e \pmod n, \qquad D(y)\equiv y^d \pmod n.$$

由上述事实知 $E$ 和 $D$ 是互逆的运算. 由于 $\varphi(n)=(p-1)(q-1)$是很大的整数，所以可以求出许多对$\{e, d\}$，满足 $ed\equiv 1(\bmod \varphi(n))$. 每个人只需使用其中一对作为自己的密钥对即可.

将 $n$ 和$e$ 公开（从而加密密钥是公开的），每个人保留自己那一个 $d$ 不被别人知道. 别人想通过 $e$ 求出 $d$，就需要解一个一次同余方程 $ex\equiv 1(\bmod \varphi(n))$.

解一次同余方程并不困难，但现在的问题是：别人并不知道模 $\varphi(n)$的大小，因为要得到 $\varphi(n)$的值必须先知道 $N$ 的素因素分解式 $pq$. 通过表 3 大家知道，得到这个分解是极其困难的. 所以别人即使知道 $n$ 和$e$，在信息保密期限内也很难得到 $d$ 和去密密码 $D$.

公开密钥体制的提出不仅解决了大量密钥的保存和管理问题，而且还解决了信息传送中另一个问题：数字签名和身份认证问题.

设想甲发信息给乙向乙借一笔钱，那么乙需要确信这条信息来自甲，以免甲事后否认. 在现实生活中，人们通常在借条上签名或按手印，但在如今广泛采用电子通讯中如何确定对方的身份呢？公开密钥体制提出之前，身份认证问题一直没有很好的解决方法. 如今采用公开密钥体制做身份认证就变得很简单：甲向乙传送信息 $x$ 之前，先用自己的私钥 $D_{甲}$ 作用成 $D_{甲}(x)=y$（数字签名），然后把 $y$ 传送给乙. 乙在公钥本上查到甲的公钥 $E_{甲}$，作用于 $y$ 便恢复成明文

$$x=E_{甲}(y)=E_{甲}\ D_{甲}(x)=x,$$

便知此信息来自甲. 由于其他人不知道甲的私钥 $D_{甲}$，所以无法伪装甲进行签名.

在公开密钥体制下，传送方可以同时对信息进行签名和加密. 例如，如果甲要向乙传送信息 $x$，甲可先签名 $D_{甲}(x)=y$，再进行加密 $E_{乙}(y)=z$，然后把密文 $z$ 传给乙. 当乙收到密文 $z$ 后，依次作用私钥 $D_{乙}$ 和甲的公钥 $E_{甲}$，便得到明文

$$E_{甲}\ D_{乙}(z)=E_{甲}\ D_{乙}\ E_{乙}(y)=E_{甲}(y)=E_{甲}\ D_{甲}(x)=x.$$

其信息传送的数学模型如图 3 所示：

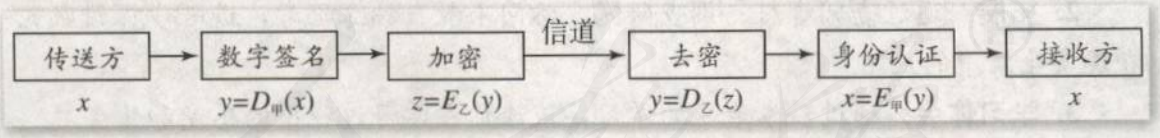



图 3

目前，公开密钥体制已经用于实现愈来愈复杂的信息安全问题.

## 学习总结报告

同学们，前面我们学习了初等数论的一些基本知识.

通过学习，我们发现辗转相除法是初等数论中最重要的方法之一，它由有限次带余除法构成. 辗转相除法将两个较大的正整数的最大公因数的计算问题不断地转化为计算两个较小的正整数的最大公因数，直至容易算出. 它是计算两个整数的最大公因数的一种有效算法. 在求解简单同余方程和一次不定方程时，我们经常要用到辗转相除法.

算术基本定理是初等数论的基石，它告诉我们正整数分解的一个重要性质：每个大于 1 的整数总可以惟一地分解成有限个素数的乘积（不计素数的次序）. 也就是说，素数是正整数最基本的构成“单位”. 利用算术基本定理，我们可以研究整数的许多重要性质. 此外，我们还可以用它来计算最大公因数和最小公倍数.

剩余类的概念及其运算是非常抽象的，它是近世代数学中一个很重要的数学模型. 我们可利用剩余类来证明费马小定理和欧拉定理，关于这一点，同学们可参考一些初等数论方面的书籍. 剩余类的运算与传统的数的运算有许多类似的地方，但也有区别，比如两个不为零的剩余类进行乘法运算可能出现零因子.

数学学习是一个循序渐进的过程，对上面提到的一些概念、方法和定理，需要不断地思考、领悟、反思和总结，才能逐步领会其中蕴含的数学思想方法.

请同学们完成一个学习总结报告. 报告应包括下面三方面的内容：

**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、方程的整数解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，进一步探讨数论在现实生活中的应用.

**3. 学习体会**. 通过对本专题的学习，谈谈你在学习过程中的感受和体会.

# 附录一　剩余系和欧拉函数

在第二讲，同学们已经学习过剩余类及其运算. 为了加深大家对剩余类的认识，我们介绍有关剩余系和欧拉函数的一些知识.

我们知道，按模 $n$ 是否同余对整数集进行分类，可得到模 $n$ 的剩余类：$[0]$，$[1]$，…，$[n-1]$，每个剩余类中的数都是这个剩余类的代表元.

**定义 1**　从模 $n$ 的每个剩余类中各取一个代表元，得到一个由 $n$ 个数组成的集合，叫做模 $n$ 的一个完全剩余系.

例如，$\{0, 1, 2, 3, 4, 5\}$，$\{6, 7, -4, 15, 10, 17\}$是模 6 的完全剩余系.

由定义，模 $n$ 的完全剩余系有无穷多个. 并且，对任意 $n$ 个整数，如果它们模 $n$ 两两不同余，那么这 $n$ 个数组成的集合就是模 $n$ 的一个完全剩余系.

如果模 $n$ 的某个剩余类中的数都与 $n$ 互素，那么称这个剩余类为模 $n$ 的互素剩余类.

注意到，模 $n$ 的一个剩余类中任意两个数模 $n$ 同余，如果其中有一个数与 $n$ 互素，那么这个剩余类中的其余数均与 $n$ 互素. 所以要判断一个剩余类是否为与模 $n$ 的互素剩余类，只需选取一个代表元，考察它与 $n$ 是否互素即可.

为了表示模 $n$ 的互素剩余类的个数，我们引入欧拉函数的概念.

**定义 2**　用 $\varphi(n)$表示 1，2，…，$n$ 中与 $n$ 互素的整数的个数，称 $\varphi(n)$为欧拉函数.

例如，$\varphi(3)=2$，$\varphi(5)=4$. 一般地，对任意素数 $p$，$\varphi(p)=p-1$.

由定义，模 $n$ 的互素剩余类一共有 $\varphi(n)$个.

**定义 3**　从模 $n$ 的每个互素剩余类中各取一个代表元，得到一个由 $\varphi(n)$个数组成的集合，叫做模 $n$ 的一个简化剩余系.

例如，$\{1, 5\}$，$\{7, 17\}$是模 6 的简化剩余系.

同样，模 $n$ 的简化剩余系有无穷多个. 并且，对任意 $\varphi(n)$个整数，如果它们模 $n$ 两两不同余且都和 $n$ 互素，那么这 $\varphi(n)$个数组成的集合就是模 $n$ 的一个简化剩余系.

关于模 $n$ 的完全剩余系和简化剩余系，我们有如下基本结论：

**定理 1**　设 $n$ 为正整数，$a$，$b$ 为整数且$(a, n)=1$. 若$\{a_1, a_2, \cdots, a_n\}$是模 $n$ 的一个完全剩余系，则$\{aa_1+b, aa_2+b, \cdots, aa_n+b\}$也是模 $n$ 的一个完全剩余系.

证明：只需证明 $aa_1+b$，$aa_2+b$，…，$aa_n+b$ 模 $n$ 两两不同余即可. 用反证法，设存在 $i$，$j(i\neq j)$，使得 $aa_i+b\equiv aa_j+b(\mathrm{mod}\ n)$，则 $aa_i\equiv aa_j(\mathrm{mod}\ n)$. 因为$(a, n)=1$，所以 $a_i\equiv a_j(\mathrm{mod}\ n\}$，这与$\{a_1, a_2, \cdots, a_n\}$是模 $n$ 的一个完全剩余系矛盾. 因此 $aa_1+b$，$aa_2+b$，…，$aa_n+b$ 模 $n$ 两两不同余.

**定理 2**　设 $n$ 为正整数，$a$ 为整数且$(a, n)=1$. 若$\{a_1, a_2, \cdots, a_{\varphi(n)}\}$为模 $n$ 的一个

简化剩余系，则$\{aa_1, aa_2, \cdots, aa_{\varphi(n)}\}$也是模 $n$ 的一个简化剩余系.

证明：由定理 1 知，$aa_1, aa_2, \cdots, aa_{\varphi(n)}$模 $n$ 两两不同余. 下面证明 $aa_1, aa_2, \cdots, aa_{\varphi(n)}$都与 $n$ 互素. 因为$(a, n)=1$，所以存在整数 $u$，$v$，使得 $au+nv=1$. 又因为$(a_i, n)=1$，所以存在整数 $s$，$t$，使得 $a_is+nt=1$. 于是

$$(au+nv)(a_is+nt)=aa_i(us)+n(aut+a_isv+nvt)=1,$$

这表明 $aa_i$ 和 $n$ 的公因数一定是 1 的因数，于是$(aa_i, n)=1$. 因此$\{aa_1, aa_2, \cdots, aa_{\varphi(n)}\}$是模 $n$ 的一个简化剩余系.

由定理 2 的证明过程，我们立即得到最大公因数的一个重要性质：

> 若$(a, n)=1$，$(b, n)=1$，则$(ab, n)=1$.

这个性质在后面定理的证明中还会用到.

**定理 3**　设 $m$，$n$ 为正整数且$(m, n)=1$. 若$\{a_1, a_2, \cdots, a_m\}$为模 $m$ 的一个完全剩余系，$\{b_1, b_2, \cdots, b_n\}$为模 $n$ 的一个完全剩余系，则所有整数 $na_i+mb_j$ 组成的集合为模 $mn$ 的一个完全剩余系.

证明：形如 $na_i+mb_j$ 的整数一共有 $mn$ 个，故只需证明这些整数模 $mn$ 两两不同余即可. 若 $na_i+mb_j\equiv na_k+mb_l \pmod{mn}$，则 $mn \mid n(a_i-a_k)+m(b_k-b_l)$. 由于 $m \mid mn$，故 $m \mid n(a_i-a_k)+m(b_k-b_l)$，又由于 $m \mid m(b_k-b_l)$，故 $m \mid n(a_i-a_k)$. 因为$(m, n)=1$，所以 $m \mid a_i-a_k$，即 $a_i\equiv a_k \pmod m$，从而 $j=k$. 类似可证：$j=l$. 因此所有形如 $na_i+mb_j$ 的整数模 $mn$ 两两不同余.

**定理 4**　设 $m$，$n$ 为正整数且$(m, n)=1$. 若$\{a_1, a_2, \cdots, a_{\varphi(m)}\}$为模 $m$ 的一个简化剩余系，$\{b_1, b_2, \cdots, b_{\varphi(n)}\}$为模 $n$ 的一个简化剩余系，则所有整数 $na_i+mb_j$ 组成的集合为模 $mn$ 的一个简化剩余系.

证明：形如 $na_i+mb_j$ 的整数一共有 $\varphi(m)\varphi(n)$个，由定理 3 知，这些整数模 $mn$ 两两不同余. 因为$(m, n)=1$，$(m, a_i)=1$，所以$(m, na_i)=1$，于是$(m, na_i+mb_j)=1$. 类似可证：$(n, na_i+mb_j)=1$. 因此$(mn, na_i+mb_j)=1$. 这表明，形如 $na_i+mb_j$ 的整数都与 $mn$ 互素.

余下只需证明：对任意整数 $a$，若$(a, mn)=1$，则 $a\equiv na_i+mb_j \pmod{mn}$.

由定理 3 知，存在整数 $x$，$y$，使得 $a\equiv nx+my \pmod{mn}$，即 $mn \mid a-(nx+my)$. 设$(m, x)=d$，则 $d \mid m$，$d \mid x$，从而 $d \mid nx+my$. 而 $d \mid mn$，故 $d \mid a-(nx+my)$. 于是 $d \mid a$. 所以 $d$ 为 $a$ 和 $mn$ 的公因数. 又因为$(a, mn)=1$，所以 $d=1$，即$(m, x)=1$. 这表明 $x\equiv a_i \pmod m$，即 $m \mid x-a_i$，于是 $mn \mid nx-na_i$. 类似可证：$mn \mid my-mb_j$. 因此 $mn \mid (nx+my)-(na_i+mb_j)$，即 $nx+my\equiv na_i+mb_j \pmod{mn}$. 所以 $a\equiv na_i+mb_j \pmod{mn}$.

由定理 4，我们立即得到下面的关系式：

> 若 $m$，$n$ 为正整数，且$(m, n)=1$，则 $\varphi(mn)=\varphi(m)\varphi(n)$.

利用上面的关系式，我们可以推出欧拉函数 $\varphi(n)$的表达式.

**定理 5** 设 $n$ 为大于 1 的整数，则 $\varphi(n)$ 有下面的表达式：

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

其中 $p_1$，$p_2$，…，$p_k$ 为 $n$ 的所有互异的素因数.

证明：不妨设 $n$ 的素因数分解式为 $n=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$. 由前面的关系式得

$$\varphi(n)=\varphi(p_1^{t_1})\varphi(p_2^{t_2})\cdots\varphi(p_k^{t_k}).$$

以下证明：对任意正整数 $t$ 和素数 $p$，总有 $\varphi(p^t)=p^t-p^{t-1}$.

因为 $p$ 是素数，所以不与 $p^t$ 互素的整数都是 $p$ 的倍数. 1 至 $p^t$ 的整数中 $p$ 的倍数为 $p$，$2p$，$3p$，…，$p^{t-1}p$，共有 $p^{t-1}$ 个，从而 1 至 $p^t$ 中共有 $p^t-p^{t-1}$ 个整数与 $p^t$ 互素. 因此 $\varphi(p^t)=p^t-p^{t-1}$.

这样一来，我们有

$$\begin{aligned}\varphi(n)&=(p_1^{t_1}-p_1^{t_1-1})(p_2^{t_2}-p_2^{t_2-1})\cdots(p_k^{t_k}-p_k^{t_k-1})\\&=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\&=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

例如，计算 $\varphi(12\,000)$，由素因数分解式：$12\,000=2^5\times3\times5^3$，我们得

$$\varphi(12\,000)=12\,000\times\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)=3\,200.$$

# 附录二　多项式的整除性

在初中，同学们已经学习过单项式和多项式. 今后，我们把单项式看作是多项式的特殊情形. 只含一个字母的多项式叫做一元多项式. 例如，$x^6-1$，$2x^3-x^2+x-1$，$-2$，$x+1$ 等都是一元多项式. 这里，我们仅讨论系数为有理数的一元多项式.

一元多项式常用符号 $f(x)$，$g(x)$，$h(x)$，…表示. 在一元多项式中可以随意添加或去掉一些系数为零的项，并且如果某项系数为 1，那么这个系数可省略不写.

单独一个数字 0 叫做零多项式. 一个非零多项式中项的最高次数叫做这个多项式的次数，并且规定，零多项式没有次数.

多项式的加、减、乘三种运算与同学们在初中学习过的运算是一样的. 多项式的除法运算与整数的除法运算类似，可借助竖式除法来实现.

例如，计算 $(x^4-2x^3+x-2)\div(x^2-x+1)$，类似于整数的竖式除法，我们有

$$
\begin{array}{r}
x^2-x-2 \\
x^2-x+1\overline{)\,x^4-2x^3\quad+x-2} \\
\underline{x^4-x^3+x^2\quad\;\;} \\
-x^3-x^2+x \\
\underline{-x^3+x^2-x\;\;} \\
-2x^2+2x-2 \\
\underline{-2x^2+2x-2} \\
0
\end{array}
$$

因此 $(x^4-2x^3+x-2)\div(x^2-x+1)=x^2-x+2$.

但是，除法在多项式中也不是永远可以实施的. 也就是说，一个多项式不一定能除尽另一个多项式. 例如，$x^2+1$ 就不能被 $x-1$ 除尽，因为

$$
\begin{array}{r}
x+1 \\
x-1\overline{)\,x^2\quad+1} \\
\underline{x^2-x\;\;} \\
x+1 \\
\underline{x-1\;\;} \\
2
\end{array}
$$

因此有必要研究一个多项式何时能被另一个非零多项式除尽，也就是多项式的整除性问题. 首先，我们看看多项式整除的概念.

**定义 1**　设 $f(x)$，$g(x)$ 是两个多项式，且 $f(x)\neq 0$. 如果存在多项式 $h(x)$，使得 $g(x)=f(x)h(x)$，我们就说 $f(x)$ 整除 $g(x)$，并说 $f(x)$ 是 $g(x)$ 的一个因式.

我们用符号 $f(x)\mid g(x)$ 表示 $f(x)$ 整除 $g(x)$，用符号 $f(x)\nmid g(x)$ 表示 $f(x)$ 不能整除

$g(x)$. 由上面定义，我们可以推出多项式整除有下列基本性质：

(1) 若 $f(x) \mid g(x)$，$g(x) \mid h(x)$，则 $f(x) \mid h(x)$.

(2) 若 $h(x) \mid f(x)$，$h(x) \mid g(x)$，则 $h(x) \mid f(x) \pm g(x)$.

(3) 若 $f(x) \mid g(x)$，则对任意多项式 $h(x)$，$f(x) \mid g(x)h(x)$.

(4) 若 $f(x) \mid g(x)$，$g(x) \mid f(x)$，则 $f(x)=cg(x)$，这里 $c$ 是一个不等于零的数.

在整数的整除性理论中，带余除法有着重要、基本的作用. 对于多项式来说，带余除法同样是多项式整除性理论的基础.

**带余除法** 设 $f(x)$和 $g(x)$是任意两个多项式，且 $f(x) \neq 0$，那么存在且仅存在一对多项式 $q(x)$和 $r(x)$，使得

$$g(x)=f(x)q(x)+r(x), \tag{1}$$

其中 $r(x)=0$，或者 $r(x)$的次数小于 $f(x)$的次数.

我们把 (1) 式中的多项式 $q(x)$和 $r(x)$分别叫做 $f(x)$除 $g(x)$的商式和余式.

和整数的情形一样，我们还可以讨论两个多项式的最大公因式.

**定义 2** 设 $f(x)$和 $g(x)$是不全为零的两个多项式. 如果多项式 $h(x)$同时为$f(x)$和$g(x)$的因式，那么 $h(x)$叫做 $f(x)$和 $g(x)$的一个公因式，其中次数最高的公因式叫做 $f(x)$与$g(x)$的最大公因式.

需要指出的是，两个多项式的最大公因式有无穷多个. 但可以证明，这些最大公因式之间只有一个非零常数因子的差别. 我们用符号$(f(x), g(x))$表示 $f(x)$与 $g(x)$的最高次项系数为 1 的最大公因式. 如果$(f(x), g(x))=1$，我们就说 $f(x)$与 $g(x)$是互素的.

如何计算两个多项式的最大公因式呢? 在这里，我们有与整数的情形类似的辗转相除法.

**辗转相除法** 设 $f(x)$和 $g(x)$为任意两个多项式，且 $f(x) \neq 0$. 应用带余除法，以 $f(x)$除 $g(x)$，得商式 $q_1(x)$和余式 $r_1(x)$. 如果 $r_1(x) \neq 0$，那么再以 $r_1(x)$除 $f(x)$，得商式 $q_2(x)$和余式 $r_2(x)$；如果 $r_2(x) \neq 0$，再以 $r_2(x)$除 $r_1(x)$，如此继续下去，有限次这种除法后，必然得到一个余式 $r_n(x) \neq 0$，它整除前一个余式 $r_{n-1}(x)$. 这样一来，我们得到一串等式：

$$\begin{aligned}
&g(x)=f(x)q_1(x)+r_1(x),\\
&f(x)=r_1(x)q_2(x)+r_2(x),\\
&r_1(x)=r_2(x)q_3(x)+r_3(x),\\
&\cdots\cdots\\
&r_{n-2}(x)=r_{n-1}(x)q_n(x)+r_n(x),\\
&r_{n-1}(x)=r_n(x)q_{n+1}(x).
\end{aligned} \tag{2}$$

我们说，(2) 式中的多项式 $r_n(x)$就是 $f(x)$和 $g(x)$的一个最大公因式.

与两个整数的最大公因数类似，最大公因式有下面的性质：

**定理 1** 设 $f(x)$和 $g(x)$是不全为零的两个多项式，那么存在多项式 $u(x)$和 $v(x)$，使以下等式成立

$$f(x)u(x)+g(x)v(x)=(f(x), g(x)).$$

从这个定理我们可以立即推出多项式的一个重要事实：

**定理 2** 如果 $f(x) \mid g(x)h(x)$，且 $f(x)$与$h(x)$互素，那么 $f(x) \mid g(x)$.

如果多项式 $f(x)$是$g(x)$的一个因式，我们就说 $g(x)$是 $f(x)$的一个倍式. 同学们可类似于整数的情形，给出两个多项式的最小公倍式的概念，并推导最小公倍式的相关性质.

在整数集中，如果一个大于 1 的正整数不能分解成两个比它小的正整数的乘积，那么这个正整数一定是素数. 反过来也成立. 在多项式中，有一类次数大于零的多项式，它们不能分解成两个次数比它低的两个多项式的乘积，如 $x^2+2$，$x+1$ 等. 我们把这样的多项式叫做不可约多项式.

不可约多项式在多项式的整除性理论中的作用相当于素数在整数的整除性理论中的作用.

对应于整数中的算术基本定理，在多项式中有下面的结论：

**定理 3** 任何一个次数大于零的多项式 $f(x)$总可以分解成若干个不可约多项式的乘积：

$$f(x)=p_1(x)p_2(x)\cdots p_k(x), \tag{3}$$

若不计（3）式中 $p_i(x)$的次序和非零常数因子的差别，这种分解式是惟一的.

例如，$x^3+x^2-2x-2=(x+1)(x^2-2)$.

如果在（3）式中限定每个不可约多项式 $p_i(x)$的最高次项系数为 1，并且将相同的不可约多项式的乘积写成幂的形式，那么（3）式可以改写成下面的形状：

$$f(x)=cq_1(x)^{n_1}q_2(x)^{n_2}\cdots q_t(x)^{n_t}, \tag{4}$$

其中 $c$ 为非零常数，$q_i(x)$（$1\leqslant i\leqslant t$）为互不相同的不可约多项式，$n_i$（$1\leqslant i\leqslant t$）为正整数.

我们把（4）式叫做多项式 $f(x)$的典型分解式，对应于整数中的素因数分解式. 利用典型分解式，我们可以求两个多项式的最大公因式和最小公倍式.

# 后　记

为了全面贯彻党的教育方针，适应时代发展的需要，为学生的终身发展奠定基础，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．

我们聘请北京师范大学刘绍学教授为主编，与高中数学课程标准研制组的部分成员、大学数学教师、数学教育理论工作者、中学数学教研员和数学教师共同组成编写委员会，根据教育部制订的《普通高中数学课程标准（实验）》，编写了这套数学实验教科书．这里特别要感谢北京师范大学数学科学学院领导对本套教科书编写工作的高度重视和大力支持，同时还要感谢所有对本套教科书提出修改意见，提供过帮助与支持的专家、学者和教师，以及社会各界朋友．

本册教科书是编委会全体成员集体智慧的成果．除已列出的主要编写者外，参加本册教科书讨论的还有：张劲松、谷丹等．

我们还要感谢使用本套教材的实验区的师生们．希望你们在使用本套教材的过程中，能够及时把意见和建议反馈给我们，对此，我们将深表谢意．让我们携起手来，共同完成教材建设工作．我们的联系方式如下：

电话：(010)58758321

E-mail：jcfk@pep.com.cn　zhangjs@pep.com.cn

人民教育出版社　课程教材研究所

中学数学课程教材研究开发中心