高等学校教材

整数与多项式

冯克勤　余红兵　编著

CHEP
高等教育出版社

Springer
施普林格出版社

(京) 112 号

图书在版编目(CIP)数据

整数与多项式 / 冯克勤，余红兵　编著．— 北京：高等教育出版社；海德堡：施普林格出版社，1999

ISBN 7-04-007890-2

Ⅰ．整…　Ⅱ．① 冯… ② 余…　Ⅲ．① 整数 ② 多项式　Ⅳ．0121.1

中国版本图书馆 CIP 数据核字(1999)第 41499 号

书　　名　整数与多项式

作　　者　冯克勤　余红兵

出版发行　高等教育出版社　施普林格出版社

社　　址　北京市东城区沙滩后街 55 号　**邮政编码**　100009

电　　话　010－64054588　**传　　真**　010－64014048

网　　址　http://www.hep.edu.cn

经　　销　新华书店北京发行所

印　　刷　北京民族印刷厂

开　　本　880×1230　1/32　**版　　次**　1999 年 10 月第 1 版

印　　张　6.5　**印　　次**　1999 年 10 月第 1 次印刷

字　　数　190 000　**定　　价**　15.00 元

序

整数(论),也称为初等数论,主要研究整数性质和方程(组)的整数解;多项式,则是代数学中一个非常基本的研究对象.

整数和多项式,初看起来,彼此并不相同,但两者有许多共同的,以及可以类比的内容.特别地,整数和多项式中许多概念、结果和方法,是近世代数中抽象概念的非常基本的模型和源泉.此外,由于计算机科学和数字通信技术的飞速进步,包括数论和代数学在内的广义离散数学得到了广泛和深入的应用.无论培养数学研究人材,还是培养数学应用人材,大学的数论和代数教学都应当有所加强.

中国科学技术大学从 1977 年起为数学系一年级学生开设了初等数论必修基础课.本书是在二十余年教学经验基础上,由原讲义改写而成.编写本书主要有两个目的:一个是较为系统地讲授整数和多项式理论的基本知识;另一个是为学习近世代数(群、环、域)提供具体的素材和实例,所以书中比较注重培养学生的代数学观点,表现整数理论与多项式理论的联系和相似之处.根据教学实践,我们相信,这样作对于培养学生抽象思考能力和代数学的思想方法,都是有好处的.

本书的主体为两个部分.第一部分的五章(共十四节)讲述整数的基础知识;第二部分的四章(共十二节)讲述多项式;另有一章作为附录,简要介绍本书内容在数字通信的信息安全方面的一些应用.根据以往的经验,作为一学期每周三(或四)学时的教材内容,可删去第 14 节,第 18 节和第 23 节不讲.

本书中每一节都配有少量的习题,其中较为基本的则标有“*”号.书末给出了部分习题的提示和注释,供读者参考.

作者感谢中国科学技术大学数学系的程艺教授、李尚志教授对编写本书的支持和鼓励；感谢单墫教授、李克正教授对本书写作提出的建议；感谢高等教育出版社徐可先生对本书出版的大力帮助；最后，我们感谢余华敏小姐耐心地打印了本书的初稿.

作　者

一九九九年五月

目　　录

第二部分 多 项 式

引　言

1. 正整数与整数. 正整数，也叫作自然数，就是我们熟知的

$$1，2，3，\cdots.$$

正整数的集合记作 **N**. 正整数的形成源于经验，其公理化定义是由皮亚诺(Peano) 作出的，这里不作讨论. 我们只提及(没有证明) 正整数的一些基本性质.

正整数中可以作**加法运算**：对任意 a，$b \in \mathbf{N}$，有唯一确定的正整数，称为 a 与 b 的和，记作 $a+b$，具有下面的运算规律

(1) 加法结合律　$(a+b)+c=a+(b+c)$；

(2) 加法交换律　$a+b=b+a$.

正整数中还可作**乘法运算**：对任意 a，$b \in \mathbf{N}$，有唯一确定的正整数，称为 a 与 b 的积，记作 $a \cdot b$(或 ab)，具有下面的运算规律

(3) 乘法结合律　$(ab) \cdot c=a \cdot (bc)$；

(4) 乘法交换律　$ab=ba$；

(5) $1 \cdot a=a \cdot 1=a$；

(6) 分配律　$a(b+c)=ab+ac$.

正整数中有**大小**(即顺序) 关系. 如果 $a=b+c(c \in \mathbf{N})$，则记作 $a>b$ 或 $b<a$. 可以证明，对任意两个数 a，b，三个关系

(7) $a<b$，　$a=b$，　$a>b$

中，有且仅有一个成立；并且

(8) 由 $a<b, b<c$ 推出 $a<c$；

(9) 由 $a<b$ 推出 $a+c<b+c$；

(10) 由 $a<b$ 推出 $ac<bc$.

正整数的最重要，最本质的性质是下面的

归纳公理　设 $S \subseteq \mathbf{N}$，满足条件(i) $1 \in S$；(ii) 如果 $n \in S$，则 $n+1 \in S$. 那么 $S=\mathbf{N}$.

归纳公理是我们常用的数学归纳法的基础.

定理 1　设 $P(n)$ 是关于正整数的一个命题. 如果

(i) 当 $n=1$ 时，$P(1)$ 成立；

(ii) 由 $P(n)$ 成立可推出 $P(n+1)$ 成立.

则 $P(n)$ 对所有正整数 n 都成立.

由归纳公理还可推出正整数的下面两个非常基本的性质：

定理 2(最小数原理)　设 T 是 $\mathbf{N}$ 的一个非空子集. 则必有 $t_0 \in T$，使得对任意 $t \in T$ 有 $t_0 \leqslant t$，即 t_0 是 T 中的最小正整数.

定理 3(最大数原理)　设 T 是 $\mathbf{N}$ 的一个非空子集. 若 T 有上界，即存在正整数 m，使得对任意 $t \in T$ 有 $t \leqslant m$. 那么，必有 $t_0 \in T$，使得对任意 $t \in T$ 有 $t \leqslant t_0$，即 t_0 是 T 中的最大正整数.

用最小数原理可以证明下面的第二数学归纳法.

定理 4　设 $P(n)$ 是关于正整数 n 的一个命题. 如果

(i) 当 $n=1$ 时，$P(1)$ 成立；

(ii) 设 $n>1$，由 $P(k)$ 对所有正整数 $k<n$ 成立，可推出 $P(n)$ 成立.

则 $P(n)$ 对所有正整数 n 成立.

通过引入记号 0(零) 及 $-a$ 可将正整数扩充为整数. 整数的集合记作 **Z**.

Z 上可定义加法与乘法. 对于加法，它适合运算规律(1)，(2)；并且，数 0 满足 $0+a=a+0=a$；以及，对每个 $a\in\mathbf{Z}$ 有唯一的 $x\in\mathbf{Z}$，使 $a+x=0$，将 x 记作 $-a$. 于是，对任意 $a,b\in\mathbf{Z}$，方程 $a+x=b$ 在 **Z** 中有唯一的解，这个解记作 $b-a$，即 **Z** 中可以作加法的逆运算——减法. 在代数学中，我们将可作加、减运算，并且适合上述运算规律的集合称为**加法群**. 因此，**Z** 是一个加法群.

Z 中的乘法适合运算规律(3)，(4)，(5)，(6). 我们将既能作加、减运算，还能作上述乘法运算的集合，称为(**交换**) **环**. 注意，对于乘法，$0\cdot a=0$；并且 $ab=0$ 当且仅当 $a=0$ 或者 $b=0$. 具有这种性质的环，称作**无零因子环**. 因此 **Z** 是一个无零因子环，从而其中(乘法) 消去律成立.(我们在第二章中将遇到与此不同的环.)

整数中也有**大小**(顺序) 的概念，它适合规律(7)，(8)，(9) 以及(10) 当 $c>0$.

整数中还引入了**绝对值**的概念：

$$|a|=\begin{cases}a, & a\in\mathbf{N},\\ 0, & a=0,\\ -a, & -a\in\mathbf{N}.\end{cases}$$

因此，$|a|$ 总是一个非负整数. 绝对值有下面的性质：

(11) $|ab|=|a||b|$，

(12)(三角不等式) $|a+b|\leqslant|a|+|b|$.

现在我们简短地提一下有理数、实数和复数的代数结构.

有理数的集合记作 **Q**，它是所有分数 $\frac{a}{b}$ 之集，其中 $a,b\in\mathbf{Z}$ 且 $b\neq 0$. 两个有理数 $\frac{a}{b}$ 与 $\frac{c}{d}$ 相等，等价于说 $ad=bc$. 由 $a=\frac{a}{1}$，可将整数 **Z** 看作 **Q** 的子集. 易于知道，对每个 $a\in\mathbf{Z}$，$a\neq 0$，a 在 **Q** 中均有唯一的(乘法)“逆”，即存在唯一的 $r\in\mathbf{Q}$，使 $ra=1$；并且 **Q** 是包含 **Z** 且具有这一性质的最小集合.

实数的集合记作 **R**. 通常我们将 **R** 看作所有十进小数的集合，因而 **Q** 是 **R** 的子集. 定义实数的一种方式是将其作为有理数的柯西(Cauchy)序列的极限，我们对此不作讨论. 然而，没有精确定义仍然可以使用实数，本书将像我们在初等数学中做过的那样对待实数.(历史上，实数也的确是在使用了几百年后，才给出了精确的定义.)

复数的集合记作 **C**，它们由所有形如 $a+bi$ 的数构成，这里 $a,b\in\mathbf{R}$，而 $\mathrm{i}=\sqrt{-1}$. 复数的实部、虚部、共轭、模、三角形式，以及几何意义等，都已在中学里学习过，这里不再讨论，我们只提及一个基本的等式(称为**欧拉**(Euler)**公式**)：

$$r(\cos\theta+\mathrm{i}\sin\theta)=r\mathrm{e}^{\mathrm{i}\theta},$$

其中 r,θ 分别是复数的模及幅角，而 e 是自然对数的底.

与 **Z** 类似，**Q**，**R**，**C** 中可作加、减法与乘法，并且具有 **Z** 中相同的运算规律. 于是，**Q**，**R**，**C** 都是环.

但从代数观点看，**Q**，**R**，**C** 与 **Z** 有很大的不同. 在 **Z** 中，方程 $ax=1$ 仅在 $a=1$ 或 -1 时可解；但在 **Q**，**R** 或 **C** 中，每一个非零元均有(乘法)“逆”，即可以作除法运算. 用代数的语言，能作加，减，乘，除(分母不为零)四则运算(并且满足通常运算规律)的集合，称为**域**. 于是，**Q**，**R**，**C** 都是域，但 **Z** 不是域. 此外，**Q** 中每个元都是 **Z** 中两个元素之商，我们因此将 **Q** 称为 **Z** 的商域；又 $\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}$，我们说 **R** 是 **Q** 的扩域，**C** 是 **R** 的扩域.

2. **多项式**. 我们用 D 代表 **Z**，**Q**，**R** 或 **C**. 设 n 是非负整数，表达式

(13)　$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

其中 $a_0, a_1, \cdots, a_n$ 属于 D，称为**系数在 D 中的一元多项式**，也可称为 D 上的一元多项式. 所有形如(13) 的多项式的集合，记作 $D[x]$.

在微积分中，我们常将(13) 称为多项式函数，即 x 视为 D 中的变量. 但在代数学中，我们将采用不同的观点，(13) 中的 x 称为**不定元** —— 并非是 D 中不确定的元素，而仅是一个不属于 D 的形式符号，我们约定 x 与 D 中元素的(形式) 运算适合 D 中元素的运算规律. 我们常用 $f(x), g(x), \cdots$ 或 $f, g, \cdots$ 等来代表多项式.

在多项式(13) 中，a_ix^i 称为 **i 次项**，a_i 称为 i 次项的**系数**. 两个多项式 $f(x)$ 和 $g(x)$ **相等**(或恒等)，记作 $f(x) = g(x)$，是指 $f(x)$ 与 $g(x)$ 中同次项的系数相等. 系数全为零的多项式称为**零多项式**，简称零，记为 0.

在(13) 中，如果 $a_n \neq 0$，则称 a_nx^n 为多项式(13) 的**首项**，a_n 为**首项系数**，n 为多项式(13) 的**次数**，记作 $n = \deg f(x)$，这通常简记为 $n = \deg f$.（多项式的次数与不定元的选取无关.）请注意，零次多项式即为 D 中非零元素，而零多项式是唯一不定义次数的多项式.

$D[x]$ 中的多项式可作加、减、乘法运算. 设

(14)　$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

(15)　$$g(x) = b_mx^m + b_{m-1}x^{m-1} + \cdots + b_0,$$

是 $D[x]$ 中两个多项式. 在表示 $f(x)$ 与 $g(x)$ 的和时，如 $n \geqslant m$，为了方便起见，我们令 $b_n = \cdots = b_{m+1} = 0$. 定义

$$f(x) + g(x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \cdots + (a_0 + b_0).$$

易于验证，多项式的加法满足结合律与交换律(因为这些均归结为系数 a_i, b_i 的加法). 零多项式在 $D[x]$ 中加法的作用相当于数 0 在 D 中加法的作用：$0 + f(x) = f(x)$. 此外，对任意 $f(x)$，我们将其每一项的系数改变符号得到的多项式，记作 $-f(x)$，则 $f(x) + (-f(x)) = 0$. 定义

$f(x)-g(x)=f(x)+(-g(x))$，于是 $D[x]$ 中可作减法运算.

$D[x]$ 中还可以作乘法. 设 $f(x),g(x)$ 如(14),(15)式，定义 $f(x)$ 与 $g(x)$ 的积为

$$f(x)\cdot g(x)=a_nb_mx^{n+m}+(a_nb_{m-1}+a_{n-1}b_m)x^{n+m-1}+\cdots+(a_1b_0+a_0b_1)x+a_0b_0,$$

其中 k 次项的系数是 $\sum_{i+j=k}a_ib_j$.

同样易于验证，$D[x]$ 中的乘法满足结合律，交换律与分配律(因这也归结为 D 中元素的加法与乘法运算). 多项式 1 在 $D[x]$ 中乘法的作用相当与数 1 在 D 中乘法的作用：$1\cdot f(x)=f(x)$.

因此，$D[x]$ 对(上面定义的) 加法与乘法形成一个交换环，我们称之为 **D 上的一元多项式环**.

最后，我们简要地介绍一下 D 上的多元多项式. 设 $x_1,\cdots,x_n$ 为 n 个不定元，形如

$$ax_1^{i_1}\cdots x_n^{i_n}$$

的式子，称为一个 n 元**单项式**，其中系数 $a\in D$，$i_1,\cdots,i_n$ 为非负整数，而 $x_1^{i_1},\cdots,x_n^{i_n}$ 允许交换次序. 如果两个单项式中相同不定元的幂次均相等，则称它们为**同类项**. 有限个(不同类的)单项式的(形式)和

$$\sum_{i_1,\cdots,i_n}a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n},\quad a_{i_1\cdots i_n}\in D,$$

称为 **系数在 D 中的 n 元多项式**，也称为 D 上的 n 元多项式. D 上所有 n 元多项式的集合记作 $D[x_1,\cdots,x_n]$. 我们常用 $F(x_1,\cdots,x_n)$，$G(x_1,\cdots,x_n),\cdots$ 或 $F,G,\cdots$ 等来代表 n 元多项式.

各个单项式的系数都是零的多项式，称为 $D[x_1,\cdots,x_n]$ 中**零多项式**，简称零，记作 0. 设 $F(x_1,\cdots,x_n)$ 与 $G(x_1,\cdots,x_n)$ 是 $D[x_1,\cdots,x_n]$ 中两个多项式，如果 F 与 G 中的单项式一一对应地为系数相等的同类项，则称 F 与 G **相等**(或恒等)，记作 $F=G$.

$D[x_1,\cdots,x_n]$ 中可定义加、减、乘法运算.

对 $F,G\in D[x_1,\cdots,x_n]$,F 与 G 的和,记作 $F+G$,是 D 上唯一确定的多项式,其中的项是 F 与 G 的诸单项式的和(将两者的同类项"合并"—— 就是将系数相加).此外,对于任意的 $F\in D[x_1,\cdots,x_n]$,改变其诸单项式的符号所得的多项式,记作 $-F$,并定义

$$F-G=F+(-G),$$

于是 $D[x_1,\cdots,x_n]$ 中可作减法运算.

$D[x_1,\cdots,x_n]$ 中两个单项式

$$ax_1^{i_1}\cdots x_n^{i_n}\quad 与\quad bx_1^{j_1}\cdots x_n^{j_n}$$

的积定义为 $abx_1^{i_1+j_1}\cdots x_n^{i_n+j_n}$;对任意 $F,G\in D[x_1,\cdots,x_n]$,F 与 G 的积,记作 FG,是 D 上唯一确定的多项式,其中的项是 F 与 G 中诸单项式两两(如上)乘积之和.

易于验证,$D[x_1,\cdots,x_n]$ 中的多元多项式,对于上述定义的加、减、乘法运算,满足与 $D[x]$ 中运算相同的运算规律,因此是一个交换环,我们称之为 **D 上的多元多项式环**.

第一部分

整　　数

第一章　数的整除性

§1. 整　　除

我们知道，整数集合中除了加法和乘法之外还可作减法运算，并且这些运算满足一些规律(见引言)，但是一般不能作除法，也就是说，如 a,b 是整数，$b\neq 0$，则 $\frac{a}{b}$ 不一定是整数，即不一定存在整数 c 使 $a=bc$. 由此引出初等数论中第一个基本概念：数的整除性.

设 a 和 b 是整数，$b\neq 0$. 如果存在整数 c 使得 $a=bc$，则称 b **整除** a，表示成 $b|a$，并称 b 是 a 的一个**约数**(或**因子**)，而 a 为 b 的**倍数**. 如果不存在上述的整数 c，则称 b **不整除** a，表示成 $b\nmid a$ ①.

由整除的定义，立即导出整除的如下的基本性质.

定理 1　设 a,b,c 是整数.

(i) 如 $b|a$，且 $c\neq 0$，则 $bc|ac$. 反之亦然，特别地，$b|a$ 等价于 $(\pm b)|(\pm a)$；

(ii) 如 $b|c$ 且 $c|a$，则 $b|a$；

(iii) 如 $b|a$ 且 $b|c$，则 a,c 的任意整系数线性组合均是 b 的倍数，即对任意整数 x,y 有 $b|(ax+cy)$；

(iv) 如 $b|a$ 且 $a\neq 0$，则 $|b|\leqslant|a|$；于是，如 $b|a$ 且 $a|b$，则 $|a|=|b|$.

现在我们给出整数的一个非常基本的性质.

---

① 国标规定不整除符号用“$\not|$”表示，本书为排印方便，用“$\nmid$”表示.

定理 2（带余除法）　设 a,b 为整数，$b\neq 0$，则存在整数 q,r，使得

$$a=bq+r,\quad \text{其中}\quad 0\leqslant r<|b|; \tag{1}$$

并且整数 q,r 由上述条件唯一决定.

证明　当 $b|a$ 时，可取 $r=0$，$q=\dfrac{b}{a}$. 当 $b\nmid a$ 时，我们考虑集合

$$E=\{a-bk\,|\,k\in\mathbf{Z}\}.$$

易知，E 中有正整数，因此 E 中有最小正整数，设为

$$r=a-bq>0.$$

我们证明必有 $r<|b|$. 因现在 $b\nmid a$，故 $r\neq|b|$. 若 $r>|b|$，则 $r'=r-|b|>0$；又 $r'\in E$，这与 r 的最小性矛盾. 于是我们作出了形如(1)的表示.

现在证明表示的唯一性. 假设

$$a=bq_1+r_1,\quad \text{其中}\quad 0\leqslant r_1<|b|.$$

结合(1)有

$$b(q-q_1)+(r-r_1)=0.$$

由此推出 $b|(r-r_1)$. 但

$$0\leqslant|r-r_1|<|b|,$$

故必须 $r-r_1=0$，即 $r=r_1$（参考定理 1(iv)），从而

$$q=q_1.$$

注记　1. 等式(1) 中的整数 q 称为 a 被 b 除的（不完全）**商**，数 r 叫做 a 被 b 除得的**余数**. $r=0$ 的情形即为 a 被 b 整除.

2. 定理 1 的核心是关于余数 r 的不等式. 论证的主要步骤是选取余数，这依赖于（正整数集合的）最小数原理. 为应用这一原理，我们首先证明所考虑的（整数）集合中有正整数，进而可从中选取最小正整数. 本书中许多地方均采用这一手法.

作为带余除法的例子，我们看到，整数被 2 除的余数有两个可能值：0 和 1. 一个整数被 2 整除则称为偶数，否则称为奇数. 因此偶数可表示为 $2k$，而奇数为 $2k+1$（k 是整数）.

类似地，整数被 3 除的余数为 0,1,2. 因此任一整数可表示为 $3k$，$3k+1$，$3k+2$ 三种形式之一.

定理 3　设 S 是 $\mathbf{Z}$ 的一个（非空）子集，对减法运算封闭，即对任意 $x,y\in S$ 有 $x-y\in S$.

则存在唯一的整数 $d\geqslant 0$，使得 S 是由 d 的所有倍数构成，即

$$S=d\mathbf{Z}=\{da\mid a\in\mathbf{Z}\}.$$

证明　我们首先注意，$0\in S$；以及，如 $x\in S$，则

$$-x=0-x\in S.$$

因此对任意 $x,y\in S$，

$$y+x=y-(-x)\in S,$$

所以 S 对加法运算也封闭. 进而由归纳法易证，对任意 $x\in S$ 及 $n\in\mathbf{Z}$ 有 $nx\in S$. 从而，S 中元素的任意整系数线性组合仍在 S 中.

现在我们证明定理. 如果 $S=\{0\}$，则结论显然成立（取 $d=0$）. 如 S 中有非零元，则其中必有正整数，从而有最小正整数 d. 显然，d 的所有倍数均属于 S. 另一方面，对任意 $x\in S$，由定理 2，我们可表示为 $x=dq+r$，其中 $0\leqslant r<d$；显然 $r=x-dq\in S$. 由于 d 的最小性，必须有 $r=0$，于是 $x=dq$. 因此 $S=d\mathbf{Z}$. 最后，因 d 是集合中最小正整数，它由（给定的）S 唯一确定.

注记　用代数的语言，满足定理 3 中条件的子集称为 $\mathbf{Z}$ 的理想，而对任意整数 d，理想 $d\mathbf{Z}$ 由一个元素 d“生成”，称为主理想，也常记作 (d). 定理 3 表明，$\mathbf{Z}$ 中每个理想都是主理想，我们因此称 $\mathbf{Z}$ 为主理想（整）环.

习　题　1

1*. 设 a,b 为整数，$a \neq b$，n 是正整数，则 $(a-b)\mid(a^n-b^n)$.

2*. 设 a,b 是整数 $a+b \neq 0$，n 是正奇数，则 $(a+b)\mid(a^n+b^n)$.

3*. 设 n 是奇数，则 $8\mid(n^2-1)$.

4. (i) 设 n 是整数，证明：$6\mid n^3-n$；

(ii) 设 $a_1,\cdots,a_k$ 是整数，$a_1+\cdots+a_k$ 被 6 整除，则 $a_1^3+\cdots+a_k^3$ 也被 6 整除.

5. 设 $n>1$ 是奇数，证明：$(1+\frac{1}{2}+\cdots+\frac{1}{n-1})(n-1)!$ 被 n 整除.

6. 设 m,n 为正整数，$m>2$. 证明：$2^m-1\nmid 2^n+1$.

7*. 对任意实数 x，定义 $[x]$ 为不超过 x 的最大整数，即整数 $[x]$ 满足 $x-1<[x]\leqslant x$.

证明：$1,2,\cdots,n$ 中恰有 $[\frac{n}{k}]$ 个数被 k 整除，这里 n,k 均是正整数.

8*. 证明：当 $b>0$ 时，定理 2 中的整数 q 可表示为 $q=[\frac{a}{b}]$；并在 $b<0$ 时给出 q 的类似表达式.

9*. 设整数 $q>1$. 证明

(i) 每个正整数 n 可唯一地表示为

$$n=a_kq^k+\cdots+a_1q+a_0,$$

其中 a_i 是满足 $0\leqslant a_i\leqslant q-1$ 的整数 $(0\leqslant i\leqslant k)$，而 $a_k\neq 0$. 这一表达式称为 n 的 **q 进制表示**，数 a_i 称为 q 进制表示中的数码；

(ii) $a_i=[\frac{n}{q^i}]-[\frac{n}{q^{i+1}}]$，$0\leqslant i\leqslant k$.

10*. 设 $\alpha_1,\cdots,\alpha_n$ 为实数，证明

$$[\alpha_1]+\cdots+[\alpha_n]\leqslant[\alpha_1+\cdots+\alpha_n]\leqslant[\alpha_1]+\cdots+[\alpha_n]+n-1.$$

11. 设 α,β 为实数，证明：

$$[2\alpha]+[2\beta]\geqslant[\alpha]+[\beta]+[\alpha+\beta].$$

12*. 设 x 是实数，$n\geqslant 2$ 为整数，证明

$$[x]+[x+\frac{1}{n}]+\cdots+[x+\frac{n-1}{n}]=[nx].$$

§2. 最大公约数与最小公倍数

设 $a,b,\cdots,c$ 是(有限个)不全为零的整数，满足下面两个条件的(唯一的)整数 d 称为它们的**最大公约数**，记作$(a,b,\cdots,c)$：

(i) d 是 $a,b,\cdots,c$ 的公(共)约数，即 $d|a,d|b,\cdots,d|c$；

(ii) d 是 $a,b,\cdots,c$ 的所有公约数中最大的，即如果整数 d_1 也是 $a,b,\cdots,c$ 的公约数，则 $d_1\leqslant d$.

我们注意，任意整数$a,b,\cdots,c$必然有公约数(例如 ± 1). 如果它们不全为零，则易见它们的公约数只有有限多个(参考 §1，定理 1(iv))，所以它们的最大公约数必然存在并且是唯一的. 此外，如 d 是 $a,b,\cdots,c$ 的公约数，则 $-d$ 也是它们的公约数，从而最大公约数一定是正整数.

如果$(a,b,\cdots,c)=1$，则称 $a,b,\cdots,c$ 是**互素**的；换句话说，$a,b,\cdots,c$ 是互素的，指它们的公约数只有 ± 1.

如果数 $a,b,\cdots,c$ 中任意两个是互素的，则称 $a,b,\cdots,c$ **两两互素**. 明显地，两两互素的数一定也互素(但反之不然)；而对于两个数而言，互素与两两互素的概念是一样的.

最大公约数有下面的简单的性质：

定理 1　(i) 任意改变 $a,b,\cdots,c$ 的符号不变$(a,b,\cdots,c)$ 的值；

(ii) 任意交换$(a,b,\cdots,c)$ 中两个字母的位置不变其值；

(iii) 设 $a\neq 0$，则$(a,a,\cdots,a)=|a|$；

(iv) $(a,b,\cdots,c)$ 作为 $b,\cdots,c$ 的函数均以 a 为周期，即

$$(a,b,\cdots,c)=(a,b+a,\cdots,c)=\cdots=(a,b,\cdots,c+a). \quad (1)$$

一般地，对任意整数 $x,\cdots,y$，有

$$(a,b,\cdots,c)=(a,b+ax,\cdots,c+ay). \tag{2}$$

证明　(i),(ii),(iii)均可以从定义看出来. 对于(iv)，我们设

$$d=(a,b,\cdots,c),\quad d'=(a,b+a,\cdots,c),$$

则 $a,b,\cdots,c$ 均被 d 整除，从而 $a,a+b,\cdots,c$ 被 d 整除，故 $d\leqslant d'$；同样地，$d'\leqslant d$. 因此 $d=d'$. 再由(ii)可得出(1)中其余等式. (2)可以反复用(1)及性质(i)推出来.

下面的定理 2 是我们建立最大公约数性质的基础.

定理 2　设 $a,b,\cdots,c$ 是不全为零的整数，则 $a,b,\cdots,c$ 的整线性组合

$$ax+by+\cdots+cz$$

(系数 $x,y,\cdots,z$ 是任意整数)的集合，恰由 $(a,b,\cdots,c)$ 的所有倍数构成.

证明　将 §1，定理 3 应用于集合

$$S=\{ax+by+\cdots+cz\mid x,y,\cdots,z\in\mathbf{Z}\},$$

便推出了 $S=D\mathbf{Z}$，这里 D 是 S 中最小正数(注意现在 $S\neq\{0\}$). 记 $d=(a,b,\cdots,c)$，下面证明 $D=d$.

首先，由于 $D\in S$，故有整数 $x,y,\cdots,z$，使 $D=ax+by+\cdots+cz$. 因 $d\mid a,d\mid b,\cdots,d\mid c$，故

$$d\mid(ax+by+\cdots+cz)\text{(参考 §1，定理 1(iii))},$$

即 $d\mid D$. 注意 d,D 均正数，故特别地有 $d\leqslant D$(§1，定理 1(iv)). 另一方面，因(显然)$a,b,\cdots,c$ 均属于 S，故它们都是 D 的倍数，即 D 是 $a,b,\cdots,c$ 的公约数，从而 $D\leqslant d$. 综合上述两方面，便证明了 $d=D$.

推论　设$a,b,\cdots,c$是不全为零的整数，则存在整数$x,y,\cdots,z$，使得

$$ax+by+\cdots+cz=(a,b,\cdots,c).$$

这一等式称为**裴蜀(Bezout)等式**. 特别地，如$a,b,\cdots,c$互素，则存在整数$x,y,\cdots,z$，使

$$ax+by+\cdots+cz=1; \tag{3}$$

并且，(3)有整数解$x,y,\cdots,z$也是$a,b,\cdots,c$互素的充分条件.

现在我们能够给出最大公约数的一些基本性质.

定理 3　(i) $a,b,\cdots,c$的每一个公约数都是它们的最大公约数的约数；

(ii) $(a,b,\cdots,c)=((a,b),\cdots,c)$；

(iii) 设m为正整数，则

$$(ma,mb,\cdots,mc)=m(a,b,\cdots,c);$$

(iv) 设$(a,b,\cdots,c)=d$，则$\left(\frac{a}{d},\frac{b}{d},\cdots,\frac{c}{d}\right)=1$；

(v) 设$(a,m)=(b,m)=1$，则$(ab,m)=1$. 一般地，如果若干个整数均与m互素，则它们的积也与m互素；

(vi) 如$c\mid ab$且$(c,b)=1$，则$c\mid a$.

证明　(i) 这是最大公约数最本质的属性，不难由裴蜀等式推出来.

(ii) 设$d=(a,b,\cdots,c)$，$d'=((a,b),\cdots,c)$. 显然d'是$a,b,\cdots,c$的公约数，故$d'\leqslant d$；另一方面，因d整除$a,b,\cdots,c$，故由(i)知$d\mid(a,b)$，从而d是$(a,b),\cdots,c$的公约数，故$d\leqslant d'$. 综合两方面知$d=d'$.

(iii) 设$d=(a,b,\cdots,c)$，$e=(ma,mb,\cdots,mc)$，我们证明$e=md$. 因md整除$ma,mb,\cdots,mc$，故由(i)知$md\mid e$. 另一方面，由裴蜀等式，存在整数$x,y,\cdots,z$使$ax+by+\cdots+cz=d$，于是

$$amx + bmy + \cdots + cmz = md,$$

故 $e|md$. 因此 $e = md$.

(iv) 显然 $\frac{a}{d}, \frac{b}{d}, \cdots, \frac{c}{d}$ 都是整数. 由(iii)可见

$$d = \left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}, \cdots, d \cdot \frac{c}{d}\right) = d\left(\frac{a}{d}, \frac{b}{d}, \cdots, \frac{c}{d}\right),$$

从而结论成立.

(v) 由 $(a,m) = (b,m) = 1$ 知,存在整数 x, y, x', y' 使得

$$ax + my = 1 \quad 及 \quad bx' + my' = 1.$$

将两式相乘,产生

$$ab(xx') + m(axy' + bx'y + myy') = 1,$$

从而 $(ab,m) = 1$. 一般情形不难用归纳法证明.

(vi) 已知 $c|ab$, 又显然有 $c|ac$. 从而由 (i) 可知 $c|(ab,ac)$. 但由(iii),$(ab,ac) = |a|(b,c) = |a|$,于是 $c|a$.

注记　1. 反复用定理 3(ii)可见,求两个以上的整数的最大公约数,化归为求两个整数的最大公约数. 对这一问题,我们有下面的算法:

欧几里德(Euclid)算法　设 a,b 为整数,$b \neq 0$,按下述方式反复作带余除法(§1,定理 1),有限步之后必然停止(即余数为零):

$$\begin{aligned}
&\text{用 } b \text{ 除 } a: \quad a = bq_0 + r_0, \quad 0 < r_0 < |b|;\\
&\text{用 } r_0 \text{ 除 } b: \quad b = r_0q_1 + r_1, \quad 0 < r_1 < r_0;\\
&\text{用 } r_1 \text{ 除 } r_0: \quad r_0 = r_1q_2 + r_2, \quad 0 < r_2 < r_1;\\
&\qquad\qquad \vdots\\
&\text{用 } r_{n-1} \text{ 除 } r_{n-2}: \quad r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1};\\
&\text{用 } r_n \text{ 除 } r_{n-1}: \quad r_{n-1} = r_n q_{n+1}.
\end{aligned}$$

则 $(a,b) = r_n$.

事实上,由于诸余数 $r_0, r_1, \cdots$ 为整数,且满足

$$r_0 > r_1 > \cdots > r_{n-1} > \cdots \geqslant 0,$$

从而上述的带余除法有限步后余数必为零. 另一方面，由定理 1(iv)，我们有

$$(a,b)=(bq_0+r_0,b)=(b,r_0)=(r_0,r_1)=$$
$$\cdots=(r_{n-1},r_n)=r_n.$$

2. 上面的算法不仅能求 (a,b)，还可以实际地求出方程

$$ax+by=(a,b) \tag{4}$$

的一组整数解. 具体的做法是将欧氏算法倒推回去：

由算法中的倒数第二行，得到

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

这就将 (a,b) 表示成 r_{n-2},r_{n-1} 的整线性组合. 用算法中在其前面的一行 $r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}$ 代入上式，消去 r_{n-1}，得出

$$(a,b)=r_{n-2}(1+q_{n-1}q_n)-r_{n-3}q_n.$$

如此进行，最终便求得方程(4) 的一组整数解 x,y.

最小公倍数是与最大公约数对偶的概念.

设 $a,b,\cdots,c$ 是(有限个) 非零整数，满足下面两个条件的(唯一的) 整数 D 称为它们的**最小公倍数**，记作 $[a,b,\cdots,c]$.

(i) D 为正整数，且 D 是 $a,b,\cdots,c$ 的公(共) 倍数，即 $D\geqslant 1$ 且 $a|D$，$b|D,\cdots,c|D$；

(ii) D 是 $a,b,\cdots,c$ 的正公倍数中的最小数，即如果 $D_1\geqslant 1$，使 $a|D_1,b|D_1,\cdots,c|D_1$，则 $D\leqslant D_1$.

定理 4　(i) $a,b,\cdots,c$ 的每个公倍数都是 $[a,b,\cdots,c]$ 的倍数；

(ii) $[a,b,\cdots,c]=[[a,b],\cdots,c]$；

(iii) 设 m 为正整数，则

$$[ma,mb,\cdots,mc]=m[a,b,\cdots,c];$$

(iv) $(a,b)[a,b]=|ab|$；

(v) 如 $a,b,\cdots,c$ 两两互素,则$[a,b,\cdots,c] = |ab\cdots c|$.

证明 (i) 设 S 是由 $a,b,\cdots,c$ 的所有公倍数构成的集合,则 S 显然满足 §1,定理 3 的条件. 因此 S 恰好是由某个正整数 D 的所有倍数构成的集合,显然 D 必是 S 中最小正整数,从而是$[a,b,\cdots,c]$. 这立即推出了所说的结论.

(ii) 用(i)像定理 3(ii)那样论证.

(iii) 设 $D = [ma,mb,\cdots,mc]$,$D' = [a,b,\cdots,c]$. 由定义,$ma,mb,\cdots,mc$ 均整除 D,故 $a,b,\cdots,c$ 整除 $\frac{D}{m}$,从而 $D' \leqslant \frac{D}{m}$. 类似地可知 $D \leqslant mD'$. 因此 $D = mD'$.

(iv) 我们可假设 a,b 均为正整数. 首先考虑 $(a,b) = 1$ 的情形. 由定义知,有整数 x,y 使

$$ax = [a,b] = by.$$

于是 $b|ax$,但 $(a,b) = 1$,从而 $b|x$(定理 3(vi)),因此 $ab|ax$,即 $ab|[a,b]$. 但 ab 是 a 和 b 的公倍数,从而必有 $ab = [a,b]$.

一般情形可化归为上述的特殊情形. 设 $d = (a,b)$,则

$$\left(\frac{a}{d},\frac{b}{d}\right) = 1\text{(定理 3(iv))}.$$

于是

$$\left[\frac{a}{d},\frac{b}{d}\right] = \frac{ab}{d^2}.$$

进而我们导出(利用(iii)及定理 3(iii))

$$\begin{aligned}(a,b)[a,b] &= d\left(\frac{a}{d},\frac{b}{d}\right)\cdot d\left[\frac{a}{d},\frac{b}{d}\right]\\ &= d^2\cdot\frac{ab}{d^2} = ab.\end{aligned}$$

(v) 这可由(ii),(iv),定理 3(v)及归纳法推出来.

习　题　2

1. 设 n 是正整数，证明：$\frac{21n+4}{14n+3}$ 是既约分数.

2. 设 n 是正整数，证明：$(n!+1,(n+1)!+1)=1$.

3. 设 m,n 为正整数，m 是奇数. 证明：$(2^m-1,2^n+1)=1$.

4*. 设 m,n,a 均为正整数，且 $a>1$. 证明

$$(a^m-1,a^n-1)=a^{(m,n)}-1.$$

5*. 设 a,b 是不为 0 或 ± 1 的整数. 证明：存在整数 x,y，满足

$$ax+by=(a,b),$$

且 $0<|x|<|b|$，$0<|y|<|a|$.

6*. 给定整数 a,b. 证明：存在整数 x,y,u,v，使得 $a=xu,b=yv$，$(x,y)=1$ 且 $[a,b]=xy$.

7*. 设 m,n 都是正整数且 $(m,n)=1$. 证明

(i) $(d,mn)=(d,m)(d,n)$；

(ii) mn 的任一个正约数 d，可唯一地表示为 $d=d_1d_2$，其中 d_1,d_2 分别是 m,n 的正约数.

8*. 设 n 为正整数，证明

(i) $(a^n,b^n)=(a,b)^n$；

(ii) 设 a,b 是互素的正整数，$ab=c^n$（c 为整数），则 a,b 都是正整数的 n 次方幂. 事实上，$a=(a,c)^n,b=(b,c)^n$.

一般地，如果若干个两两互素的正整数之积是整数的 n 次幂，则这些整数都是 n 次方幂.

9. 设 n 为正整数，k 为正奇数，证明

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

10*. 设 $a,b,\cdots,c$ 是不全为零的整数，则方程

$$ax+by+\cdots+cz=d$$

有整数解 $x,y,\cdots,z$ 的充分必要条件是 $(a,b,\cdots,c)\mid d$.

11*. 设 a,b,c 为整数，$(a,b)\mid c$. 设 $x=x_0,y=y_0$ 是方程

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

的一组整数解(称为方程(1)的**特解**)，则方程(1)的全部整数解(通解)为

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

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

其中 t 为任意整数.

12. 用欧氏算法求 963 和 657 的最大公约数，并求出方程

$$963x+657y=(963,657)$$

的一组特解，及所有整数解.

13*. 设 a,b 为正整数且 $(a,b)=1$. 证明：当整数 $n>ab-a-b$ 时，方程

$$ax+by=n \tag{2}$$

有非负的整数解；但当 $n=ab-a-b$ 时，方程(2) 没有非负整数解.

14. 求下列方程的全部整数解：

(i) $x+2y+3z=10$；

(ii) $6x+20y-15z=23$；

(iii) $9x+24y-5z=4$；

(iv) $25x+13y+7z=2$.

§3. 唯一分解定理

设 p 为大于 1 的整数，如果 p 没有真因子，即 p 的正约数只有 1 和 p 自身，则称 p 为**素数**(或质数)，否则称为**合数**(或复合数).

于是，正整数被分成三类：数 1 单独作一类，素数类及合数类.

容易看到，大于 1 的整数至少有一个素因子. 这是因为大于 1 的整数当然有大于 1 的正约数，其中的最小数必是素数.

关于素数最经典的一个结果是公元前 3 世纪欧几里德证明的：

定理 1　素数有无穷多个.

证明　用反证法. 假设素数只有有限多个，设 $p_1,\cdots,p_r$ 是全部素数，考虑 $N = p_1\cdots p_r + 1$. 由于 $N > 1$，故 N 一定有素约数 p. 由假设 p 必然等于某个 $p_i(1 \leqslant i \leqslant r)$，因而 p 整除 $N - p_1\cdots p_k = 1$，这不可能. 因此素数有无穷多个.

设 p 为素数，n 是任意整数. 由于 (p,n) 是 p 的正约数，故 $(p,n) = 1$ 或 p，即或者 p 与 n 互素，或者 p 整除 n.

定理 2　设 p 是素数，$a,b,\cdots,c$ 是整数. 如果 p 整除乘积 $ab\cdots c$，则 $a,b,\cdots,c$ 中至少有一个被 p 整除.

证明　假如结论不对，则 $a,b,\cdots,c$ 均与 p 互素，从而它们的积也与 p 互素（§2，定理 3(v)），与已知矛盾.

现在我们能够证明整数中最基本的一个结果，它表明素数是整数的“基石”：

定理 3(唯一分解定理)　(i) 每个不等于 1 的正整数均可分解为有限个素数的乘积；

(ii) 如果不计素因数在乘积中的次序，则(i) 中的分解方式是唯一的.

证明　(i) 我们对 n 归纳. 如果 $n = 2$，因 2 是素数，从而结论成立. 假设结论对小于 n 的正整数均成立，现在考虑 n. 如果 n 是素数，则结论

对 n 成立；如果 n 是合数，则 n 有真因子 a，而 $n = ab$（a,b 均是大于 1 的正整数）. 显然 a,b 都小于 n，由归纳假设，a,b 均可分解为有限个素数之积，从而 n 也如此.

(ii) 我们仍对 n 归纳，$n = 2$ 时，分解显然是唯一的. 假设结论对小于 n 的正整数均成立，现在考虑 n. 如果 n 有两种方式分解为素数的积：$n = p_1 \cdots p_r$ 及 $n = q_1 \cdots q_s$，则 p_1 整除 $q_1 \cdots q_s$. 由定理 2，素数 p_1 必整除某个 $q_i (1 \leqslant i \leqslant s)$，无妨设 $p_1 | q_1$. 因 q_1 是素数，故必须 $p_1 = q_1$.

令 $n' = \dfrac{n}{p_1} (= \dfrac{n}{q_1})$. 如果 $n' = 1$，即 $n = p_1 = q_1$，则结论对 n 当然成立. 如 $n' > 1$，则因 $n' < n$，对 n' 用归纳假设便推出，$r = s$ 并且 $p_2, \cdots, p_r$ 是 $q_2, \cdots, q_s$ 的一个排列，从而 n 的素因数分解是唯一的.

由定理 3 立即推出，不等于 -1 的负整数，除 ± 1 因子之外，可唯一地分解为素数的乘积. 我们说 $\mathbf{Z}$ 是唯一分解环或具有唯一分解性.

对于不等于 ± 1 的非零整数 n，将其分解中相同的素因子收集在一起，即知 n 可唯一地表示为

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

其中 $p_1, \cdots, p_k$ 是互不相同的素数，$\alpha_1, \cdots, \alpha_k$ 为正整数，而 $\varepsilon = \pm 1$. 这称为 n 的素因数**标准分解**.

注记　1. 定理 3 的核心是分解的唯一性. 事实上，分解的存在性是素数定义的直接推论，但唯一性却远远不是平凡的. 作为一个说明，大数学家希尔伯特(Hilbert)曾提出过下面的例子：考虑集合

$$S = \{4x + 1 | x = 0, 1, 2, \cdots\}.$$

显然，S 对乘法运算封闭. 设 $n \in S$ 且 $n \neq 1$，如果 n 不能分解为 S 中两个大于 1 的数之积，则定义 n 为 S 中的“素数”. 于是 5,9,13,17,21 都是 S 中的“素数”，但 25,45 则不是“素数”. 由定义即知，S 中不为 1 的数均可分解成 S 中的“素数”之积.

另一方面，如果 p,q 均是 $4k - 1$ 型的素数 $(p \neq q)$，则 pq, p^2, q^2 都

是 S 中“素数”. 但等式

$$(pq)^2 = pq \cdot pq = p^2 \cdot q^2$$

表明，S 中的数 $(pq)^2$ 有两种不同的方式分解为(S 中的)“素数”之积. 由于 $4k-1$ 型的素数有无穷多个(习题 3.5)，故 S 中有无穷多个数，它们分解为“素数”乘积的方式不唯一. 然而，这些数在 S 之外则有唯一的素因数分解(定理 3(ii)).

2. 定理 3(ii) 的证明依靠分解的存在性(定理 3(i)) 及定理 2. 反过来，由定理 3 也能够证明定理 2，即如果素数 $p|ab$，则 $p|a$ 或 $p|b$.

事实上，设 $ab = pc$，并令(我们可设整数 a,b 均大于 1)

$$a = \prod_i p_i, \quad b = \prod_j p_j', \quad c = \prod_k q_k$$

是 a,b,c 的素因数分解(定理 3(i)). 我们有

$$\prod_i p_i \cdot \prod_j p_j' = p \prod_k q_k,$$

因此由定理 3(ii) 推出，p 必然与 p_i 及 p_j' 之一相同，从而 $p|a$ 或者 $p|b$.

由正整数的标准分解，我们容易确定正整数的约数.

推论 1　设 $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 n 的标准分解，则正整数 d 是 n 的约数的充分必要条件是其标准分解为

$$d = p_1^{\beta_1}\cdots p_k^{\beta_k}, \quad 0 \leqslant \beta_1 \leqslant \alpha_1, \cdots, 0 \leqslant \beta_k \leqslant \alpha_k. \tag{1}$$

证明　充分性是显然的. 下面证明必要性. 如 $d = 1$，这是(1) 的形式(所有 $\beta_i = 0$). 如 $d > 1$，则由 $d|n$ 及定理 3 知，d 的素因数必在 $p_1,\cdots,p_k$ 中，所以 d 的标准分解式必为 $d = p_1^{\beta_1}\cdots p_k^{\beta_k}$(每个 β_i 为非负整数). 我们来证明 $\beta_i \leqslant \alpha_i (1 \leqslant i \leqslant k)$. 如有一个 $\beta_i > \alpha_i$，无妨设 $i = 1$. 则由 $p_1^{\beta_1}|d$ 及 $d|n$ 推出 $p_1^{\beta_1-\alpha_1}|p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，由此及定理 2 知，$p_1$ 必与 $p_2,\cdots,p_k$ 之一相等，矛盾! 因此 d 具有(1)的形式.

推论 2　设 a,b 是正整数，它们的标准分解为

$$a = p_1^{\alpha_1}\cdots p_k^{\alpha_k},\quad b = p_1^{\beta_1}\cdots p_k^{\beta_k},$$

其中 $p_1,\cdots,p_k$ 是不同的素数. 为了使两个分解式在形式上包含同样的素数，我们允许 α_i,β_i 可取 0，即 α_i 和 β_i 是非负整数($1\leqslant i\leqslant k$). 则

(i) $(a,b) = p_1^{a_1}\cdots p_k^{a_k}$，其中 $a_i = \min(\alpha_i,\beta_i)$；

(ii) $[a,b] = p_1^{b_1}\cdots p_k^{b_k}$，其中 $b_i = \max(\alpha_i,\beta_i)$.

证明　记 $m = p_1^{a_1}\cdots p_k^{a_k}$，则 m 是 a 和 b 的公约数. 另一方面，由推论 1 易证 a 和 b 的任一公约数必整除 m，因此 $m = (a,b)$. 同样可证明 (ii).

注记　1. 多于两个整数的最大公约数与最小公倍数有类似的表达式. 这些公式的价值是在于理论上的 —— 对证明最大公约数与最小公倍数的某些性质非常有用，并非是实际计算的简单工具，因为，一般而言，作出一个整数的标准分解是极其困难的事情.

2. 我们提及(但不作讨论)下面的事实：唯一分解定理能够不用 §1 和 §2 中的准备直接证明；而由此为出发点，像推论 2 那样定义最大公约数与最小公倍数，也可以建立数的整除理论(即证明 §2 中定理 3 和定理 4).

推论 3　设 $n\geqslant 1$，定义**除数函数** $\tau(n)$ 为 n 的正约数的个数；**除数和函数** $\sigma(n)$ 为 n 的正约数之和. 设 $n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ 是 n 的标准分解.

(i) 我们有

$$\tau(n) = (\alpha_1+1)\cdots(\alpha_k+1), \tag{2}$$

及

$$\sigma(n) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}; \tag{3}$$

(ii) 如 $(m,n) = 1$，则有

$$\tau(mn)=\tau(m)\tau(n)\quad 及\quad \sigma(mn)=\sigma(m)\sigma(n).$$

证明　(i) 公式(2)易由推论 1 导出来;由于 $\tau(1)=1$,故(2) 对 $n=1$ 也成立(看作 $\alpha_1=\cdots=\alpha_k=0$ 的情形). 为了证明(3),仍用推论 1,我们有

$$\sigma(n)=\sum_{\substack{0\leqslant\beta_i\leqslant\alpha_i\\1\leqslant i\leqslant k}} p_1^{\beta_1}\cdots p_k^{\beta_k}=\sum_{\beta_1=0}^{\alpha_1}p_1^{\beta_1}\Big(\sum_{\substack{0\leqslant\beta_i\leqslant\alpha_i\\2\leqslant i\leqslant k}} p_2^{\beta_2}\cdots p_k^{\beta_k}\Big)=\cdots$$

$$=\Big(\sum_{\beta_1=0}^{\alpha_1}p_1^{\beta_1}\Big)\cdots\Big(\sum_{\beta_k=0}^{\alpha_k}p_k^{\beta_k}\Big)$$

$$=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_k^{\alpha_k+1}-1}{p_k-1}.$$

(ii) 这是(i)的直接推论.(两整数互素,意味着它们的标准分解中没有相同的素因子;反之亦然.) (ii)也可以不用唯一分解定理,而由习题 2.7 推出来.

注记　我们将定义在正整数集上的函数称为**数论函数**,它们的取值通常是整数,但也允许为复数. 设 $f(n)$ 是一个数论函数,如果当 $(m,n)=1$ 时有

$$f(mn)=f(m)f(n),$$

则称 $f(n)$ 是**积性函数**. 推论 3(ii)表明,除数函数及除数和函数均是积性函数. 很明显,积性函数 $f(n)$ 的值由它在 $n=1$ 及 n 为素数幂处的值决定;又容易看出,如果 $f(n)$ 是一个不恒为零的积性函数,则 $f(1)=1$.

习　题　3

1*. 设 n 为正整数,$n\geqslant 2$. 如果 n 不被不超过 $\sqrt{n}$ 的素数整除,则 n 是素数.

2. 设 $n>1$ 为整数，如果对于任何整数 m，或者 $n\mid m$ 或者 $(n,m)=1$，则 n 必是素数.

3. 设整数 $n>2$，证明：n 和 $n!$ 之间必有素数. 由此证明素数有无穷多个.

4*. 设整数 $n\geqslant 2$，证明：存在连续 n 个正整数，其中每一个都不是素数.（这表明，在正整数序列中，可以有任意长的一段区间中不包含素数.）

5*. 证明：(i) 形如 $4m+3$ 的素数有无穷多个；

(ii) 形如 $6m+5$ 的素数有无穷多个.

6. 证明：如果 $p,p+2,p+4$ 都是素数，则 $p=3$.

7. 用唯一分解定理证明习题 2.8 的结论.

8. 设整数 $10^{n-1}+10^{n-2}+\cdots+1(n>1)$ 是素数，则 n 是素数；但反之不成立.

9*. (i) 设 m 为正整数，证明：如 2^m+1 为素数，则 m 为 2 的方幂；

(ii) 对 $n\geqslant 0$，记 $F_n=2^{2^n}+1$，这称为**费马**(Fermat)**数**. 证明：如 $m>n$，则 $F_n\mid(F_m-2)$；

(iii) 证明：如 $m\neq n$，则 $(F_m,F_n)=1$. 由此证明素数有无穷多个.

注记　费马数中的素数称为**费马素数**. 例如 $F_0=3$，$F_1=5$，$F_2=17$，$F_3=257$，$F_4=65537$ 都是素数. 费马曾经猜测所有的 F_n 都是素数，但是欧拉在 1732 年证明了 $F_5=641\cdot 6700417$，不是素数. 目前人们不知道是否还有费马素数，更不知道这样的素数是否有无穷多个.

10*. (i) 设 m,n 都是大于 1 的整数，证明：如果 m^n-1 是素数，则 $m=2$ 并且 n 是素数.

(ii) 设 p 是素数，记 $M_p=2^p-1$，这称为**梅森**(Merseme)**数**. 证明：如 p,q 是不同的素数，则 $(M_p,M_q)=1$.

注记　1644 年，法国数学家梅森研究过形如 $M_p=2^p-1$ 的素数，后来人们将这样的素数称为梅森素数，它们与所谓的偶完全数紧密相关(参考习题 3.18). 到 1996 年底，共找到了 34 个梅森素数. 是否有无穷多个梅森素数，这也是一个未解决的问题.

11. 设 a,b,c,d 是正整数，满足 $ab=cd$. 证明：$a^4+b^4+c^4+d^4$ 不是素数.

12*. 设 n 是正整数，对每个素数 p，我们用 $p^e\|n$ 表示 $p^e|n$ 但 $p^{e+1}\nmid n$. 设 $p^e\|n!$，证明

(i) $e=\sum_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$;

(ii) 如 n 的 p 进制表示中数码之和记为 $S_p(n)$（见习题 1.9），则 $e=\frac{n-S_p(n)}{p-1}$.

13*. 设 $a_1,\cdots,a_k$ 为正整数，证明 $\frac{(a_1+\cdots+a_k)!}{a_1!\cdots a_k!}$ 是整数.

14. 设 m,n 为正整数，证明 $\frac{(2m)!(2n)!}{m!n!(m+n)!}$ 是整数.

15. 设 a,b 是整数，$a\neq b$，n 是正整数. 如果 $n|(a^n-b^n)$，则 $n|\frac{a^n-b^n}{a-b}$.

16*. 设 $n\geqslant 1$. 证明

(i) n 为完全平方数的充分必要条件是 $\tau(n)$ 为奇数；

(ii) $\tau(n)\leqslant 2\sqrt{n}+1$;

(iii) n 的正约数之积等于 $n^{\frac{\tau(n)}{2}}$.

17. 证明：(i) $(a,[b,c])=[(a,b),(a,c)]$;

(ii) $[a,(b,c)]=([a,b],[a,c])$.

18*. 正整数 n 称为**完全数**，如果 $\sigma(n)=2n$. 证明：偶数 n 为完全数的充分必要条件是 $n=2^{k-1}(2^k-1)$，且 2^k-1 是素数.

19. 证明：(i) $1+\frac{1}{2}+\cdots+\frac{1}{n}$ 不是整数 $(n>1)$;

(ii) $1+\frac{1}{3}+\cdots+\frac{1}{2n+1}$ 不是整数 $(n>1)$.

第二章　同　　余

§4.　同余式与同余类

设 m 是非零整数，a 和 b 是整数. 如 $m|(a-b)$，则称 a 和 b **模 m 同余**(或 a **模** m **同余于** b)，记作

$$a \equiv b \pmod{m}; \tag{1}$$

如果 $m\nmid(a-b)$，则称 a 和 b **模 m 不同余**，记作

$$a \not\equiv b \pmod{m}.$$

关系式(1)称为(模 m 的) **同余式**.

容易看出，a 与 b 模 m 同余的充分必要条件是 a 与 b 被 m 除得相同的余数. 由于同余式(1)等价于 $a \equiv b(\mathrm{mod}\ (-m))$，故我们可以只考虑 m 为正整数的情形.

对于固定的模 m，同余式与通常的等式有许多类似的性质.

定理 1　同余关系是等价关系，即有

(i)(**自返性**)　$a \equiv a(\mathrm{mod}\ m)$;

(ii)(**对称性**)　如果 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$;

(iii)(**传递性**)　如果 $a \equiv b \pmod{m}$，$b \equiv c(\mathrm{mod}\ m)$，则

$$a \equiv c \pmod{m}.$$

证明　(i) 和(ii) 均是显然的，对于(iii)，由已知及定义，我们有 $m|(a-b)$ 及 $m|(b-c)$. 从而 $m|(a-b)+(b-c)$，即 $m|(a-c)$，因此 $a \equiv c \pmod{m}$.

定理 2　如果 $a \equiv b \pmod{m}$，$c \equiv d \pmod{m}$，则

(i) $a \pm c \equiv b \pm d \pmod{m}$；

(ii) $ac \equiv bd \pmod{m}$.

证明　(i) 是显然的. (ii) 可以从等式

$$ac - bd = a(c - d) + d(a - b)$$

及已知条件推出来.

反复用定理 1 和定理 2 可推出下面的一般结果.

定理 3　设 $F(x_1, \cdots, x_n)$ 是 n 元整数系数多项式(见引言). 如 $a_i \equiv b_i \pmod{m}$ $(1 \leqslant i \leqslant n)$，则

$$F(a_1, \cdots, a_n) \equiv F(b_1, \cdots, b_n) \pmod{m}.$$

下面的定理 4 可看作同余式中的消去律(这是复数中消去律的类似).

定理 4　若

$$ac \equiv bc \pmod{m}. \tag{2}$$

则 $a \equiv b \pmod{\frac{m}{(c,m)}}$. 特别地，当 $(c,m) = 1$ 时，我们有

$$a \equiv b \pmod{m}.$$

证明　由(2) 知 $m \mid c(a - b)$，这等价于

$$\frac{m}{(c,m)} \Big| \frac{c}{(c,m)} (a - b).$$

由 §2，定理 3(iv)及(vi)得出 $\frac{m}{(c,m)} \Big| (a - b)$.

现在提及几个涉及模的简单但有用的性质.

定理 5　(i) 如 $a \equiv b \pmod{m}$，$d \mid m$，则 $a \equiv b \pmod{d}$；

(ii) 如 $a \equiv b \pmod{m}$，$d \neq 0$，则 $da \equiv db \pmod{dm}$. 反之亦然；

(iii) 如 $a \equiv b \pmod{m_i}$ $(1 \leqslant i \leqslant n)$，则 $a \equiv b \pmod{[m_1, \cdots, m_n]}$；反之亦然.

证明　(i)，(ii)均是显然的. (iii)的两个方面可分别由(i)及 § 2，定理 4(i)推出来.

设 m 是一个固定的正整数. 由于“模 m 同余”是整数集上的一个等价关系(定理 .)，由此可以将整数按模 m 是否同余分为若干个两两不相交的类，使得同一个类中的任意两个数模 m 同余，而不同类中的两个数模 m 不同余；每一个这样的类称为**模 m 的同余类**. 我们将整数 a 所属的模 m 的同余类记作 $\bar{a} \pmod{m}$，在不引起混淆时可简记为 $\bar{a}$，它由所有模 m 同余于 a 的整数组成，即

$$\bar{a} = \{n \mid n \in \mathbf{Z},\ n \equiv a \pmod{m}\},$$

a 称为它的一个**代表元**. 容易得知，当 $a \equiv b \pmod{m}$ 时有 $\bar{a} = \bar{b}$；否则 $\bar{a}$ 与 $\bar{b}$ 不相交(即没有公共元素).

由带余除法，任一整数必与 $0, 1, \cdots, m-1$ 中的一个模 m 同余，而 $0, 1, \cdots, m-1$ 彼此模 m 不同余. 因此，模 m 恰有 m 个不同的同余类，它们是 $\bar{0}, \bar{1}, \cdots, \overline{m-1}$. 我们用 $\mathbf{Z}_m$ 表示这 m 个类的集合. (一个类看作一个元素！)

例如，模 2 的同余类共有两个：$\bar{0}, \bar{1}$，前者是全体偶数之集，后者则是所有奇数之集.

如果 $(a, m) = 1$，则由 § 2，定理 1(iv) 易知，同余类 $\bar{a}$ 中每个整数也均与 m 互素，这样的同余类称为模 m 的**缩同余类**. 换句话说，$\bar{a}$ 是(模 m) 缩同余类指的是 $(a, m) = 1$. 我们用 $\mathbf{Z}_m^*$ 表示模 m 的缩同余类组成的集合，其元素个数记作 $\varphi(m)$，称为**欧拉函数**，这是初等数论中一个重要的函数. 显然，$\varphi(1) = 1$，而对 $m > 1$，$\varphi(m)$ 即为 $1, 2, \cdots,$

$m-1$ 中与 m 互素的数的个数.

例如,若 p 是素数,则模 p 共有 $p-1$ 个缩同余类:$\bar{1},\bar{2},\cdots,\overline{p-1}$,从而 $\varphi(p)=p-1$.

m 个整数 $c_1,\cdots,c_m$ 称为**模 m 的完全剩余系**,简称为模 m 的**完系**,是指 $c_1,\cdots,c_m$ 彼此模 m 不同余. 数 $0,1,\cdots,m-1$ 则称为模 m 的**最小非负完系**.

$\varphi(m)$ 个整数 $r_1,\cdots,r_{\varphi(m)}$ 称为**模 m 的缩剩余系**,简称为**缩系**,是指它们彼此模 m 不同余,且均与 m 互素. 不超过 m 且与 m 互素的 $\varphi(m)$ 个正整数则叫作模 m 的**最小正缩系**.

于是,$c_1,\cdots,c_m$ 为模 m 的完系,等价于说 $\bar{c}_1,\cdots,\bar{c}_m$ 恰好是模 m 的全部 m 个同余类;而 $r_1,\cdots,r_{\varphi(m)}$ 是模 m 的缩系,则等价于说 $\bar{r}_1,\cdots,\bar{r}_{\varphi(m)}$ 恰好是模 m 的全部 $\varphi(m)$ 个缩同余类. 因此,任意两个完(缩)系中的数,将其中一个的顺序适当调整,必然两两模 m 同余.

定理 6　设 $(a,m)=1$,b 是任意整数.

(i) 如 $c_1,\cdots,c_m$ 是模 m 的完系,则 $ac_1+b,\cdots,ac_m+b$ 也是模 m 的完系;

(ii) 如 $r_1,\cdots,r_{\varphi(m)}$ 是模 m 的缩系,则 $ar_1,\cdots,ar_{\varphi(m)}$ 也是模 m 的缩系;

(iii) 存在 x 使 $ax\equiv b(\mathrm{mod}\ m)$ 成立,所有这样的 x 形成模 m 的一个同余类.

证明　(i) $ac_1+b,\cdots,ac_m+b$ 共 m 个数,其中任两数模 m 不同余. 因假如

$$ac_i+b\equiv ac_j+b(\mathrm{mod}\ m),$$

则有 $ac_i\equiv ac_j(\mathrm{mod}\ m)$. 由于 $(a,m)=1$,故 $c_i\equiv c_j(\mathrm{mod}\ m)$(定理 4),这就证明了结论.

(ii) 由(i)可特别地推出,$\varphi(m)$ 个数 $ar_1,\cdots,ar_{\varphi(m)}$ 中任两个模 m 不同余,又它们均与 m 互素(§2,定理 3(v)),因此(按定义)它们是模 m

的一个缩系.

(iii) 任取模 m 的一个完系 $c_1,\cdots,c_m$,由(i),$ac_1-b,\cdots,ac_m-b$ 是模 m 的完系.特别地,有某个 i 使 $ac_i-b\equiv 0(\mathrm{mod}\ m)$,即

$$ac_i\equiv b(\mathrm{mod}\ m).$$

如果 x,x' 满足 $ax\equiv b(\mathrm{mod}\ m)$, $ax'\equiv b(\mathrm{mod}\ m)$, 则

$$ax\equiv ax'(\mathrm{mod}\ m),$$

所以 $x\equiv x'(\mathrm{mod}\ m)$(见(i)中论证),即 x 与 x' 属于模 m 的同一个同余类.

由定理 6(iii) 推出,如 $(a,m)=1$,则存在 x 使

$$ax\equiv 1\ (\mathrm{mod}\ m).$$

我们将这样的 x 称为 a **对模 m 的逆**,记作 $a^{-1}(\mathrm{mod}\ m)$ 或 a^{-1},它们形成模 m 的一个同余类(从而在模 m 的意义下唯一).特别地,有一个 a^{-1} 满足 $1\leqslant a^{-1}<m$.

定理 7　设 $(a,m)=(b,m)=1$,则

(i) $(ab)^{-1}\equiv a^{-1}\cdot b^{-1}(\mathrm{mod}\ m)$;

(ii) $a^{-1}\equiv b^{-1}(\mathrm{mod}\ m)$ 的充分必要条件是 $a\equiv b(\mathrm{mod}\ m)$;

(iii) 如果 $r_1,\cdots,r_{\varphi(m)}$ 是模 m 的任一缩系,则它们的逆 $r_1^{-1},\cdots,r_{\varphi(m)}^{-1}$ 也是模 m 的一个缩系.

证明　(i) 与(ii) 均是定义的直接推论;(iii) 可由(ii) 导出来.

例 1　求满足 $24x\equiv 7\ (\mathrm{mod}\ 59)$ 的所有 x.

解　由于 $(24,59)=1$,从而

$$\begin{aligned}x&\equiv\frac{7}{24}\equiv\frac{7+59}{24}\equiv\frac{66}{24}\equiv\frac{11}{4}\equiv\frac{-48}{4}\\&\equiv-12\ (\mathrm{mod}\ 59).\end{aligned}$$

例 2　设 p 是素数，$p \geqslant 5$，则

$$\sum_{i=1}^{p-1} \frac{1}{i^2} \equiv 0 \pmod{p}. \tag{3}$$

证明　对任意与 p 互素的整数 a，由定理 6(ii)，$a, 2a, \cdots, (p-1)a$ 是模 p 的缩系，故(参考定理 7(iii))

$$\sum_{i=1}^{p-1}\left(\frac{1}{i}\right)^2 \equiv \sum_{i=1}^{p-1}\left(\frac{1}{ai}\right)^2 \pmod{p},$$

即

$$\left(\frac{1}{a^2}-1\right)\sum_{i=1}^{p-1}\frac{1}{i^2} \equiv 0 \pmod{p}. \tag{4}$$

因为 $a^2 \equiv 1 \pmod{p}$ 意味着 $a \equiv \pm 1 \pmod{p}$；故对 $p \geqslant 5$，必存在 a 使 $p \nmid a$ 且 $p \nmid \left(\frac{1}{a^2}-1\right)$. 对这样选择的 a，由(4) 推出(3) 成立.

(3) 也可采用更直接的证明：因 $1, \frac{1}{2}, \cdots, \frac{1}{p-1}$ 是模 p 的一个缩系，从而(对 $p \geqslant 5$)

$$\sum_{i=1}^{p-1}\left(\frac{1}{i}\right)^2 \equiv \sum_{i=1}^{p-1} i^2 = \frac{1}{6}\,p(p-1)(2p-1) \equiv 0 \pmod{p}.$$

习　题　4

1*. 证明：连续 n 个整数中恰有一个被 n 整除.

2*. 对正整数 n，记 $S(n)$ 为其十进制表示中的数码之和；$T(n)$ 为其数码的正负交错和. 例如

$$S(123) = 1+2+3 = 6;\ T(123) = 1-2+3 = 2.$$

证明

$$S(n) \equiv n \pmod{9} \quad 及 \quad T(n) \equiv n \pmod{11}.$$

3*. (i) 证明:完全平方数模 3 同余于 0 或 1;模 4 同余于 0 或 1;模 5 同余于 0,1 或 4.

(ii) 证明:完全立方数模 9 同余于 0 或 ± 1;整数的四次幂模 16 同余于 0 或 1.

4*. 设 a 是奇数,n 为正整数,证明

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}.$$

5*. (i) 证明:当 $n \geqslant 3$ 时,$\varphi(n)$ 是偶数;

(ii) 证明:当 $n \geqslant 2$ 时,不超过 n 且与 n 互素的正整数之和是 $\frac{1}{2}n\varphi(n)$.

6. 设 n 为偶数,$a_1,\cdots,a_n$ 及 $b_1,\cdots,b_n$ 都是模 n 的完系,则 $a_1+b_1,\cdots,a_n+b_n$ 不是模 n 的完系.

7. 设 m,n 都是正整数,$m=nt$. 则模 n 的任一个同余类

$$\{x \in \mathbf{Z} \mid x \equiv r \pmod{n}\}$$

可表示为 t 个模 m 的(两两不同的)同余类

$$\{x \in \mathbf{Z} \mid x \equiv r+in \pmod{m}\}\ (i=0,1,\cdots,t-1)$$

之并.

8. 设 $f(x)=a_nx^n+\cdots+a_1x+a_0$, $n>0$, $a_i(1 \leqslant i \leqslant n)$ 是整数,且 $a_n>0$. 证明:$f(n)(n=1,2,\cdots)$ 中有无穷多个合数.

9*. 设 $1 \leqslant k \leqslant p-1$ 是素数,则 $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$.

10. 设 p 是素数,证明:$\binom{n}{p} \equiv \left[\frac{n}{p}\right] \pmod{p}$.

11. 设 a,b 是整数,$a+b \neq 0$ 且 $(a,b)=1$; p 是素数. 证明:$\left(a+b, \frac{a^p+b^p}{a+b}\right)=1$ 或 p.

12. 设 a,b 为整数,n 是正整数,证明

$$n! \mid b^{n-1}a(a+b)(a+2b)\cdots(a+(n-1)b).$$

13. 用例 1 的方法求满足下面同余式的 x:

(i) $8x \equiv 5 \pmod{23}$;

(ii) $60x \equiv 7 \pmod{37}$.

§5. 同余类的运算

设 $m > 1$ 是一个固定的正整数,现在我们定义 $\mathbf{Z}_m$ 中的运算.

设 $\bar{a}, \bar{b} \in \mathbf{Z}_m$,我们将模 m 的同余类 $\overline{a+b}$ 称为同余类 $\bar{a}$ 与 $\bar{b}$ 之和,表示成

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

如果我们在 $\bar{a}, \bar{b}$ 中分别取另外两个元素 a', b',则 $a \equiv a' \pmod{m}$, $b \equiv b' \pmod{m}$. 从而

$$a + b \equiv a' + b' \pmod{m} (\S 4, \text{定理 } 2(\text{i})),$$

于是 $\overline{a+b} = \overline{a'+b'}$. 这表明,同余类 $\overline{a+b}$ 与我们对 $\bar{a}, \bar{b}$ 的代表元的选取无关,即上面定义的和 $\bar{a} + \bar{b}$ 是(由同余类 $\bar{a}, \bar{b}$) 唯一确定的.

容易验证,如上定义的 $\mathbf{Z}_m$ 中的加法运算与复数中的加法运算一样,满足(通常的) 结合律与交换律. 又同余类 $\bar{0}$ 具有这样的性质:对任意 $\bar{a} \in \mathbf{Z}_m, \bar{0} + \bar{a} = \bar{a}$;并且方程 $\bar{x} + \bar{a} = \bar{0}$ 在 $\mathbf{Z}_m$ 中有唯一的解

$$\bar{x} = \overline{-a}.$$

因此,同余类 $\bar{0}$ 在 $\mathbf{Z}_m$ 的加法运算中所起的作用,相当于复数中的数 0 在加法中所起的作用. 我们通常将 $\bar{0}$ 称为 $\mathbf{Z}_m$ **中的(加法) 零元**,而将 $\overline{-a}$ 称作 a 的(**加法**) **逆元**,并记作 $-\bar{a}$. 于是,对任意 $\bar{a}, \bar{b} \in \mathbf{Z}_m$,方程 $\bar{x} + \bar{a} = \bar{b}$ 有唯一的解

$$\bar{x} = \bar{b} - \bar{a}.$$

所以,$\mathbf{Z}_m$ 中可以作加法的逆运算 —— 减法. 在代数学中,具有上面性质的集合叫作(交换) 群. 于是 $\mathbf{Z}_m$ 对于加法形成一个群,叫做**模 m 的加法群**,这是由 m 个元素构成的有限群.

除了加、减法运算外，$\mathbf{Z}_m$ 中还可作乘法. 设 $\bar{a},\bar{b}\in\mathbf{Z}_m$，我们将模 m 的同余类 $\overline{ab}$ 称为同余类 $\bar{a}$ 与 $\bar{b}$ 的积，表示成

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

与上面类似地可知，$\bar{a}\cdot\bar{b}$ 是不依赖于 $\bar{a},\bar{b}$ 中代表元的选取而唯一确定的.

此外，易于验证，$\mathbf{Z}_m$ 中的乘法运算也与复数中的乘法一样，满足结合律与交换律；并且，乘法与加法还满足分配律. 而同余类 $\bar{1}$ 则相当于复数中数 1 的作用：对任意 $\bar{a}\in\mathbf{Z}_m$，$\bar{1}\cdot\bar{a}=\bar{a}$. 我们因此将 $\bar{1}$ 称为 **$\mathbf{Z}_m$ 中的(乘法) 单位**. 代数学中，满足上述(加、减、乘法) 三种运算和运算律的集合叫作交换环. 我们熟悉的复数集合，实数集合，有理数集合和整数集合都是环，这些环均具有无限多个元素. 而现在我们给出了有限环的例子：模 m 的 m 个同余类组成的集合，叫作**模 m 的同余类环**.

对于乘法，我们前面已提到过，$\mathbf{Z}_m$ 中乘法单位 $\bar{1}$ 类似于复数中的数 1. 在复数中，每个非零元都有乘法逆，即任给 $\alpha\in\mathbf{C},\alpha\neq 0$，方程 $x\alpha=1$ 有唯一的解 $x\in\mathbf{C}$. 但在 $\mathbf{Z}_m$ 中，方程 $\bar{x}\cdot\bar{a}=\bar{1}$ 并非对每个 $\bar{a}\in\mathbf{Z}_m(\bar{a}\neq\bar{0})$ 有解，即 $\bar{a}$ 在 $\mathbf{Z}_m$ 中不一定总有乘法逆. 例如，在 $\mathbf{Z}_6$ 中就不存在 $\bar{x}$，使 $\bar{2}\cdot\bar{x}=\bar{1}$(因这意味着 $2x\equiv 1\pmod 6$，显然不可能).

$\mathbf{Z}_6$ 中的元素 $\bar{2}$ 没有逆的原因，在于它是 $\mathbf{Z}_6$ 中的所谓零因子. 一般地，$\mathbf{Z}_m$ 中的元素 $\bar{x}$ 称为 $\mathbf{Z}_m$ 中的**零因子**，是指 $\bar{x}\neq\bar{0}$，但存在 $\bar{y}\in\mathbf{Z}_m$，$\bar{y}\neq\bar{0}$ 使 $\bar{x}\cdot\bar{y}=\bar{0}$.(对称地，$\bar{y}$ 也是 $\mathbf{Z}_m$ 中的零因子.) 如果 $\bar{x}$ 是 $\mathbf{Z}_m$ 中的零因子，则 $\bar{x}$ 在 $\mathbf{Z}_m$ 中便不可能有乘法逆. 因如果存在 $\bar{z}$ 使 $\bar{x}\cdot\bar{z}=\bar{1}$，又设 $\bar{y}\neq\bar{0}$ 使 $\bar{x}\cdot\bar{y}=\bar{0}$，则产生

$$\bar{y}=(\bar{x}\cdot\bar{z})\cdot\bar{y}=(\bar{x}\cdot\bar{y})\cdot\bar{z}=\bar{0}\cdot\bar{z}=\bar{0}.$$

然而，不难验证，模 m 的 $\varphi(m)$ 个缩同余类构成的集合 $\mathbf{Z}_m^*$ **形成(交换的) 乘法群**.

首先，两个缩同余类之积仍是缩同余类(§ 2，定理 3(v))，即 $\mathbf{Z}_m^*$ 对乘法封闭. 此外，$\mathbf{Z}_m^*$ 是 $\mathbf{Z}_m$ 的子集，故在 $\mathbf{Z}_m^*$ 中乘法仍满足结合律与交换

律；而同余类 $\bar{1}$ 显然是 $\mathbf{Z}_m^*$ 中的乘法单位. 最后，由 §4，定理 6(iii) 推出，对每个 $\bar{a} \in \mathbf{Z}_m^*$，方程 $\bar{x} \cdot \bar{a} = \bar{1}$ 有唯一的解

$$\bar{x} = \overline{a^{-1}},$$

称为 $\bar{a}$ 的(**乘法**) **逆元**($\bar{a}$ 与 $\overline{a^{-1}}$ 显然是互逆的). 我们将 $\overline{a^{-1}}$ 记作 $\bar{a}^{-1}$，于是，对任意 $\bar{a}, \bar{b} \in \mathbf{Z}_m^*$，方程 $\bar{a} \cdot \bar{x} = \bar{b}$ 有唯一的解

$$\bar{x} = \bar{b} \cdot \bar{a}^{-1}\left(\text{也可写成} \frac{\bar{b}}{\bar{a}}\right).$$

换句话说，只有模 m 的缩同余类才可以作“分母”. 于是，在 $\mathbf{Z}_m^*$ 中可以作除法运算. 特别当 m 为素数 p 时，$\mathbf{Z}_p$ 中除 $\bar{0}$ 之外，其它 $p-1$ 个同余类均是缩同余类，因此其中可以作加、减、乘、除四则运算(当然 $\bar{0}$ 不能作为分母)，这样的集合叫作域. 我们熟悉的复数集合，实数集合及有理数集合都是域，它们均具有无穷多个元素. 现在我们对于每个素数 p，给出了由**模 p 的 p 个同余类构成的有限域**.

另一方面，对 $m > 1$，只有当 m 是素数时，模 m 的剩余类环才能是域. 这是因为，若 m 不是素数，则 m 有正约数 d，$1 < d < m$. 显然 $\bar{d}$ 及 $\frac{\overline{m}}{d}$ 都不是 $\mathbf{Z}_m$ 中的零元，但 $\bar{d} \cdot \frac{\overline{m}}{d} = \overline{m} = \bar{0}$，即 $\mathbf{Z}_m$ 中有零因子，因此 $\mathbf{Z}_m$ 中非零元之集对乘法不形成群，从而 $\mathbf{Z}_m$ 不是域.

对素数 p，我们通常用 $\mathbf{F}_p$ 表示由模 p 的 p 个同余类构成的域.

例 1　设 p 是素数，则 $(p-1)! \equiv -1 \pmod{p}$.

证明　$p = 2$ 时结论显然成立. 设 $p \geqslant 3$，由于对模 p 的任一缩同余类 $\bar{a}$，存在唯一的(逆) $\bar{a}^{-1}$，满足

$$\bar{a} \cdot \bar{a}^{-1} = \bar{1};$$

而 $\bar{a} = \bar{a}^{-1}$ 等价于 $\bar{a}^2 = \bar{1}$，即 $\bar{a} = 1$ 或 $\overline{p-1}$. 于是 $p-3$ 个同余类 $\bar{2}, \bar{3}, \cdots, \overline{p-2}$ 可按互逆配成 $\frac{p-3}{2}$ 个对. 因此

$$\overline{(p-1)!}=\bar{1}\cdot\bar{2}\cdot\cdots\cdot\overline{(p-2)}\cdot\overline{(p-1)}$$
$$=\overline{p-1}=\overline{-1}.$$

这就是 $(p-1)!\equiv -1 \pmod{p}$.

注记　1. 上面的论证，不难改换成同余式的记号来表述. 我们强调一下，整数的“$\equiv \pmod{m}$”与 $\mathbf{Z}_m$ 中同余类的“$=$”是一回事.

许多问题，以同余类的观点作的论证，往往更能揭示其实质，这一点在学习了群论后将看得很清楚. 但限于本书的目的，我们在大多数场合下仍采用同余式的语言，有兴趣的读者可以将它们换成同余类的说法.

2. 例 1 的结论，通常称为**威尔逊**(Wilson)**定理**，其一个引人注目之处在于，如果 $p>1$ 满足例 1 中的同余式，则 p 必是素数. 事实上，如果 p 有素因子 $q\leqslant p-1$，则 $q\mid(p-1)!$，从而易知 $q\mid 1$，矛盾！

习　题　5

1. 列出 $\mathbf{Z}_6$ 中的加法表与乘法表.

2. 列出 $\mathbf{F}_7$ 中的加法与乘法表.

3. 设 m 是整数，$m>1$，确定 $\mathbf{Z}_m$ 中零因子的个数.

4*. 设 m 是整数，$m>1$. 证明：在 $\mathbf{Z}_m^*$ 中乘法的消去律成立，即设 $\bar{a},\bar{b},\bar{c}\in\mathbf{Z}_m^*$，$\bar{a}\cdot\bar{b}=\bar{a}\cdot\bar{c}$，则 $\bar{b}=\bar{c}$.

5*. 设 m 是整数，$m>1$. 证明：$\mathbf{Z}_m^*$ 中任一元与 $\mathbf{Z}_m^*$ 中所有元的积，恰给出 $\mathbf{Z}_m^*$.

6. 用同余类的语言重述 §4，定理 7.

7*. 设 p 是素数，

(i) 如果 $\bar{a}\in\mathbf{F}_p$，则 $p\bar{a}=\underbrace{\bar{a}+\cdots\bar{a}}_{p\text{个}}=\bar{0}$；

(ii) 设 n 是整数，$\bar{a}\in\mathbf{F}_p$，$\bar{a}\neq\bar{0}$. 若 $n\bar{a}=\bar{0}$，则 $p\mid n$.

8. 设 p 为奇素数，证明

(i) $1^2 \cdot 3^2 \cdot \cdots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$；

(ii) $2^2 \cdot 4^2 \cdot \cdots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$.

9. 设 p 是素数，$r_1, \cdots, r_{p-1}$ 与 $r_1', \cdots, r_{p-1}'$ 是模 p 的两个缩系，证明：$r_1 r_1', \cdots, r_{p-1} r_{p-1}'$ 不是模 p 的缩系.

§6. 欧拉—费马定理

本节讲述初等数论中几个重要的定理.

我们首先给出关于欧拉函数 $\varphi(n)$ 的基本结果.

定理 1　(i) 欧拉函数 $\varphi(n)$ 是积性的，即如果 $(m,n)=1$，则有

$$\varphi(mn) = \varphi(m)\varphi(n);$$

(ii) 设 $n \geqslant 2$，$n = p_1^{a_1} \cdots p_k^{a_k}$ 是 n 的标准分解，则

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right);$$

(iii) 设 n 是正整数，则

$$\sum_{d \mid n} \varphi(d) = n,$$

其中求和表示 d 通过 n 的所有正约数.

证明　(i) 设 $1, \alpha, \cdots, \gamma$ 是不超过 m 且与 m 互素的正整数. 则不超过 mn 且与 m 互素的正整数是

$$\begin{array}{cccc} 1 & \alpha & \cdots & \gamma \\ m+1 & m+\alpha & \cdots & m+\gamma \\ \vdots & \vdots & \vdots & \vdots \\ (n-1)m+1 & (n-1)m+\alpha & \cdots & (n-1)m+\gamma \end{array}$$

数表中同一列中的数在模 m 的同一个剩余类中. 因 $(m,n)=1$，由 §4，

定理 6(i) 知，每一列中的 n 个数恰构成模 n 的一个完系，从而其中恰包含 $\varphi(n)$ 个数与 n 互素. 因共有 $\varphi(m)$ 列，因此，共有 $\varphi(m)\varphi(n)$ 个小于 mn 的正整数既与 m 互素，又与 n 互素，从而与 mn 互素. 于是

$$\varphi(mn) = \varphi(m)\varphi(n).$$

(ii) 由(i) 及归纳法知，如 $n_1,\cdots,n_k$ 两两互素，则

$$\varphi(n_1\cdots n_k) = \varphi(n_1)\cdots\varphi(n_k).$$

因此，$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{a_i})$. 于是问题化归为计算 $\varphi(p^\alpha)$(p 为素数，$\alpha \geqslant 1$).

因 p 是素数，故对每个整数 m，或者 $p|m$ 或者 $(p^\alpha, m) = 1$. 而在 $1,\cdots,p^\alpha$ 中，被 p 整除的数共有 $\frac{p^\alpha}{p} = p^{\alpha-1}$ 个，所以其中与 p^α 互素的共有 $p^\alpha - p^{\alpha-1}$ 个，即

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

因此

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{a_i} - p_i^{a_i-1}) = \prod_{i=1}^{k} p_i^{a_i}(1 - \frac{1}{p_i})$$

$$= n\prod_{i=1}^{k} (1 - \frac{1}{p_i}).$$

(iii) 设 $n = p_1^{a_1}\cdots p_k^{a_k}$ 是 n 的标准分解，则 n 的每个正约数 d 均唯一地表示为 $d = p_1^{\beta_1}\cdots p_k^{\beta_k}$，其中 $0 \leqslant \beta_i \leqslant a_i (1 \leqslant i \leqslant k)$(§3，定理 3 的推论 1). 故由(i)及(ii)，我们有

$$\sum_{d|n} \varphi(d) = \sum_{0\leqslant\beta_i\leqslant a_i} \varphi(p_1^{\beta_1}\cdots p_k^{\beta_k})$$

$$= \sum_{0\leqslant\beta_i\leqslant a_i} \varphi(p_1^{\beta_1})\cdots\varphi(p_k^{\beta_k})$$

$$= \prod_{i=1}^{k} \sum_{0\leqslant\beta_i\leqslant a_i} \varphi(p_i^{\beta_i})$$

$$= \prod_{i=1}^{k} (1 + (p_i - 1) + \cdots + (p_i^{a_i} - p_i^{a_i-1}))$$

$$= \prod_{i=1}^{k} p_i^{q_i} = n.$$

定理 2(欧拉定理)　设 m 为正整数,a 为整数且$(a,m) = 1$,则

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

证明　设模 m 的缩同余类是$\bar{r}_1,\cdots,\bar{r}_{\varphi(m)}$,则$\bar{a}\cdot\bar{r}_1,\cdots,\bar{a}\cdot\bar{r}_{\varphi(m)}$也是模 m 的缩同余类.因此(参考习题 5.5)

$$\bar{r}_1\cdots\bar{r}_{\varphi(m)} = (\bar{a}\cdot\bar{r}_1)\cdots(\bar{a}\cdot\bar{r}_{\varphi(m)}),$$

即

$$\bar{r}_1\cdots\bar{r}_{\varphi(m)} = \bar{a}^{\varphi(m)}(\bar{r}_1\cdots\bar{r}_{\varphi(m)}).$$

故$\bar{a}^{\varphi(m)} = \bar{1}$(习题 5.4),这就是 $a^{\varphi(m)} \equiv 1\ (\mathrm{mod}\ m)$.

在定理 2 中取 m 为素数 p,由于 $\varphi(p) = p - 1$,我们得到

定理 3(费马定理)　设 p 是素数,a 为整数且 $p\nmid a$,则

$$a^{p-1} \equiv 1\ (\mathrm{mod}\ p). \tag{1}$$

费马定理等价于下面更便利的

定理 3′　设 p 是素数,则对任意整数 a,有

$$a^p \equiv a(\mathrm{mod}\ p) \tag{2}$$

实际上,当 $p\nmid a$ 时,(1) 与(2) 是等价的;而当 $p|a$ 时,(2) 显然成立.因此定理 3 与定理 3′ 是等价的.

基于不同的想法,定理 3′(从而定理 3) 有许多种不同的直接证明,我们在此提及其中一个.

引理　设 p 是素数，则对 $1 \leqslant k \leqslant p-1$，二项式系数 $\binom{p}{k}$ 均被 p 整除.

证明　由于

$$k\binom{p}{k} = p\binom{p-1}{k-1},$$

故 $p \mid k\binom{p}{k}$. 但 $1 \leqslant k \leqslant p-1$，从而 $p \nmid k$，因此 $p \mid \binom{p}{k}$.

定理 3′ 的证明　由于当 $a \equiv b \pmod{p}$ 时

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

这表明，同余式(2)仅依赖于 a 模 p 的余数. 因此我们只需对 $a = 0, 1, \cdots, p-1$ 证明(2).

对 a 归纳. 当 $a = 0$ 时，(2) 显然成立. 假设(2) 对于 a 已成立 $(0 \leqslant a \leqslant p-2)$，则由二项式定理，上述引理及归纳假设，我们有

$$\begin{aligned}(a+1)^p &\equiv a^p + \sum_{k=1}^{p-1}\binom{p}{k}a^k + 1 \\ &\equiv a^p + 1 \equiv a + 1 \pmod{p}.\end{aligned}$$

从而(2)对 $a+1$ 也成立. 证毕.

另一方面，由定理 3 及 $\varphi(m)$ 的计算公式(定理 1(ii)) 也能证明定理 2. 因此，定理 2 与定理 3 实际上是等价的.

定理 2 的另一证明　设 $m = p_1^{a_1}\cdots p_k^{a_k}$ 是 m 的标准分解. 由 §4，定理 5(iii)，我们只需证明，对 $1 \leqslant i \leqslant k$，

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

但

$$\varphi(m) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1).$$

因此,这只需对素数 p 及整数 $\alpha \geqslant 1$,证明

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^{\alpha}} \tag{3}$$

(§4,定理 2(ii)).现在我们用归纳法证明同余式(3)成立.当 $\alpha = 1$ 时,这就是定理 3(我们已作出其直接证明).设(3) 对于 α 已成立,即

$$a^{p^{\alpha-1}(p-1)} = 1 + p^{\alpha} x,$$

其中 x 是一个整数.则由二项式定理得知

$$a^{p^{\alpha}(p-1)} \equiv (1 + p^{\alpha} x)^{p} \equiv 1 \pmod{p^{\alpha+1}},$$

这就证明了(3)对 $\alpha \geqslant 1$ 均成立.

我们注意,由上面的证明可见,如记 $l(m) = [\varphi(p_1^{\alpha_1}), \cdots, \varphi(p_k^{\alpha_k})]$,则当 $(a,m) = 1$ 时有

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

这一结果往往比欧拉定理强(参考 §8).

习 题 6

1. 计算 $\varphi(360), \varphi(429)$.

2. 求 3^{400}(十进制表示中) 的末两位数码.

3. 设整数 $n \geqslant 3$,分别用欧拉定理和 $\varphi(n)$ 的公式,证明 $\varphi(n)$ 为偶数.

4. 设 m,n 为正整数,$(m,n) = 1$. 证明:

$$m^{\varphi(n)} + n^{\varphi(m)} \equiv 1 \pmod{mn}.$$

5. 设 $(a,10) = 1$,证明:$a^{20} \equiv 1 \pmod{100}$.

6. 设 $m > 1, \bar{a} \in \mathbf{Z}_m^*$,用欧拉定理给出 $\bar{a}$ 的逆.

7*. 设 p 是素数,证明

(i) 对任意 $\alpha \in \mathbf{F}_p$,有 $\alpha^p = \alpha$;

(ii) 对任意 $\alpha,\beta \in \mathbf{F}_p$，有 $(\alpha+\beta)^p = \alpha^p + \beta^p$.

8*. 对 $n \geqslant 1$，**墨比乌斯**(Möbius) **函数** $\mu(n)$ 定义为

$$\mu(n) = \begin{cases} 1, & n = 1, \\ (-1)^r, & n = p_1 \cdots p_r, \\ 0, & \text{其他}, \end{cases}$$

其中 $p_1,\cdots,p_r$ 是互不相同的素数，

(i) 证明：$\mu(n)$ 是积性函数；

(ii) 证明：$\sum_{d|n} \mu(d) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$

9*. 设 $f(n)$ 为任一个数论函数. 证明

$$\sum_{\substack{x=1 \\ (x,n)=1}}^{n} f(x) = \sum_{d|n} \mu(d)\, S_d,$$

其中 $S_d = \sum_{l=1}^{n/d} f(dl)$.

10*. (**墨比乌斯反转公式**) 设 $f(n)$ 及 $F(n)$ 是两个数论函数，如果

$$F(n) = \sum_{d|n} f(d),$$

则

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right);$$

反之亦然.

11*. 设 $f(n), g(n)$ 是两个积性数论函数，则

$$H(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$$

也是积性函数.

12. 证明：$\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \frac{n}{\varphi(n)}$.

13. 用习题 6.9 证明：$\sum_{d|n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}$；并由此给出定理 1 中(i)和(iii)的不同证明.

§7. 同余方程(组)

对给定的正整数 m，及一个整系数多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \tag{1}$$

初等数论中一个基本课题是**模 m 的同余方程**

$$f(x) \equiv 0 \pmod{m} \tag{2}$$

的求解问题.

设 $x = c$ 时同余式(2)成立，则称 c 是**同余方程(2)的解**. 这时同余类 $\bar{c}$ 中所有数也是解(§4，定理 3)；我们将这些解视为相同的，并称同余类 $\bar{c}$ 是同余方程(2)的一个解，记作 $x \equiv c \pmod{m}$.

如果 c, c' 均为(2)的解，且模 m 不同余，则称它们是同余方程(2)的不同的解. 所有两两模 m 不同余的解的个数，称为同余方程(2)的**解数**. 因此，求同余方程(2)的解，只需在模 m 的任一完系(有限集!)中求解，这完系中解的个数就是(2)的解数. 于是同余方程(2)的解数不超过 m.

设 $f(x)$ 由(1)给出，如果 $m \mid (a_n, \cdots, a_0)$，则同余方程(2)恒成立(所有整数 x 都是解)，于是(2)有 m 个解.

当 $m \nmid (a_n, \cdots, a_0)$ 时，必有唯一的 $k(0 \leqslant k \leqslant n)$，满足 $m \mid a_i (k < i \leqslant n)$，但 $m \nmid a_k$. 此时，同余方程(2)与同余方程

$$a_k x^k + \cdots + a_1 x + a_0 \equiv 0 \pmod{m} \tag{3}$$

的解(及解数)相同. 我们称(2)与(3)等价的，并称(2)为 k **次同余方程**，也称 $f(x)$ 为**模 m 的 k 次多项式**. (注意，$f(x)$ 作为整系数多项式的次数，与 $f(x)$ 模 m 的次数是两个不同的概念；而当 $m \mid (a_n, \cdots, a_0)$ 时，我们不定义 $f(x)$ 模 m 的次数).

本节我们主要讨论一次同余方程(组)的求解.

定理 1　设 $(a, m) = d$，则一次同余方程

$$ax \equiv b(\mathrm{mod}\ m) \tag{4}$$

有解的充分必要条件是 $d|b$. 当此条件成立时,同余方程(4) 共有 d 个解,它们是

$$x \equiv x_0 + t \cdot \frac{m}{d} \pmod{m}, \quad t = 0, \cdots, d-1; \tag{5}$$

其中 x_0 是同余方程

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}} \tag{6}$$

的任一个解.

证明　设同余方程(4)有解 $x = c$, 则 $m|(ac - b)$, 从而 $d|(ac - b)$. 但 $d|a$,故 $d|b$.

反过来,如 $d|b$,则由 §4,定理 5(ii) 知,同余方程(4) 和(6) 等价. 因 $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$,故由 §4,定理 6(iii) 知,同余方程(6) 有解. 若 x_0 是(6) 的解,则同余方程(6) 的解,进而同余方程(4) 的解是模 $\frac{m}{d}$ 的一个同余类

$$x \equiv x_0 (\mathrm{mod}\ \frac{m}{d}). \tag{7}$$

最后,由习题 4.7 可知,满足(7)的所有 x 可表示为(5) 中 d 个模 m 的同余类之并.

对于一般的高于一次的同余方程,解的个数及求解问题将变得非常复杂和困难,本书不作深入讨论. 我们将在第四章中研究二次同余方程,在这里则只证明下面的简单但很有用的结果.

定理 2(拉格朗日(Lagrange))　设 p 是素数,令

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

是一个模 p 为 n 次的整系数多项式(即 $p \nmid a_n$), 则同余方程

$$f(x) \equiv 0 \pmod{p} \tag{8}$$

至多有 n 个解.

证明　我们对 n 归纳. 当 $n=1$ 时,同余方程(8)恰有一个解,故结论成立. 假设结论对于所有模 p 为 $n-1$ 次的多项式已成立. 如果方程(8)有 $n+1$ 个(模 p 互不同余的)解 $x_1,\cdots,x_{n+1}$. 令 $y=x-x_1$,则(8)变为等价的 n 次同余方程

$$a_n y^n + a_{n-1}' y^{n-1} + \cdots + a_1' y + a_0' \equiv 0 \pmod{p}, \tag{9}$$

其首项系数仍是 a_n,并且有 $n+1$ 个解

$$0, x_2 - x_1, \cdots, x_{n+1} - x_1.$$

因为 $y=0$ 适合(9),故 $a_0' \equiv 0 \pmod{p}$. 因此(9)可改写成

$$y(a_n y^{n-1} + a_{n-1}' y^{n-2} + \cdots + a_1') \equiv 0 \pmod{p}.$$

现在,n 个数 $x_2-x_1,\cdots,x_{n+1}-x_1$(均不被 p 整除)满足上述同余方程,故它们均满足 $n-1$ 次同余方程

$$a_n y^{n-1} + a_{n-1}' y^{n-2} + \cdots + a_1' \equiv 0 \pmod{p},$$

这与归纳假设矛盾!

注记　如果定理 2 中的素数 p 换成合数,则命题不必正确. 例如,模 8 的二次同余方程 $x^2 \equiv 1 \pmod 8$ 却有四个解:

$$x \equiv 1,3,5,7 \pmod 8.$$

现在我们讨论(一次)同余方程组. 同余方程组不一定总有解,即使其中每一个同余方程都有解. 例如,同余方程 $x \equiv 0 \pmod 2$ 及 $x \equiv 1 \pmod 4$ 都有解,但显然它们没有公共解. 这一例子中,两个同余方程的模(分别是 2 和 4)不互素. 我们将证明,如果若干个可解的一次同余方程的模两两互素,则它们必有公共解. 我们首先证明下面的基本结果.

定理 3(中国剩余定理)　设 $m_1,\cdots,m_k$ 是两两互素的正整数,则对

任意整数 $b_1,\cdots,b_k$，一次同余方程组

$$x \equiv b_1 (\mathrm{mod}\ m_1),\quad \cdots,\quad x \equiv b_k (\mathrm{mod}\ m_k) \tag{10}$$

必有解，且全部解是模 $m_1\cdots m_k$ 的一个同余类. 确切地说，同余方程组(10)的解是

$$x \equiv M_1 M_1^{-1} b_1 + \cdots + M_k M_k^{-1} b_k (\mathrm{mod}\ m_1\cdots m_k) \tag{11}$$

其中 M_i 及 $M_i^{-1}(1 \leqslant i \leqslant k)$ 由下面的条件决定：

$$m_1\cdots m_k = M_i m_i,\quad M_i M_i^{-1} \equiv 1 (\mathrm{mod}\ m_i).$$

证明　由条件知 $(m_i, M_i) = 1$，故有 M_i^{-1} 使 $M_i M_i^{-1} \equiv 1 (\mathrm{mod}\ m_i)$. 此外，对 $j \neq i$ 有 $m_j | M_i$，因此数 $d_i = M_i M_i^{-1}$ 满足

$$d_i \equiv 1 (\mathrm{mod}\ m_i),\quad d_i \equiv 0 (\mathrm{mod}\ m_j) \text{ 对 } j \neq i. \tag{12}$$

我们注意，同余方程组(12)是(10)的 k 种特殊情形. 易于验证，对 $1 \leqslant i \leqslant k$，(12) 的解的“叠加”(即线性组合)$b_1 d_1 + \cdots + b_k d_k$，满足同余方程组(10)，从而(11) 是(10) 的解.

另一方面，如果 x, x' 都是同余方程组(10)的解，则

$$x \equiv x' \ (\mathrm{mod}\ m_i),\quad 1 \leqslant i \leqslant k.$$

故 $x \equiv x' (\mathrm{mod}\ m_1\cdots m_k)$（§ 4，定理 5(iii) 及 § 2，定理 4(v)）. 因此原同余方程组的解是模 $m_1\cdots m_k$ 的一个同余类.

推论　设正整数 $m_1,\cdots,m_k$ 两两互素，则同余方程组

$$a_1 x \equiv b_1 (\mathrm{mod}\ m_1),\quad \cdots,\quad a_k x \equiv b_k (\mathrm{mod}\ m_k)$$

有解的充分必要条件是每一个同余方程 $a_i x \equiv b_i (\mathrm{mod}\ m_i)$ 均可解.

证明　所说的条件显然是必要的. 反过来，如条件已满足，则由定理 1 知，对 $i = 1,\cdots,k$ 有 $d_i | b_i$，这里 $d_i = (a_i, m_i)$. 因 $\left(\frac{a_i}{d_i}, \frac{m_i}{d_i}\right) = 1$，故有 c_i 使

$$\frac{a_i}{d_i}c_i \equiv 1(\mathrm{mod}\ \frac{m_i}{d_i}).$$

因此原同余方程组等价于

$$x \equiv c_i \frac{b}{d_i}\ (\mathrm{mod}\ \frac{m_i}{d_i}),\quad \cdots,\quad x \equiv c_k \frac{b_k}{d_k}\ (\mathrm{mod}\ \frac{m_k}{d_k}).$$

因 $\frac{m_1}{d_i},\cdots,\frac{m_k}{d_k}$ 显然两两互素，所说的结果便可从定理 3 推出来.

定理 3 在国外文献和教科书中均称作“中国剩余定理”，并且在代数学中被推广成非常一般的形式. 我们则常把它叫作“孙子定理”，因为我国古代数学著作《孙子算经》中载有下面的“物不知其数”问题：今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？

用现在的记号，这个问题相当于求解同余方程组

$$x \equiv 2(\mathrm{mod}\ 3),\quad x \equiv 3(\mathrm{mod}\ 5),\quad x \equiv 2(\mathrm{mod}\ 7).$$

程大位在《算法统宗》(1593 年)中将这一问题的解法总结成如下的歌诀：

三人同行七十稀，五树梅花廿一枝.
七子团圆半个月，除百零五便得知.

其中，前三句的 70，21 和 15(半个月)分别就是定理 3 证明中的 d_1,d_2,d_3. 所以“物不知其数”问题的一个解是

$$70 \cdot 2 + 21 \cdot 3 + 15 \cdot 2 = 233.$$

而歌诀最后一句的含义应当是与 233 相差 105($=2\cdot5\cdot7$) 任意倍数的正数都是问题的解，即解为满足 $x \equiv 233(\mathrm{mod}\ 105)$ 的正整数，其中最小的解是 23.

例 1　解同余方程组

$$x \equiv 1\ (\mathrm{mod}\ 4),\ x \equiv 2\ (\mathrm{mod}\ 5),\ x \equiv 4\ (\mathrm{mod}\ 7),$$

解　设 d_1 是 $d_1 \equiv 1\ (\mathrm{mod}\ 4), d_1 \equiv 0\ (\mathrm{mod}\ 5), d_1 \equiv 0\ (\mathrm{mod}\ 7)$ 的

一个解，即 d_1 满足条件 $d_1 \equiv 1 \pmod 4$ 和 $35 \mid d_1$. 因而可取 $d_1 = -35$. 类似地，可取 $d_2 = 56$ 满足 $d_2 \equiv 1 \pmod 5$ 和 $28 \mid d_2$；可取 $d_3 = -20$ 满足 $d_3 \equiv 1 \pmod 7$ 和 $20 \mid d_3$. 于是同余方程组的解是

$$x \equiv -35 \cdot 1 + 56 \cdot 2 - 20 \cdot 4 \equiv -3 \pmod{140}.$$

例 2　解同余方程组

$$5x \equiv 7 \pmod{12},\ 7x \equiv 1 \pmod{10}.$$

解　由于 12 与 10 不互素，我们不能直接应用孙子定理. 但是 $5x \equiv 7 \pmod{12}$ 等价于 $x \equiv 2 \pmod 3$ 和 $x \equiv 3 \pmod 4$；而 $7x \equiv 1 \pmod{10}$ 等价于 $x \equiv 1 \pmod 2$ 和 $x \equiv 3 \pmod 5$. 因此原同余方程组等价于

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

注意 $x \equiv 3 \pmod 4$ 和 $x \equiv 1 \pmod 2$ 等价于同余方程 $x \equiv 3 \pmod 4$. 因此问题归结为求

$$x \equiv 2 \pmod 3,\ x \equiv 3 \pmod 4,\ x \equiv 3 \pmod 5$$

的解. 现在可以用孙子定理，得到解 $x \equiv 23 \pmod{60}$. 这也是原同余方程组的解.

例 3　设 n 是奇数，$n > 1$；k 是整数，且对 n 的任一素因子 p，有 $(p-1) \nmid k$. 记

$$S_k(n) = \sum_{\substack{i=1 \\ (i,n)=1}}^{n} i^k.$$

证明 $n \mid S_k(n)$.

证明　我们首先考虑特殊情形：$n = p$ 是一个奇素数. 对任意与 p 互素的整数 a，数 $a, 2a, \cdots, (p-1)a$ 为模 p 的缩系，故

$$\sum_{i=1}^{p-1} i^k \equiv \sum_{i=1}^{p-1} (ai)^k (\mathrm{mod}\ p). \tag{13}$$

因此

$$(a^k - 1)S_k(p) \equiv 0\ (\mathrm{mod}\ p). \tag{14}$$

现在我们证明，可以选取 a，满足 $p \nmid a$ 及 $p \nmid (a^k - 1)$. 由此及(14)便导出 $p \mid S_k(p)$.

事实上，由带余除法及 $(p-1) \nmid k$ 可知，$k = (p-1)q + r$，q 是整数，而余数 r 现在满足 $0 < r \leqslant p - 2$. 由拉格朗日定理，同余方程 $x^r - 1 \equiv 0\ (\mathrm{mod}\ p)$ 至多有 $r(\leqslant p-2)$ 个解，从而 $p-1$ 个数 $1,2,\cdots,p-1$ 中必有一个 a 满足 $p \nmid (a^r - 1)$，于是 $p \nmid (a^k - 1)$. 这就证明了 $n = p$ 时的结论.

现在设 n 为大于 1 的奇数，对任一个与 n 互素的整数 a，与(13)，(14)类似地有

$$(a^k - 1)S_k(n) \equiv 0\ (\mathrm{mod}\ n). \tag{15}$$

我们证明，可选择 a 使得

$$(a, n) = (a^k - 1, n) = 1.$$

由此及(15)便证明了结论.

设 n 的不同素因子为 $p_1, \cdots, p_l$. 由于 $(p_i - 1) \nmid k$，从上面的论证知，对每个 p_i，存在 a_{p_i} 使

$$(a_{p_i}, p_i) = (a_{p_i}^k - 1, p_i) = 1.$$

由孙子定理，存在 a 满足下面 l 个同余式.

$$a \equiv a_{p_i} (\mathrm{mod}\ p_i)\ (1 \leqslant i \leqslant l).$$

这样的 a 显然满足 $p_i \nmid a\ (1 \leqslant i \leqslant l)$，从而 $(a, n) = 1$；又 $a^k - 1 \equiv a_{p_i}^k - 1\ (\mathrm{mod}\ p_i)$，故 $p_i \nmid a^k - 1 (1 \leqslant i \leqslant l)$，即 a 满足 $(a^k - 1, n) = 1$. 这就完成了证明.

习　题　7

1. 解下列同余方程：

(i) $32x \equiv 12 \pmod 8$；

(ii) $28x \equiv 124 \pmod{116}$；

(iii) $5x \equiv 44 \pmod{81}$.

2. 解下列一次同余方程组：

(i) $x \equiv 1 \pmod 3$，$x \equiv 1 \pmod 5$，$x \equiv 2 \pmod 7$；

(ii) $x \equiv 1 \pmod 4$，$x \equiv 2 \pmod 5$，$x \equiv 3 \pmod 9$.

3. 用孙子定理解同余方程 $37x \equiv 31 \pmod{77}$.

4. 解同余方程组

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

5. 求 2^{400} 被 319 除得的余数.

6*. (i) 设 m_1, m_2 都是正整数，b_1, b_2 是任意整数. 证明：一次同余方程组

$$x \equiv b_1 \pmod{m_1},\quad x \equiv b_2 \pmod{m_2}$$

有解的充分必要条件是 $(m_1, m_2) \mid (b_1 - b_2)$；并且当此条件成立时，该同余方程组的解是模 $[m_1, m_2]$ 的一个同余类；

(ii) 设 $m_1, \cdots, m_k$ 是正整数，$b_1, \cdots, b_k$ 是任意整数，证明：一次同余式组

$$x \equiv b_1 \pmod{m_1},\ \cdots,\ x \equiv b_k \pmod{m_k}$$

有解的充分必要条件是对任意 $i \neq j$，有 $(m_i, m_j) \mid (b_i - b_j)$；并且，在此条件成立时，同余方程组的解是模 $[m_1, \cdots, m_k]$ 的一个同余类.

7*. 设 $m_1, \cdots, m_k$ 是两两互素的正整数，且

$$m_1 \cdots m_k = m_i M_i (1 \leqslant i \leqslant k).$$

(i) 证明：模 $m_1 \cdots m_k$ 的完(缩)系可以表示为

$$M_1 x_1 + \cdots + M_k x_k,$$

其中 $x_1,\cdots,x_k$ 分别通过模 $m_1,\cdots,m_k$ 的完(缩)系;

(ii) 由(i)的结论证明:$\varphi(m_1\cdots m_k)=\varphi(m_1)\cdots\varphi(m_k)$.

8. 设 n 为正整数,证明必有 n 个连续的整数,其中每一个数都具有平方因子(即被某个大于 1 的完全平方数整除).

9. 设 a,b 是互素的整数,m 是给定的正整数.证明:数列 $a+bn(n\geqslant 0)$ 中有无穷个项与 m 互素.

第三章　原根和指数

§8. 原　　根

设 $m>1$ 是给定的正整数，我们现在研究模 m 的 $\varphi(m)$ 个缩同余类 $\mathbf{Z}_m^*$ 对乘法形成的群的结构(参考 §5).

引理 1　设 $(a,m)=1$，则

(i) 存在正整数 n，$1\leqslant n<m$，使 $a^n\equiv 1(\mathrm{mod}\ m)$；

(ii) 设 n 为(i)中最小的正整数，则对整数 k 和 l，同余式 $a^k\equiv a^l(\mathrm{mod}\ m)$ 成立的充分必要条件是 $k\equiv l(\mathrm{mod}\ n)$. 特别地，$a^k\equiv 1(\mathrm{mod}\ m)$ 成立的充分必要条件为 $n|k$.

证明　(i) 取 $n=\varphi(m)$，所说的结论则是欧拉定理(§6，定理 2)的推论. 我们也可采用下面(更直接)的论证.

m 个数 $a,a^2,\cdots,a^m$ 均与 m 互素，因此必有两个不同的数模 m 同余. 设 $a^k\equiv a^l(\mathrm{mod}\ m)$，其中 $1\leqslant l<k\leqslant m$，进而

$$a^l(a^{k-l}-1)\equiv 0(\mathrm{mod}\ m).$$

因 $(a,m)=1$，故 $(a^l,m)=1$. 因此对 $n=k-l$，有 $a^n\equiv 1(\mathrm{mod}\ m)$，且 n 满足 $1\leqslant n<m$.

(ii) 如果 $a^k\equiv a^l(\mathrm{mod}\ m)$，其中 $k\geqslant l$. 设 $N=k-l$，则与(i)中相同论证可见 $a^N\equiv 1(\mathrm{mod}\ m)$. 由带余除法，$N=nq+r$，其中 $0\leqslant r<n$. 于是

$$a^r\cdot a^{nq}\equiv 1\ (\mathrm{mod}\ m),$$

即 $a^r\equiv 1(\mathrm{mod}\ m)$. 由 n 的最小性及 $0\leqslant r<n$，推出必须 $r=0$；

即 $k \equiv l(\mathrm{mod}\ m)$. 反过来的结论显而易见. 证毕.

对与 m 互素的整数 a，满足 $a^n \equiv 1(\mathrm{mod}\ m)$ 的最小正整数 n，称为 **a 模 m 的阶**.

显然，a 模 m 的阶为 n，等价于说在(乘法) 群 $\mathbf{Z}_m^*$ 中，n 是最小正整数使 $\bar{a}^n = \bar{1}$($\mathbf{Z}_m^*$ 中的单位!).

由欧拉定理及引理 1(ii) 可见，对于每个与 m 互素的 a，a 模 m 的阶都是 $\varphi(m)$ 的某个约数，从而阶的值不超过 $\varphi(m)$.

如果存在整数 g，$(g,m) = 1$，使 g 模 m 的阶恰是 $\varphi(m)$，则称**模 m 有原根**，并称 g 是模 m 的一个原根. (很明显，如 g 是模 m 的原根，则模 m 的同余类 $\bar{g}$ 中所有数均是模 m 的原根.)

若模 m 存在原根 g，则模 m 的缩系呈现特别简单的结构. 因为，由引理 1(ii) 推出，$g^0 = 1, g, \cdots, g^{\varphi(m)-1}$ 彼此模 m 不同余，并且均与 m 互素，从而这 $\varphi(m)$ 个成几何级数的数形成模 m 的一个缩系，这给研究某些问题带来便利.

换一个角度说，模 m 存在原根 g，等价于乘法群

$$\mathbf{Z}_m^* = \{\bar{1}, \bar{g}, \cdots, \bar{g}^{\varphi(m)-1}\},$$

即 $\mathbf{Z}_m^*$ 由一个元 $\bar{g}$“生成”. 这样的群，称为**循环群**，是代数结构最为简单的一类群.

然而，不幸的是，并非对每个整数 $m > 1$ 都有原根. 我们易于证明

引理 2　设 $m \neq 2, 4, p^l$ 或 $2p^l$(p 是奇素数，$l \geqslant 1$)，则模 m 没有原根.

证明　(i) 设 $m = 2^l$，其中 $l \geqslant 3$，则对任意与 m 互素的整数 a，有

$$a^{2^{l-2}} \equiv 1(\mathrm{mod}\ 2^l)(\text{习题 } 4.4).$$

于是 a 模 2^l 的阶 $\leqslant 2^{l-2} < \varphi(2^l)$，故模 m 不存在原根.

对于满足引理的条件且不是 $2^l(l \geqslant 3)$ 形式的 m，我们可表示为

$m = r \cdot s$，其中 r,s 均大于 2 且互素. 当 $(a,m) = 1$ 时，由欧拉定理，$a^{\varphi(r)} \equiv 1 \pmod{r}$ 及 $a^{\varphi(s)} \equiv 1 \pmod{s}$. 由于现在 $\varphi(r),\varphi(s)$ 均是偶数，故

$$a^{\frac{1}{2}\varphi(r)\varphi(s)} \equiv 1 \pmod{rs}.$$

但

$$\varphi(m) = \varphi(r)\varphi(s) > \frac{1}{2}\varphi(r)\varphi(s),$$

从而模 m 没有原根.

换句话说，若模 m 存在原根，则 m 必须具有形式 $2,4,p^l$ 和 $2p^l$（其中 p 为奇素数而 $l \geqslant 1$）. 易知 1 和 -1 分别是模 2 和模 4 的原根. 现在我们着手证明原根理论中最为基本的结果：

定理 1　对每个奇素数 p，模 p 有原根.

为此需要下面一个简单但有用的引理.

引理 3　设 $(a,m) = 1$，a 模 m 的阶为 n，则 a^k 模 m 的阶是 $\frac{n}{(k,n)}$. 特别地，a^k 模 m 的阶为 n 的充分必要条件是 $(k,n) = 1$.

证明　设 l 为正整数，由引理 1(ii)可见，同余式

$$(a^k)^l \equiv 1 \pmod{m} \tag{1}$$

等价于 $n \mid kl$. 这显然又等价于

$$\frac{n}{(k,n)} \mid l \cdot \frac{k}{(k,n)},$$

即 $\frac{n}{(k,n)} \mid l$. 因此，使(1)成立的最小正整数 l 为 $\frac{n}{(k,n)}$，即 a^k 模 m 的阶是 $\frac{n}{(k,n)}$.

定理 1 的证明　$p-1$ 个数 $1,2,\cdots,p-1$ 模 p 的阶都是 $\varphi(p)=p-1$ 的约数. 对 $p-1$ 的每一个正约数 d, 令

$$S(d)=\{x\mid 1\leqslant x\leqslant p-1,\ x \text{ 模 } p \text{ 的阶是 } d\}.$$

我们的目标是证明 $S(p-1)$ 非空.

显然诸集合 $S(d)$(其中 $d\mid p-1$) 是集合 $\{1,2,\cdots,p-1\}$ 的一个划分,即每个 $x(1\leqslant x\leqslant p-1)$ 恰属于一个集合 $S(d)$. 记 R_d 是 $S(d)$ 的元素个数,则

$$\sum_{d\mid p-1} R_d=p-1. \tag{2}$$

显然, $S(d)$ 中的元素均是同余方程

$$x^d-1\equiv 0 \pmod p \tag{3}$$

的解. 另一方面,如果 $R_d\neq 0$,即有某个 a 模 p 的阶为 d,由引理 1(ii) 知, d 个数 $1,a,\cdots,a^{d-1}$ 彼此模 p 不同余,又它们都满足同余方程(3). 但由 §7, 定理 2 知, 同余方程(3) 的解数不超过 d 个. 因此, $x\equiv 1,a,\cdots,a^{d-1}\pmod p$ 恰是同余方程(3)的全部解,所以模 p 阶为 d 的数均在 $1,a,\cdots,a^{d-1}$ 之中. 由引理 3,它们当中共有 $\varphi(d)$ 个模 p 的阶为 d. 因此我们证明了: $R_d=0$ 或者 $R_d=\varphi(d)$. 于是, $R_d\leqslant\varphi(d)$. 从而

$$\sum_{d\mid p-1} R_d\leqslant\sum_{d\mid p-1}\varphi(d)=p-1$$

(最后一个等式见 §6,定理 1(iii)). 结合(2)可见,必须对每个 $d\mid p-1$ 有 $R_d=\varphi(d)$. 特别地,

$$R_{p-1}=\varphi(p-1)\geqslant 1,$$

即 $S(p-1)$ 非空. 证毕.

由定理 1 我们能够证明下面的结果.

定理 2　设 p 是奇素数,则对 $l\geqslant 2$,模 p^l 必有原根.

证明　首先,我们注意,模 p^l 的原根必然也是模 p^r 的原根,其中

$1 \leqslant r < l$. (这一简单的事实请读者自己证明.) 因此,特别地,模 p^l 的原根必然在模 p 的原根之集中.

另一方面,如果模 p 的原根 g 也是模 p^l 的原根,则 g 必是模 p^2 的原根,即 g 模 p^2 的阶是 $p(p-1)$. 所以

$$g^{p-1} \not\equiv 1 \pmod{p^2} \tag{4}$$

是 g 应满足的必要条件. 下面我们将证明,(4) 也是模 p 的原根 g 成为模 p^l 原根的充分条件.

第一步,我们先证明存在模 p 的原根 g 满足条件(4).

取 g 是模 p 的一个原根,如 g 满足(4),则已无需证明. 如 g 不满足(4),由于对任意整数 x,$g + px$ 也是模 p 的原根,而

$$\begin{aligned}(g + px)^{p-1} &\equiv g^{p-1} + p(p-1)xg^{p-2} \\ &\equiv 1 + p(p-1)xg^{p-2} \pmod{p^2}.\end{aligned}$$

现在取 $x = 1$,则 $g_0 = g + p$ 便满足 $g_0^{p-1} \not\equiv 1 \pmod{p^2}$. 这就证明了我们的断言.

第二步,我们用归纳法证明,对每个正整数 r,均有

$$g^{\varphi(p^r)} = 1 + p^r k_r, \quad \text{其中} \quad p \nmid k_r. \tag{5}$$

当 $r = 1$ 时,由我们对 g 的选取知结论成立. 设(5) 对 r 已成立,则易知

$$g^{\varphi(p^{r+1})} = (1 + p^r k_r)^p \equiv 1 + p^{r+1} k_r \pmod{p^{r+2}}.$$

由于 $p \nmid k_r$(归纳假设),这表明(5) 式对 $r + 1$ 也成立.

最后,我们证明 g 为模 p^l 的原根. 设 g 模 p^l 的阶为 d,则 d 是 $\varphi(p^l) = (p-1)p^{l-1}$ 的因子. 又 g 是模 p 的原根,故 $(p-1) \mid d$(引理 1(ii)). 从而

$$d = (p-1)p^{r-1} = \varphi(p^r), \quad \text{其中} \ 1 \leqslant r \leqslant l.$$

但是由(5) 知,当 $r < l$ 时,

$$g^{\varphi(p^r)} = 1 + p^r k_r \not\equiv 1 \pmod{p^l}.$$

因此必然 $r = l$，即 $d = \varphi(p^l)$，从而 g 是模 p^l 的原根.

定理 3　设 p 是奇素数，整数 $l \geqslant 1$，则模 $2p^l$ 必有原根.

证明　设 g 是模 p^l 的原根，则 $g + p^l$ 也是模 p^l 的原根；因 p 是奇数，故 g 与 $g + p^l$ 中必有一个是奇数，记之为 g_0. 我们证明，g_0 是模 $2p^l$ 的原根.

设 g_0 模 $2p^l$ 的阶为 d，则 $d \leqslant \varphi(2p^l)$. 另一方面，$g_0^d \equiv 1 (\mathrm{mod}\ p^l)$，而 g_0 是模 p^l 的原根，故 $\varphi(p^l) \mid d$，即 $d \geqslant \varphi(p^l) = \varphi(2p^l)$. 从而

$$d = \varphi(2p^l),$$

即 g_0 是模 $2p^l$ 的原根.

由以上的结果，我们有

定理 4　设 m 为大于 1 的整数，则模 m 有原根的充分必要条件是 $m = 2, 4, p^l$ 和 $2p^l$，其中 p 是奇素数，而 $l \geqslant 1$.

进一步，对这些 m，设正整数 d 是 $\varphi(m)$ 的一个约数，g 是模 m 的一个原根. 则模 m 共有 $\varphi(d)$ 个（互不同余的）阶为 d 的数，它们是

$$\{g^{\frac{\varphi(m)}{d}k} \mid 1 \leqslant k \leqslant d,\quad (k,d) = 1\}.$$

证明　定理中的第一个断言是定理 1—定理 3 及引理 2 的重述.

为了证明第二个断言，设 g 是模 m 的一个原根，则 $g, \cdots, g^{\varphi(m)}$ 为模 m 的缩系. 对 $1 \leqslant l \leqslant \varphi(m)$，由引理 3，$g^l$ 的阶为 d 的充分必要条件是 $\dfrac{\varphi(m)}{(l,\varphi(m))} = d$，即

$$(l,\varphi(m)) = \frac{\varphi(m)}{d}, \tag{6}$$

令

$$\varphi(m) = dd',\quad l = d'k,$$

则(6)等价于$(d,k)=1$,其中k满足$1\leqslant k\leqslant\frac{\varphi(m)}{d'}=d$,这样的$k$恰由$\varphi(d)$个.由此即知结论成立.

习　题　8

1. 设p是奇素数,g是模p的一个原根.求一g对于模p的阶.

2. 设p是奇素数.证明:模p的任意两个原根之积不是模p的原根.

3*. 设p是一个奇素数,假设存在一个a使得对$p-1$的所有素因子q,有$a^{(p-1)/q}\not\equiv 1(\mathrm{mod}\ p)$,则$a$是模$p$的原根.反过来的命题显然也成立.

4. 设p是奇素数,用模p存在原根来证明威尔逊定理(§5,例1).

5. 设p是奇素数,$n>1$是整数,并记$S_n=\sum_{k=1}^{p-1}k^n$.用模p有原根来证明

$$S_n\equiv\begin{cases}0\ (\mathrm{mod}\ p), & \text{如果 } p-1\mid n,\\ -1\ (\mathrm{mod}\ p), & \text{如果 } p-1\nmid n.\end{cases}$$

6*. 设p是奇素数,$p>3$.证明

(i) 模p的互不同余的原根之积$\equiv 1(\mathrm{mod}\ p)$;

(ii) 模p的互不同余的原根之和$\equiv\mu(p-1)\ (\mathrm{mod}\ p)$.

7. 设n,a都是正整数且$a>1$,证明:$n\mid\varphi(a^n-1)$.

8. 设$n>1$,证明:$n\nmid(2^n-1)$.

9*. 设m是正整数,a和b是整数,满足$ab\equiv 1(\mathrm{mod}\ m)$.证明:$a$和$b$对于模$m$的阶相等.

10*. 设m是正整数,整数a和b对于模m的阶分别是s及t,且$(s,t)=1$.证明:ab模m的阶是st.

11*. 证明:如果有两个整数模m的阶分别为s和t,则必有一个整数模m的阶为$[s,t]$.

12*. 设 m,n 是互素的正整数，a 对于模 m 和模 n 的阶分别是 d_1 和 d_2，则 a 对于模 mn 的阶为 $[d_1,d_2]$.

13*. (i) 设 $a\geqslant 2$，p 为奇素数，证明：a^p-1 的素因子如果不整除 $a-1$，则必有形式 $2px+1$，x 为整数；

(ii) 设 p 是给定的奇素数，证明：有无穷多个素数具有 $2px+1$ 的形式.

14*. (i) 设 $F_n=2^{2^n}+1$，$n\geqslant 1$. 证明：F_n 的每个素因子都具有形式 $2^{n+1}x+1$，x 是整数.

(ii) 设 $l>1$ 是给定的整数，证明：有无穷多个素数具有 2^lx+1 的形式.

15. (i) 对 $p=3,5,7,11,13,17,19,23$，求模 p 的最小正原根；

(ii) 求模 7^2 及模 5^{10} 的一个原根.

§9. 指　数

设模 m 有原根 g，则 $1,g,\cdots,g^{\varphi(m)-1}$ 为模 m 的缩系. 所以对每个与 m 互素的整数 a，必存在唯一的整数 k，$0\leqslant k\leqslant\varphi(m)-1$，使得

$$a\equiv g^k(\mathrm{mod}\ m).$$

上述的 k 称为 a（**对于原根 g**）**模 m 的指数**，记作 $k=\mathrm{ind}_g a$，在不引起混淆时可简记为 $\mathrm{ind}\ a$.

下面的结果表明，指数与通常的对数有许多类似的性质. 因此指数（取值为整数!）也常称为离散对数.

定理 1　设 g 是模 m 的原根，$(a,m)=(b,m)=1$. 则

(i) $\mathrm{ind}\ 1=0$ 及 $\mathrm{ind}\ g=1$；

(ii) $\mathrm{ind}\ (ab)\equiv\mathrm{ind}\ a+\mathrm{ind}\ b\ (\mathrm{mod}\ \varphi(m))$；

(iii) $\mathrm{ind}\ a^n\equiv n\ \mathrm{ind}\ a\ (\mathrm{mod}\ \varphi(m))$，其中 $n\geqslant 1$；

(iv) 如果 g_1 也是 mod m 的原根，则

$$\operatorname{ind}_g a \equiv \operatorname{ind}_{g_1} a \cdot \operatorname{ind}_g g_1 (\operatorname{mod} \varphi(m));$$

(v) $a \equiv b \pmod m$ 的充分必要条件是 $\operatorname{ind} a = \operatorname{ind} b$.

证明　(i) 由定义显而易见.

(ii) 由指数的定义推出

$$g^{\operatorname{ind} a + \operatorname{ind} b} = g^{\operatorname{ind} a} \cdot g^{ind\ b} \equiv ab \equiv g^{\operatorname{ind} ab} (\operatorname{mod} m).$$

故由 §8,引理 1(ii)导出所说的结论.

(iii) 这是(ii)的推论.

(iv) 设 $x = \operatorname{ind}_{g_1} a$ 及 $g_1 \equiv g^y (\operatorname{mod} m)$,则 $y \equiv \operatorname{ind}_g g_1 (\operatorname{mod} \varphi(m))$.

于是

$$a \equiv g_1^x \equiv (g^y)^x (\operatorname{mod} m),$$

故

$$\operatorname{ind}_g a \equiv xy \equiv \operatorname{ind}_{g_1} a \cdot \operatorname{ind}_g g_1 (\operatorname{mod} \varphi(m)).$$

(v) 如果 $\operatorname{ind} a = \operatorname{ind} b$,则 $g^{\operatorname{ind} a} = g^{\operatorname{ind} b}$,即 $a \equiv b \pmod m$. 反过来,如果 $a \equiv b \pmod m$,则 $g^{\operatorname{ind} a} \equiv g^{\operatorname{ind} b} (\operatorname{mod} m)$,故 $\operatorname{ind} a - \operatorname{ind} b$ 是 $\varphi(m)$ 的倍数. 但 $|\operatorname{ind} a - \operatorname{ind} b| < \varphi(m)$,所以

$$\operatorname{ind} a = \operatorname{ind} b.$$

现在我们考虑同余方程

$$x^k \equiv a \pmod m, \tag{1}$$

其中 $k \geqslant 2$, $(a,m) = 1$. 如果同余方程(1)有解,则称 a 是**模 m 的 k 次剩余**,否则称 a 是**模 m 的 k 次非剩余**.

在模 m 存在原根的情况下,我们能够给出下面(理论上的)判别法.

定理 2　设模 m 存在原根,$k \geqslant 2$, $(a,m) = 1$, $d = (k, \varphi(m))$. 则

(i) 同余方程(1)有解的充分必要条件是 $d \mid \operatorname{ind}_g a$,其中 g 是模 m

的一个原根；这也等价于

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}; \tag{2}$$

(ii) 在(i)中条件满足时，同余方程(1)模 m 共有 d 个解；

(iii) 模 m 的缩系中恰有 $\frac{\varphi(m)}{d}$ 个 k 次剩余.

证明　(i) 由定理 1(iii)，(v)可知，同余方程(1)等价于

$$k \cdot \operatorname{ind}_g x \equiv \operatorname{ind}_g a \pmod{\varphi(m)}, \tag{3}$$

这是关于 $\operatorname{ind}_g x$ 的一次同余方程. 由 §7，定理 1 知，同余方程(3) 有解的充分必要条件是 $d \mid \operatorname{ind}_g a$.

另一方面，$d \mid \operatorname{ind}_g a$ 显然等价于

$$\frac{\varphi(m)}{d} \cdot \operatorname{ind}_g a \equiv 0 (\operatorname{mod} \varphi(m)).$$

由定理 1(i)，(iii) 及(v) 知，这又等价于同余式(2).

(ii) 当同余方程(3) 可解时，则它模 $\varphi(m)$ 共有 d 个解，这等价于同余方程(1) 模 m 共有 d 个解.

(iii) 由(i)，a 是模 m 的 k 次剩余，等价于 $d \mid \operatorname{ind}_g a$，即 $\operatorname{ind}_g a = dl$，其中 $l = 0, 1, \cdots, \frac{\varphi(m)}{d} - 1$，从而

$$a \equiv g^0, g^d, \cdots, g^{d(\frac{\varphi(m)}{d}-1)} \pmod{m}.$$

因此模 m 的 k 次剩余共有 $\frac{\varphi(m)}{d}$ 个.

当 m 不太大时，我们能够用定理 2 的证明方法实际地解某些同余方程(1). 为了这样的目的，我们首先需求出模 m 的一个原根 g，并计算 $g^i (0 \leqslant i \leqslant \varphi(m) - 1)$ 模 m 的最小正剩余，得到模 m 的最小正缩系中每个数的指数. 将所得的结果，按指数的大小顺序或最小正缩系的大小顺序列表. 这样的表格称为(模 m 的)指数表(类似于通常的对数表)，供具体应用时查用.

例 1　解同余方程

$$x^8 \equiv 3 \pmod{11}. \tag{4}$$

解　我们求得 2 是模 11 的原根. 模 11 的指数表为

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2\, a$	0	1	8	2	4	9	7	3	6	5

因为同余方程(4)等价于(用指数表)

$$8\mathrm{ind}\ x \equiv \mathrm{ind}\ 3 \equiv 8 \pmod{12},$$

即 $\mathrm{ind}\ x \equiv 1 \pmod 5$. 从而

$$\mathrm{ind}\ x \equiv 1, 6 \pmod{10}.$$

于是(由指数表) $x \equiv 2, 9 \pmod{11}$.

例 2　解指数同余方程

$$7 \cdot 3^x \equiv 6 \pmod{11}. \tag{5}$$

解　利用前面给出的指数表,(5)等价于

$$\mathrm{ind}\ 7 + x\ \mathrm{ind}\ 3 \equiv \mathrm{ind}\ 6 \pmod{10},$$

即

$$8x \equiv 2 \pmod{10},$$

从而解为 $x \equiv 4 \pmod 5$.

本题也可以采用下面的方法:同余方程(5)等价于

$$3^x \equiv 4 \pmod{11}.$$

易于验证:3 模 11 的阶为 5,而当 x 模 5 同余于 0,1,2,3,4 时,3^x 模 11(周期地) 依次取值 1,3,9,5,4. 因此所求之解是 $x \equiv 4 \pmod 5$.

习　题　9

1. 解同余方程：

(i) $x^8 \equiv 3 \pmod{13}$；

(ii) $x^8 \equiv 3 \pmod{143}$.

2. 用例 2 中的两种方法解同余方程：

(i) $6 \cdot 3^x \equiv 7 \pmod{11}$；

(ii) $5 \cdot 6^x \equiv 3 \pmod{13}$.

3. 解同余方程：

(i) $8x^5 \equiv 3 \pmod{17}$；

(ii) $7^x \equiv 4 \pmod{17}$.

4. 写出模 11 的全部二次剩余.

5. 写出模 37 的全部 8 次剩余及 15 次剩余.

6. 设 p 是素数，$p \equiv 2 \pmod{3}$，a 和 b 是整数. 证明：

$$a^3 \equiv b^3 \pmod{p}$$

成立的充分必要条件是 $a \equiv b \pmod{p}$.

第四章　二次剩余

§10. 二次剩余

本节讨论模为素数 p 的二次同余方程

$$ax^2 + bx + c \equiv 0 (\mathrm{mod}\ p), \quad p \nmid a. \tag{1}$$

当 $p = 2$ 时，同余方程(1) 极易求解. 因此以后我们总设 p 为奇素数.

由于 $p \nmid 4a$，故(1)等价于同余方程

$$(2ax + b)^2 \equiv b^2 - 4ac \ (\mathrm{mod}\ p). \tag{2}$$

令 $y \equiv 2ax + b (\mathrm{mod}\ p)$，由于 $p \nmid 2a$，故 x 与 y(模 p) 一一对应，因此(2)与同余方程

$$y^2 \equiv b^2 - 4ac \ (\mathrm{mod}\ p)$$

是等价的. 由以上讨论可见，我们只要研究形如

$$x^2 \equiv a \ (\mathrm{mod}\ p) \tag{3}$$

的同余方程. 当 $p \mid a$ 时，(3) 仅有一个解 $x \equiv 0 (\mathrm{mod}\ p)$. 所以我们以下总假定 $p \nmid a$.

如果同余方程(3) 有解，则称 a 是**模 p 的二次剩余**(在不引起混淆时，简称为二次剩余)；否则称 a 是**模 p 的二次非剩余**(简称二次非剩余)(参考 §9).

若 a 是模 p 的二次剩余，则同余方程(3) 恰有两个解. 此外，若 a 是二次剩余，则模 p 同余类 $\bar{a}$ 中每个数都是二次剩余. 对于二次非剩余也是如此.

定理 1　设 p 是奇素数，则模 p 的任一完系中恰有 $\frac{p-1}{2}$ 个二次剩

余，以及$\frac{p-1}{2}$个二次非剩余；并且模p的全部二次剩余在数

$$1^2,2^2,\cdots,\left(\frac{p-1}{2}\right)^2 \tag{4}$$

所属的(模p的)同余类中.

证明　定理的第一部分是§9，定理2(iii)的推论.也可采用下面的论证：首先我们注意，(4)中的数彼此模p不同余.这是因为，如$x^2\equiv y^2(\mathrm{mod}\ p)$，其中$1\leqslant x,\ y\leqslant\frac{p-1}{2}$，则

$$(x-y)(x+y)\equiv 0(\mathrm{mod}\ p).$$

但$1<x+y<p$，故

$$x-y\equiv 0(\mathrm{mod}\ p),$$

因此$x=y$.又因为模p的二次剩余当然(模p)同余于$1^2,2^2,\cdots,(p-1)^2$；而

$$(p-k)^2\equiv k^2(\mathrm{mod}\ p),$$

故每个二次剩余恰与(4)中一个数模p同余，即模p的任一完系中恰有$\frac{p-1}{2}$个二次剩余，从而二次非剩余有$(p-1)-\frac{p-1}{2}=\frac{p-1}{2}$个.

定理2　设p为素数，则模p的两个二次剩余之积是二次剩余，模p的一个二次剩余和一个二次非剩余之积是二次非剩余，模p的两个二次非剩余之积是二次剩余.

证明　由§9，定理2(iii)的证明可看到，取g是模p的一个原根，则模p(互不同余)的二次剩余恰由g^{2i}组成$(1\leqslant i\leqslant\frac{p-1}{2})$，从而二次非剩余为$g^{2i-1}(1\leqslant i\leqslant\frac{p-1}{2})$.由此立刻推出我们的结论.

定理2也可采用下面更为直接的论证：

两个模p的二次剩余之积显然是二次剩余.现设a,b分别是模p的

二次剩余和二次非剩余，则有整数 x_0 使 $x_0^2 \equiv a \pmod{p}$. 由于 $p \nmid a$，故 $p \nmid x_0$. 于是有整数 x_0' 使 $x_0 x_0' \equiv 1 \pmod{p}$. 如果 ab 是模 p 的二次剩余，则有整数 y_0 使 $y_0^2 \equiv ab \pmod{p}$. 由此易知

$$(x_0' y_0)^2 \equiv x_0'^2 ab \equiv (x_0 x_0')^2 b \equiv b \pmod{p},$$

这与 b 是二次非剩余矛盾.

最后，设 a 是模 p 的任一个二次非剩余，由于 $p \nmid a$，故若 $a_1, \cdots, a_{p-1}$ 是模 p 的缩系，则 $aa_1, \cdots, aa_{p-1}$ 也是模 p 的缩系. 无妨设 $a_1, \cdots, a_r$ 是模 p 的二次剩余，这里 $r = \dfrac{p-1}{2}$；则 $a_{r+1}, \cdots a_{p-1}$ 是模 p 的二次非剩余. 上面已证明，$aa_1, \cdots, aa_r$ 是二次非剩余，所以 $aa_{r+1}, \cdots, aa_{p-1}$ 均是二次剩余. 这就证明了，任两个二次非剩余之积是二次剩余.

为了将定理 2 表达成更为简洁的形式，我们引入模 p 的**勒让德**(Legendre)**符号**：

对每个整数 a，定义

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{如果 } a \text{ 是模 } p \text{ 的二次剩余；} \\ -1, & \text{如果 } a \text{ 是模 } p \text{ 的二次非剩余；} \\ 0, & \text{如果 } p \mid a. \end{cases}$$

于是定理 2 可叙述成：当 $p \nmid ab$ 时，有

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right). \tag{5}$$

不难看出，当 $p \mid ab$ 时，此式仍然成立. 由定义还可知，对给定的 p，勒让德符号 $\left(\dfrac{a}{p}\right)$ 是周期为 p 的周期函数，而同余方程(3) 的解数可表示为 $1 + \left(\dfrac{a}{p}\right)$.

由于在 $p \nmid a$ 时同余方程(3) 可解的充分必要条件是 $\left(\dfrac{a}{p}\right) = 1$，所以，问题归结为如何有效地计算勒让德符号 $\left(\dfrac{a}{p}\right)$ 的值. 在这方面首先有

定理 3(欧拉判别法则)　设 p 为奇素数,则

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

证明　当 $p|a$ 时结论显然成立. 当 $p\nmid a$ 时,由费马定理知

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

所以

$$(a^{\frac{p-1}{2}} + 1)(a^{\frac{p-1}{2}} - 1) \equiv 0 \pmod{p}.$$

故

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

但由 §9,定理 2(iii) 知,$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ 当且仅当 a 是模 p 的二次剩余,从而结论成立.

我们也可采用下面的论证:

当 $\left(\frac{a}{p}\right) = 1$ 时,有整数 b 使 $b^2 \equiv a \pmod{p}$,于是

$$a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 = \left(\frac{a}{p}\right) \pmod{p}.$$

如果 $\left(\frac{a}{p}\right) = -1$,即 a 是模 p 的二次非剩余,记 $r = \frac{p-1}{2}$,并设 $a_1, \cdots, a_r$ 是模 p 全部二次剩余,则 $aa_1^{-1}, \cdots, aa_r^{-1}$ 是模 p 的全部二次非剩余(定理 2). 因此 $a_1, \cdots, a_r, aa_1^{-1}, \cdots, aa_r^{-1}$ 为模 p 的缩系,于是由威尔逊定理(§5,例 1)

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv a_1 \cdots a_r \cdot (aa_1^{-1}) \cdots (aa_r^{-1}) \\ &\equiv (p-1)! \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod{p}. \end{aligned}$$

作为欧拉判别法则的直接推论,我们有

推论 1　设 p 为奇素数，则

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, & \text{如 } p\equiv 1 \pmod 4,\\ -1, & \text{如 } p\equiv 3 \pmod 4.\end{cases}$$

证明　由定理 3 知，$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}\pmod p$. 但这同余式两边取值均为 ± 1，而 $p\geqslant 3$，因此必然

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$$

推论 2　设 p 是奇素数，则

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1, & \text{如 } p\equiv\pm 1 \pmod 8,\\ -1, & \text{如 } p\equiv\pm 3 \pmod 8.\end{cases}$$

证明　考虑下面 $\frac{p-1}{2}$ 个同余式：

$$\begin{aligned}p-1&\equiv 1\cdot(-1)^1\pmod p;\\ 2&\equiv 2\cdot(-1)^2\pmod p;\\ p-3&\equiv 3\cdot(-1)^3\pmod p;\\ 4&\equiv 4\cdot(-1)^4\pmod p;\\ &\vdots\\ r&\equiv\frac{p-1}{2}(-1)^{\frac{p-1}{2}}\pmod p.\end{aligned}$$

这里 $r=\frac{p-1}{2}$（如果 $4\mid p-1$）或 $r=p-\frac{p-1}{2}$（如果 $4\mid p+1$）. 将这些同余式相乘，得出

$$2\cdot 4\cdot\cdots\cdot(p-1)\equiv\left(\frac{p-1}{2}\right)!(-1)^{1+2+\cdots+\frac{p-1}{2}}\pmod p.$$

因此

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}}\pmod p.$$

因 $p\nmid\left(\frac{p-1}{2}\right)!$，故

$$2^{\frac{p-1}{2}}\equiv(-1)^{\frac{p^2-1}{8}}(\mathrm{mod}\ p),$$

由此结合定理 3(取 $a=2$) 即得结果.

设 p 是给定的奇素数，$p\nmid a$. 设 a 的标准分解为 $a=\pm q_1^{a_1}\cdots q_k^{a_k}$，则(反复用(5))有

$$\left(\frac{a}{p}\right)=\left(\frac{\pm 1}{p}\right)\left(\frac{q_1}{p}\right)^{a_1}\cdots\left(\frac{q_k}{p}\right)^{a_k}.$$

因此，为了计算 $\left(\frac{a}{p}\right)$，只需求出

$$\left(\frac{-1}{p}\right),\left(\frac{2}{p}\right)\text{和}\left(\frac{q}{p}\right)\ (q\text{ 为奇素数},q\neq p).$$

上面的两个推论计算出了 $\left(\frac{-1}{p}\right)$ 和 $\left(\frac{2}{p}\right)$，于是剩下的主要问题是求 $\left(\frac{q}{p}\right)$.

对这一问题，定理 3 的价值在于理论上的，并非是实用的工具. 事实上，当给定的素数 p 不太大时，为了判别 q 是否为模 p 的二次剩余，我们往往通过直接(模 p) 计算(4) 中所列的数来确定，而不采用(计算更麻烦的) 定理 3. 当素数 p 很大时，两种方法均不实用.

另一方面，推论 1 和推论 2 确定了以 -1 及 2 为二次剩余(及非剩余) 的所有素数. 一个自然的问题是：给定 a，确定怎样的素数 p 以 a 为二次剩余.

两个问题的解答都依赖下一节中讲的二次互反律.

习　题　10

1*. 设 p 是奇素数，a,b 为整数且 $p\nmid a$. 证明

$$\sum_{n=0}^{p-1}\left(\frac{an+b}{p}\right)=0.$$

2. 设 p 是奇素数，n 是 $1,2,\cdots,p-1$ 中最小的模 p 二次非剩余. 证明 n 是素数.

3. (i) 证明：形如 $4n+1$ 的素数有无穷多个；

(ii) 证明：形如 $8n+3,8n+5,8n+7$ 的素数均有无穷多个.

4. 设 p 是奇素数，证明：有无穷多个素数都是模 p 的二次非剩余.

5. 设 p 与 $q=2p+1$ 都是素数. 证明

(i) 当 $p\equiv 1 \pmod 4$ 时，2 是模 q 的原根；

(ii) 当 $p\equiv 3 \pmod 4$ 时，-2 是模 q 的原根.

6*. 设 p 是素数，$p\equiv 3 \pmod 4$. 记 $q=2p+1$ 及 $M_p=2^p-1$. 证明：当且仅当 q 为素数时有 $q\mid M_p$.

7. 设 p 是奇素数. 证明

$$\prod_{\substack{r=1\\ \left(\frac{r}{p}\right)=1}}^{p-1} r\equiv-\left(\frac{-1}{p}\right) \pmod p.$$

8. 设 p 是素数，$p\equiv 1 \pmod 4$. 证明

(i) $\sum\limits_{\substack{r=1\\ \left(\frac{r}{p}\right)=1}}^{p-1} r=\dfrac{p(p-1)}{4}$；

(ii) $\sum\limits_{a=1}^{p-1} a\left(\dfrac{a}{p}\right)=0$；

(iii) $\sum\limits_{k=1}^{\frac{p-1}{2}}\left[\dfrac{k^2}{p}\right]=\dfrac{(p-1)(p-5)}{24}$.

9. 设 p 是素数，$p\equiv 3 \pmod 4$，且 $p>3$. 证明

(i) $\sum\limits_{\substack{r=1\\ \left(\frac{r}{p}\right)=1}}^{p-1} r\equiv 0 \pmod p$；

(ii) $\sum\limits_{a=1}^{p-1} a\left(\dfrac{a}{p}\right)\equiv 0 \pmod p$.

10*. 设 p 是奇素数，a 是整数且 $p\nmid a$，则

$$\sum_{x=0}^{p-1}\left(\frac{x^2+ax}{p}\right)=-1.$$

11. 设 p 是奇素数，a 是整数.

(i) 证明：同余方程 $x^2-y^2\equiv a \pmod p$ 必有解；

(ii) 若 (x,y) 和 (x',y') 均是上述同余方程的解，当 $x\equiv x'$ 且 $y=y' \pmod p$ 时，我们将 (x,y) 和 (x',y') 看成是模 p 的同一个解.

证明：(i) 中同余方程的解数是 $p-1$（如果 $p\nmid a$）或 $2p-1$（如果 $p\mid a$）.

12*. 设 p 是奇素数，证明

$$\sum_{x=0}^{p-1}\left(\frac{x^2+a}{p}\right)=\begin{cases}-1, & \text{如果 } p\nmid a,\\ p-1, & \text{如果 } p\mid a.\end{cases}$$

13*. 设 p 是奇素数，$f(x)=ax^2+bx+c$ 且 $p\nmid a$. 记

$$D=b^2-4ac.$$

证明

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)=\begin{cases}-\left(\frac{a}{p}\right), & \text{如果 } p\nmid D,\\ (p-1)\left(\frac{a}{p}\right), & \text{如果 } p\mid D.\end{cases}$$

14*. 设 p 是奇素数，$k\geqslant 1$. 则同余方程 $x^2\equiv a \pmod{p^k}$ 有解的充分必要条件是 $\left(\frac{a}{p}\right)=1$；并在此条件满足时，模 p^k 恰有两个解.

15*. 设 a 是奇数，则

(i) $x^2\equiv a \pmod 2$ 对所有 a 有解；

(ii) $x^2\equiv a \pmod 4$ 有解的充分必要条件是 $a\equiv 1 \pmod 4$，并且在此条件满足时，恰有两个不同的解；

(iii) 同余方程 $x^2\equiv a \pmod{2^k}$ $(k\geqslant 3)$ 有解的充分必要条件是 $a\equiv 1 \pmod 8$，并且在条件成立时恰有四个解. 如果 x_0 是一个解，则 $\pm x_0$，$\pm x_0+2^{k-1}$ 是所有解.

§11. 二次互反律

本节的主要目的是证明下面重要的结果：

定理 1(二次互反律)　设 p,q 是两个不同的奇素数，则

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}=\begin{cases}-1, & \text{如 } p\equiv q\equiv 3 \pmod 4,\\ 1, & \text{其它情形.}\end{cases}$$

注记　由 §10 我们知道，勒让德符号 $\left(\frac{p}{q}\right)$ 及 $\left(\frac{q}{p}\right)$ 分别刻画了二次同余方程

$$x^2\equiv p \pmod q$$

和

$$x^2\equiv q \pmod p$$

是否可解；即 p 是否为模 q 的二次剩余及 q 是否为模 p 的二次剩余. 上面两个二次同余方程的模和剩余恰好互换了位置，而定理 1 给出了这样两个同余方程可解性的联系，因此称为二次互反律.

为了证明定理 1，我们需要一个基本的引理.

引理(高斯引理)　设 p 是奇素数，$p\nmid a$，$r=\frac{p-1}{2}$. 记 μ 是数

$$a,2a,\cdots,ra \tag{1}$$

中模 p 的最小正剩余大于 $\frac{p}{2}$ 的个数，则

$$\left(\frac{a}{p}\right)=(-1)^{\mu}. \tag{2}$$

证明　在 $a,2a,\cdots,ra$ 被 p 除得的余数中，设 $b_1,\cdots,b_\lambda$ 与 $c_1,\cdots,c_\mu$

分别是小于$\frac{p}{2}$及大于$\frac{p}{2}$的数，这里$\lambda+\mu=r$. 由于(1)中的数彼此模p不同余，故诸b_i中无两者相同，诸$p-c_j$中也无两数相同. 又易见b_i与$p-c_j$不会有相同者；因假设有i,j使$b_i=p-c_j$，则相应地有$x,y(1\leqslant x,y\leqslant r)$使

$$ax\equiv -ay(\mathrm{mod}\ p),$$

即$a(x+y)\equiv 0(\mathrm{mod}\ p)$. 但$p\nmid a$，故有$x+y\equiv 0(\mathrm{mod}\ p)$；这不可能，因$1<x+y<p$.

注意到$0<p-c_j\leqslant r\ (1\leqslant j\leqslant \mu)$. 我们推出$r$个数$b_1,\cdots,b_\lambda$，$p-c_1,\cdots,p-c_\mu$是$1,2,\cdots,r$的一个排列，故

$$r!=b_1\cdots b_\lambda(p-c_1)\cdots(p-c_\mu). \tag{3}$$

将(3)模p，产生

$$r!\equiv(-1)^\mu b_1\cdots b_\lambda c_1\cdots c_\mu\equiv(-1)^\mu r!a^r(\mathrm{mod}\ p).$$

因$p\nmid r!$，故我们有$a^r\equiv(-1)^\mu(\mathrm{mod}\ p)$. 结合欧拉判别法(§10，定理3)，便证明了(2).

现在我们能够证明定理1.

第一步，在a为奇数时，我们给出公式(2)一种解析的表示形式.

由带余除法(见习题1.8)，对$1\leqslant i\leqslant r=\frac{p-1}{2}$，有

$$ai=p\left[\frac{ai}{p}\right]+r_i,\quad 0<r_i<p. \tag{4}$$

将余数r_i中小于$\frac{p}{2}$及大于$\frac{p}{2}$者分别改记为b_i与$c_j(1\leqslant i\leqslant\lambda,\ 1\leqslant j\leqslant\mu)$，并用$B$与$C$分别表示诸$b_i$的和及诸$c_j$的和. 将(4)中$r$个等式相加，得出

$$\frac{p^2-1}{8}\cdot a=pA+B+C, \tag{5}$$

其中$A=\sum_{i=1}^{r}\left[\frac{ai}{p}\right]$. 另一方面，由高斯引理的证明中可见

$$b_1 + \cdots + b_\lambda + (p - c_1) + \cdots + (p - c_\mu) = 1 + 2 + \cdots r.$$

于是

$$\mu p - C + B = \frac{p^2 - 1}{8}.$$

结合(5)给出

$$\frac{p^2 - 1}{8} \cdot (a - 1) = (A - \mu)p + 2C. \tag{6}$$

注意 p 是奇数，故$\frac{p^2 - 1}{8}$ 为整数，而 $a - 1$ 是偶数；故(6) 给出

$$(A - \mu)\ p \equiv 0 \pmod 2),$$

即 $\mu \equiv A \pmod 2$. 因此，如果 $2 \nmid a$，则由(2)得出$\left(\frac{a}{p}\right) = (-1)^A$. 特别地，对奇素数 $q \neq p$，我们有

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{r}[\frac{qi}{p}]}.$$

类似地，我们也有

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{s}[\frac{pj}{q}]}, \quad \text{其中 } s = \frac{q-1}{2}.$$

因此

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum_{i=1}^{r}[\frac{qi}{p}]+\sum_{j=1}^{s}[\frac{pj}{q}]}. \tag{7}$$

第二步，我们证明

$$\sum_{i=1}^{r}[\frac{qi}{p}] + \sum_{j=1}^{s}[\frac{pj}{q}] = rs. \tag{8}$$

由此及(7)就证明了定理 1. 为此，我们考虑平面上以 $(0,0)$，$(0,\frac{q}{2})$，$(\frac{p}{2},0)$，$(0,\frac{q}{2})$ 为顶点的矩形. 显然，满足 $1 \leqslant x \leqslant \frac{p}{2}$，$1 \leqslant y \leqslant \frac{q}{2}$ 的整点(x,y) 共有 rs 个，而连接$(0,0)$ 和$(\frac{p}{2},\frac{q}{2})$ 两点的直线 l 将此矩形

分成两部分（图 10.1），并且上述 rs 个整点都不在直线 l 上. 这是因为若有所说的整点(x,y)在 l 上，则 $xq = yp$，故 $p|xq$. 因 p 和 q 为不同素数，从而 $p|x$，这不可能，因 $1 \leqslant x \leqslant r < p$.

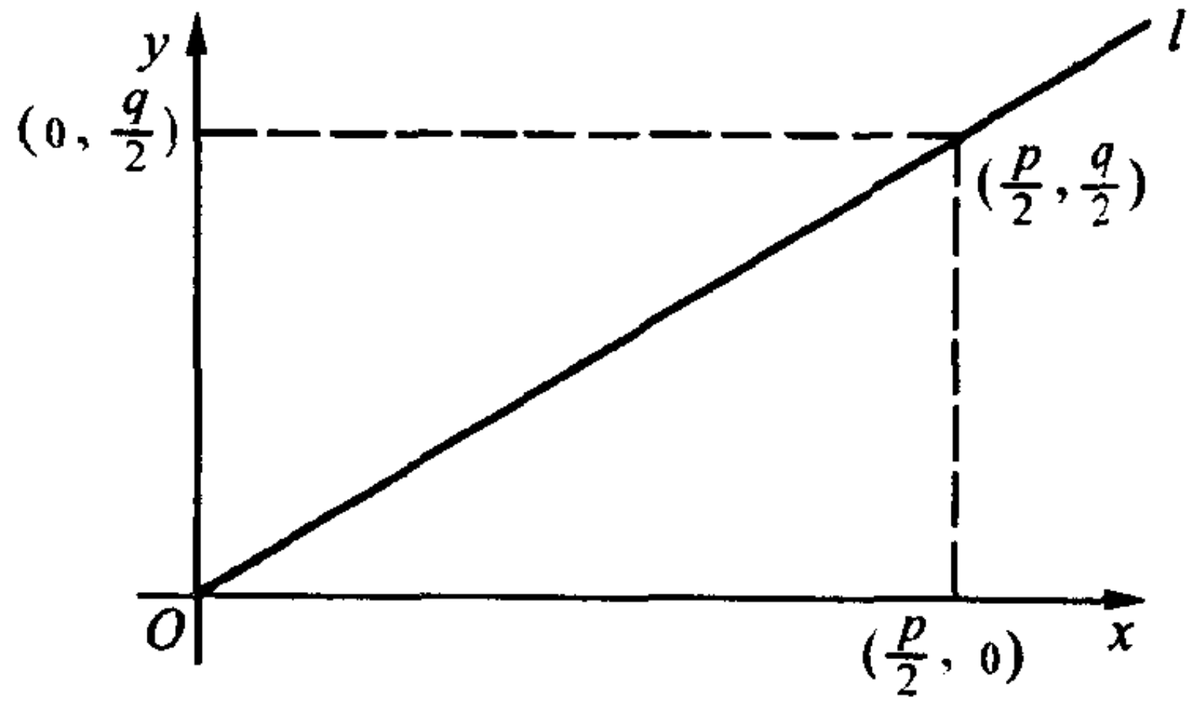


图 10.1

现在考虑直线 l 下面那部分所包含的整点个数. 由于坐标 $x = i$ 的整点为(i,y)，其中 $1 \leqslant y \leqslant \frac{qi}{p}$，因此这部分的整点共有 $\sum_{i=1}^{r}[\frac{qi}{p}]$ 个. 同样，直线 l 上面部分的整点数为 $\sum_{j=1}^{s}[\frac{pj}{q}]$ 个. 综合两方面的结果，即知 (8) 成立. 因此二次互反律得到了证明.

二次剩余的概念最早出现于欧拉 1754 年发表的论文中. 1783 年欧拉明确 地叙述了二次互反律，他的提法如下面的定理 2. 勒让德和高斯也都 独立地发现了二次互反律，定理 1 的形式就是勒让德提出的. 但是二次互反律的第一个完整证明是高斯在 1796 年给出的(当时高斯 19 岁!). 高斯一生共给出了七个不同证明，上面讲的证明是其中之一. 二次互反律是十八世纪数论中最富于首创精神，并且能从中引出众多成果的一个伟大发现. 二次互反律的各种角度的推广，构成近代数论的一项重要内容.

用二次互反律可以有效地计算勒让德符号.

例 1　判断同余方程 $x^2 \equiv 219 \pmod{383}$ 是否有解.

解　由于 383 是素数,而 $219 = 3 \cdot 73$,从而

$$\left(\frac{219}{383}\right) = \left(\frac{3}{383}\right)\left(\frac{73}{383}\right).$$

用二次互反律

$$\left(\frac{3}{383}\right) = \left(\frac{383}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{383-1}{2}} = -\left(\frac{383}{3}\right) = -\left(\frac{2}{3}\right) = 1;$$

$$\left(\frac{73}{383}\right) = \left(\frac{383}{73}\right) = \left(\frac{18}{73}\right) = \left(\frac{2}{383}\right) = 1.$$

于是 $\left(\frac{219}{383}\right) = 1$,即所说的同余方程有解.

作为二次互反律的另一个(理论上的)应用,我们(原则上)能够确定以给定的(非零)整数 a 为二次剩余的所有素数 p. 首先考虑特殊情形:$a = q$ 是一个奇素数.

定理 2　设 q 是一个奇素数.

(i) 如 $q \equiv 1 \pmod 4$,则 q 是模 p 的二次剩余的充分必要条件是 $p \equiv r \pmod q$,其中 r 是模 q 的任一个二次剩余;

(ii) 如 $q \equiv 3 \pmod 4$,则 q 是模 p 的二次剩余的充分必要条件是 $p \equiv \pm b^2 \pmod{4q}$,其中 b 是任意奇整数,且 $(b,q) = 1$.

证明　(i) 如果 $q \equiv 1 \pmod 4$,则由定理 1 知 $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$. 由此即知结论成立.

(ii) 如果 $q \equiv 3 \pmod 4$,定理 1 给出

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right). \tag{9}$$

首先设 $p \equiv \pm b^2 \pmod{4q}$,其中 b 是与 q 互素的奇数. 当

$p \equiv b^2 \pmod{4q}$ 时，我们有

$$p \equiv b^2 \equiv 1 \pmod 4 \quad 及 \quad p \equiv b^2 \pmod q.$$

因此

$$(-1)^{\frac{p-1}{2}} = 1 \quad 及 \quad \left(\frac{p}{q}\right) = 1,$$

从而 $\left(\frac{q}{p}\right) = 1$；当 $p \equiv -b^2 \pmod{4q}$ 时，类似地可得出

$$(-1)^{\frac{p-1}{2}} = -1,$$

以及

$$\left(\frac{p}{q}\right) = \left(\frac{-b^2}{q}\right) = \left(\frac{-1}{q}\right) = -1 \text{（注意 } q \equiv 3 \pmod 4\text{）}.$$

从而也有 $\left(\frac{q}{p}\right) = 1$.

反过来，假设 $\left(\frac{q}{p}\right) = 1$. 则由(9)得出

$$(-1)^{\frac{p-1}{2}} = 1 \quad 且 \quad \left(\frac{p}{q}\right) = 1; \tag{10}$$

或

$$(-1)^{\frac{p-1}{2}} = -1 \quad 且 \quad \left(\frac{p}{q}\right) = -1. \tag{11}$$

当(10)成立时，我们有 $p \equiv 1 \pmod 4$ 及 $p \equiv b^2 \pmod q$. 显然可设 b 是奇数（否则以 $b' = q - b$ 代替 b），于是 $b^2 \equiv 1 \pmod 4$，故 $p \equiv b^2 \pmod 4$. 从而 $p \equiv b^2 \pmod{4q}$，其中 b 是与 q 互素的奇数.

当(11)成立时，我们有 $p \equiv 3 \pmod 4$ 及 $p \equiv -b^2 \pmod q$. 类似于前一种情形，我们可设 b 是奇数，故 $p \equiv -b^2 \pmod 4$. 从而

$$p \equiv -b^2 \pmod{4q}.$$

证毕.

对任意的(非零)整数 a,为确定使 $\left(\frac{a}{p}\right)=1$ 的素数 p,我们可设 a 没有平方因子,即设 $a=\pm 2q_1\cdots q_k$(q_i 是互不相同的奇素数). 由定理 2,§10 中推论 1 和推论 2 及习题 7.6 易于证明,使 $\left(\frac{a}{p}\right)=1$ 的素数 p 一定属于有限个固定的算术级数. 此外,狄利克雷(Dirichlet)的一个著名结果断言,公差与首项互素的算术级数中一定有无穷多个素数. 由此可证明,以 a 为二次剩余的素数有无穷多个. 事实上,更深入的方法能够证明,这样的素数在全体素数集中大致占了一半.

当 a 的素因子较少时,可以实际地确定以 a 为二次剩余的素数(所属的算术级数). 我们举一个简单例子.

例 2　确定以 6 为二次剩余的素数.

解　因 $\left(\frac{6}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$,因此 $\left(\frac{6}{p}\right)=1$ 等价于

$$\left(\frac{2}{p}\right)=1 \quad 且 \quad \left(\frac{3}{p}\right)=1; \tag{12}$$

或

$$\left(\frac{2}{p}\right)=-1 \quad 且 \quad \left(\frac{3}{p}\right)=-1. \tag{13}$$

由定理 2(ii)知,$\left(\frac{3}{p}\right)=1$ 成立的充分必要条件是

$$p\equiv\pm 1,\pm 5^2,\pm 7^2,\pm 11^2 \pmod{12},$$

即 $p\equiv\pm 1 \pmod{12}$. 从而满足 $p\equiv\pm 5 \pmod{12}$ 的素数以 3 为二次非剩余. 结合 §10,推论 2 可见,(12)成立等价于

$$p\equiv\pm 1 \pmod 8 \quad 且 \quad p\equiv\pm 1 \pmod{12}; \tag{14}$$

而(13)成立等价于

$$p\equiv\pm 3 \pmod 8 \quad 且 \quad p\equiv\pm 5 \pmod{12}. \tag{15}$$

解同余式组(14),(15),分别得出

$$p \equiv \pm 1 (\mathrm{mod}\ 24) \quad 及 \quad p \equiv \pm 5 (\mathrm{mod}\ 24).$$

因此$\left(\frac{6}{p}\right) = 1$的充分必要条件是$p \equiv \pm 1, \pm 5 (\mathrm{mod}\ 24)$.

习　题　11

1. 设p是奇素数,用高斯引理计算$\left(\frac{2}{p}\right)$.

2. 计算$\left(\frac{17}{23}\right), \left(\frac{19}{37}\right), \left(\frac{60}{79}\right), \left(\frac{92}{101}\right)$.

3. (i) 确定以 -3 为二次剩余的素数;

(ii) 确定以 5 为二次剩余的素数;

(iii) 确定以 15 为二次剩余的素数.

4. 证明:形如$6n+1$的素数有无穷多个.

5. 设$p = 4k+1$是素数,a是k的约数.证明:$\left(\frac{a}{p}\right) = 1$.

6. 设$p = 10n-1$是素数,证明:$p \mid 5^{5n-1} - 1$.

7. 设$n > 1, p = 2^n + 1$是素数.证明:模p的原根之集与模p的二次非剩余之集相同;进而证明 3,7 都是模p的原根.

第五章　不定方程

§12.　不定方程与同余方程

所谓不定方程，大致地说，是指未知数个数多于方程的个数，而未知数的取值范围受某些限制(如整数，正整数或有理数)的方程. 不定方程是数论的一个重要课题，也是一个非常复杂和困难的课题. 为了研究一些不定方程，人们创造了许多强有力的方法和工具，但是仍有许多问题没有解决. 我们在这一章中只是简要地涉及不定方程与前面某些知识的联系，并给出不定方程中几个较为简单和基本的经典结果.

在形形色色的不定方程中，占据中心位置的是所谓的多项式不定方程，即研究方程

$$F(x_1, \cdots, x_n) = 0 \tag{1}$$

的整数解，其中 F 是一个整系数多项式. 最简单的情形当然是一次多项式方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n - b = 0. \tag{2}$$

容易知道(参考习题 2.10)，方程(2)有整数解的充分必要条件是 a_1，$\cdots$，a_n 的最大公约数整除 b.

一般而言，判定(1)是否有解，是一个相当困难的问题. 然而，如果方程(1)有整数解，则它必须满足下面的

条件(i)　方程(1)有实数解；

条件(ii)　对所有正整数 m，方程(1) 在 $\mathbf{Z}_m$ 上有解，即同余方程

$$F(x_1, \cdots, x_n) \equiv 0 \pmod{m} \tag{3}$$

有解.

这是因为，若(1)有整数解 $x_i = x_i'(1 \leqslant i \leqslant n)$. 这当然是满足(1)的实数解，并且满足同余方程(2).

注记　容易证明，条件(ii)等价于下面的

条件(iii)　对所有素数 p 及整数 $k \geqslant 1$，同余方程

$$F(x_1, \cdots, x_n) \equiv 0 \pmod{p^k} \tag{4}$$

有解.

事实上，条件(ii)当然蕴含着条件(iii). 反过来，若条件(iii)成立，我们设 $m = p_1^{a_1} \cdots p_l^{a_l}$ 是 $m > 1$ 的标准分解，并设

$$x_i \equiv x_i^{(j)} \pmod{p_j^{a_j}} \quad (1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant l)$$

是同余方程

$$F(x_1, \cdots, x_n) \equiv 0 \pmod{p_j^{a_j}}$$

的一组解. 由孙子定理知，对每个 $i(1 \leqslant i \leqslant n)$，同余方程组

$$x \equiv x_i^{(j)} \pmod{p_j^{a_j}} \quad (1 \leqslant j \leqslant l)$$

有解 $x \equiv x_i' \pmod{m}$. 于是，$x_i \equiv x_i' \pmod{m}(1 \leqslant i \leqslant n)$ 是同余方程(3)的解.

如果 $F(x_1, \cdots, x_n)$ 满足上面的条件(i)和(ii)(或(iii))，则称方程(1)**局部可解**. 上面的讨论表明，方程(1)局部可解是它有整数解的必要条件. 换句话说，如果(1)没有实数解，或者有某个 $m > 1$ 使同余方程(3)无解，则方程(1)没有整数解. 由于方程(1)是否有实数解以及它在(有限集合)$\mathbf{Z}_m$ 上的可解性通常更易于把握，因此，所说的原则提供了证明某些方程无整数解(或帮助求解)的一个基本出发点.

例 1　证明方程

$$x^2 + y^2 - 4z^2 = 3 \tag{5}$$

没有整数解.

证明　模 4,因整数的平方模 4 同余 0 或 1,故

$$(5)\text{的左边} \equiv 0,1,2 \pmod 4,$$

但右边 $\equiv 3 \pmod 4$. 即方程(5) 在 $\mathbf{Z}_4$ 中无解,从而它没有整数解.

例 2　证明方程

$$y^2 = x^3 + 7 \tag{6}$$

没有整数解.

证明　如果(6)有解,则 x 是奇数;否则将(6) 模 4 产生

$$y^2 \equiv 3 \pmod 4,$$

这不可能. 将(6)改写成

$$y^2 + 1 = (x + 2)((x - 1)^2 + 3) \tag{7}$$

因为 $(x-1)^2+3$ 模 4 同余于 3,故它必有一个素因子 $p \equiv 3 \pmod 4$. 现在将(7) 模 p,产生 $y^2 \equiv -1 \pmod p$,即 $\left(\frac{-1}{p}\right) = 1$,这不可能.

另一方面,一个自然的问题是:如果条件(i)和(ii)均得到满足,是否方程(1)必然有整数解?

对于最简单的一次不定方程(2),不难看出这一问题的回答是肯定的. 但一般情况下的答案并非总如此.

例 3　证明:方程

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0 \tag{8}$$

有实数解,且对所有 $m > 1$,同余方程

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \equiv 0 \pmod m \tag{9}$$

可解. 但方程(8)没有整数解.

证明　我们只要证明同余方程(9)对所有 $m>1$ 可解(其余断言均是显然的). 由前面的注记,我们只要对 $m=p^k$ 来证明就够了,其中 p 是任意素数,而 $k\geqslant 1$.

若素数 $p\neq 13,17,2$,由于

$$\left(\frac{221}{p}\right)=\left(\frac{13\cdot 17}{p}\right)=\left(\frac{13}{p}\right)\left(\frac{17}{p}\right),$$

故$\left(\frac{13}{p}\right),\left(\frac{17}{p}\right),\left(\frac{221}{p}\right)$不能同时为 -1. 因此三个同余方程

$$x^2\equiv 13 \pmod{p^k},$$
$$x^2\equiv 17 \pmod{p^k},$$
$$x^2\equiv 221 \pmod{p^k}$$

必有一个在 $k=1$ 时可解,进而它对所有 $k\geqslant 1$ 可解(参考习题10.14),从而(9)在 $m=p^k$ 时可解.

当 $p=13$ 或 17 时,由二次互反律知

$$\left(\frac{13}{17}\right)=\left(\frac{17}{13}\right)=1,$$

故上述结论也成立.

最后,由于 $17\equiv 1 \pmod 8$,故由习题 10.15 知,$x^2\equiv 17 \pmod{2^k}$ 对 $k\geqslant 1$ 均可解. 综合起来,就证明了我们的结论.

我们应当提及,能够证明,对于一大类重要的不定方程,条件(i)和(ii)也是它们有整数解的充分条件. 这是数论中相当深刻和迷人的结果,称为"局部—整体原则",也称为哈塞(Hasse)原理.

习　题　12

1. 证明下面的方程没有整数解:

(i) $2x^2-5y^2=7$;

(ii) $x^2 - 2xy^2 + 5z^3 + 3 = 0$.

2. 证明:方程 $x_1^4 + \cdots + x_{14}^4 = 1599$ 没有整数解.

3. 证明下面的方程仅有平凡整数解 $x = y = z = 0$:

(i) $x^2 - 3y^2 - 2z^2 = 0$;

(ii) $x^3 + 7y^3 + 49z^3 = 0$;

(iii) $x^2 + y^2 + z^2 = 2xyz$;

(iv) $x^2 + y^2 + z^2 = x^2y^2$.

4. 求方程 $x^2 - xy + y^2 - x - y = 0$ 的全部整数解.

5. 证明下面的方程没有整数解:

(i) $y^2 = 41x^3 + 3$;

(ii) $y^2 = x^3 - 6$.

6. 求所有正整数 m,n, 使得

$$1! + 2! + \cdots + m! = n^2.$$

§13. 费马方程

费马方程是指不定方程 $x^n + y^n = z^n$,其中 n 是大于 1 的正整数. 当 $n = 2$ 时,方程的一组正整数解相当于存在三边长为整数 x,y,z 的一个直角三角形. 我国古代《周髀算经》中就已记载有"勾广三,股修四,弦隅五",即一直角三角形三边长分别为 3,4,5. 现在我们将给出方程

$$x^2 + y^2 = z^2 \tag{1}$$

的全部整数解.

显然,我们可只考虑(1)的正整数解. 其次,如果 $d = (x,y)$,则由(1) 知 $d^2 | z^2$,于是 $d | z$. 令 $x = dx'$, $y = dy'$, $z = dz'$,则 x', y', z' 也满足(1),并且 $(x',y') = 1$. 因此我们只需求出(1) 中满足 $(x,y) = 1$ 的正整数解,这样的解称为(1) 的**本原解**. (易于看到,此时 x,y,z 实际上两两互素.) 最后,x,y 不能都是奇数,否则将(1) 模 4 产生

$$z^2 \equiv 2 \pmod 4.$$

所以 x,y 必须一奇一偶.

因此,为了我们的目的,只需证明下面的结果.

定理 1　不定方程(1)满足

$$(x,y)=1,\quad 2|y \tag{2}$$

的全部正整数解可表示成

$$x=a^2-b^2,\quad y=2ab,\quad z=a^2+b^2, \tag{3}$$

其中 a,b 是满足 $a>b>0$, a,b 一奇一偶且 $(a,b)=1$ 的任意整数.

证明　我们首先证明,对(1)的任一组满足条件(2)的正整数解 x,y,z,一定存在所说的整数 a,b,使 x,y,z 具有(3)的形式.

因 $2|y$ 及 $(x,y)=1$,故 x,z 均为奇数且 $(x,z)=1$. 因此 $\frac{z-x}{2}$, $\frac{z+x}{2}$ 都是整数,并且

$$\left(\frac{z-x}{2},\frac{z+x}{2}\right)=\left(\frac{z-x}{2}+\frac{z+x}{2},2\cdot\frac{z+x}{2}\right)$$
$$=(z,z+x)=(z,x)=1.$$

将(1)分解为

$$\frac{z-x}{2}\cdot\frac{z+x}{2}=\left(\frac{y}{2}\right)^2.$$

因上式右边是整数平方,故左边互素的两因数 $\frac{z-x}{2}$, $\frac{z+x}{2}$ 必须都是整数的平方(参考习题 2.8). 即有整数 $a>b>0$, $(a,b)=1$, 使得

$$\frac{z+x}{2}=a^2,\quad \frac{z-x}{2}=b^2,\quad y=2ab.$$

这时显然有 $x=a^2-b^2$, $y=2ab$, $z=a^2+b^2$. 又因为 z 为奇数,故 a,b 一奇一偶. 这就证明了定理 1 中第一部分.

反过来,因为

$$(a^2-b^2)^2+(2ab)^2=(a^2+b^2)^2,$$

故若 a,b 满足定理中说的条件，则(3) 给出的数都是(1) 的正整数解. 我们需证明这样的解满足(2)，即是(1) 的本原解.

$2|y$ 是明显的. 我们来证明 $(x,y)=1$. 设 $(x,y)=d$，则 $d|x,d|z$，即

$$d|(a^2-b^2) \quad \text{且} \quad d|(a^2+b^2),$$

从而 $d|2a^2,d|2b^2$，于是 $d|2(a^2,b^2)$. 因 $(a,b)=1$，所以 $(a^2,b^2)=1$. 这样，必须 $d|2$. 但 a,b 一奇一偶，这意味着 $x=x^2-b^2$ 是奇数，故只能 $d=1$. 证毕.

当 $n>2$ 时，费马方程 $x^n+y^n=z^n$ 的解呈现完全不同的情形. 当 $xyz=0$ 时，费马方程显然对所有 $n\geqslant 3$ 有整数解，这些解称为方程的**平凡整数解**. 然而，费马(大约于 1637 年) 曾写下(没有证明) 下面一个令人瞩目的断言：

当 $n\geqslant 3$ 时，$x^n+y^n=z^n$ 没有非平凡整数解.

这就是所谓的费马猜想. 自 1770 年欧拉首先对 $n=3$ 证明了上述断言始，几百年来，无数优秀的数学家都冲击过这一问题，虽然得出了极为丰富的成果，但均未成功. 直到 1995 年，费马的断言才被伟大的英国数学家安德鲁·怀尔斯(Andrew Wiles) 证明.

容易看出，为了证明费马猜想，只需对 $n=4$ 及 n 为奇素数的情形来证明就够了. 在这里我们只证明 $n=4$ 时费马方程无非平凡整数解. 这一工作是费马本人完成的，他实际上证明了下面的略强的结论.

定理 2　方程

$$x^4+y^4=z^2 \tag{4}$$

没有非平凡的整数解.

证明　反证法. 设(4)有一组整数解 $x_0y_0z_0\neq 0$. 可设 $x_0>0$，$y_0>0,z_0>0$. 我们在所有这样的解中选取一组使 z_0 最小的解. 论证的核心是造出(4) 的另一组正整数解 r,s,t 使 $t<z_0$. 由于 z_0 已选择为最小，这

就导出矛盾.

现在 x_0,y_0 必然互素;否则就有素数 $p|(x_0,y_0)$,从而 $p^2|z_0$. 而

$$\left(\frac{x_0}{p}\right)^4+\left(\frac{y_0}{p}\right)^4=\left(\frac{z_0}{p^2}\right)^2$$

表明,方程(4) 有一组新的正整数解. 但 $\frac{z_0}{p^2}<z_0$, 与 z_0 的选取矛盾.

将(4)改写为

$$(x_0^2)^2+(y_0^2)^2=z_0^2.$$

由于 $(x_0,y_0)=1$,故$(x_0^2,y_0^2)=1$. 于是(x_0^2,y_0^2,z_0) 是方程(1)的一组本原解. 由定理 1 知,存在整数 $a>b>0$, $(a,b)=1$, a,b 一奇一偶,使得(不妨设 y_0 是偶数)

$$x_0^2=a^2-b^2,\quad y_0^2=2ab,\quad z_0=a^2+b^2. \tag{5}$$

由

$$x_0^2+b^2=a^2 \tag{6}$$

及 $(a,b)=1$ 知,(x_0,b,a) 也是方程(1)的一组本原解;又 x_0 是奇数,故 b 是偶数. 再应用定理 1 知,存在整数 $c>d>0$, $(c,d)=1$, c,d 一奇一偶,使

$$x_0=c^2-d^2,\quad b=2cd,\quad a=c^2+d^2.$$

代入(5)得到

$$y_0^2=4cd(c^2+d^2),$$

即

$$\left(\frac{y_0}{2}\right)^2=cd(c^2+d^2).$$

因 $(c,d)=1$,易知 c,d,c^2+d^2 两两互素. 由上式知它们都是整数的平方,即有正整数 r,s,t, 使

$$c=r^2,\quad d=s^2,\quad c^2+d^2=t^2,$$

从而

$$r^4 + s^4 = t^2.$$

于是我们得出了(4)的一组正整数解 (r,s,t)，但

$$0 < t = \sqrt{c^2 + d^2} = \sqrt{a} < \sqrt{z_0} \leqslant z_0,$$

和 z_0 的最小性矛盾.

注记　定理 2 的证明方法，称为**无穷递降法**，这是费马首先提出的一个重要方法.

采用无穷递降法证明不定方程无正整数解(满足某些限制的解)的主要步骤为：从相反的结论出发，假设存在一组正整数解，设法造出这个方程(或一个同类方程)的另一组正整数解，而新的解比原来的解“严格地小”. 这里所说的严格地小，是指某一个与解有关的、取正整数值的量严格递减，这样的量可取为一组解的某个坐标(或坐标的绝对值)，或坐标的和、积等. 如果上述过程可以无限地进行下去，则由于严格递减的正整数数列只可能有有限多项，两者产生矛盾.

无穷递降法也可采用不同的形式(与上面说的实质相同)：假设存在正整数解，并从中选择一组“最小”的解；这里的最小解，是指某一个与解有关的、取正整数值的量达到最小. 论证的核心仍是设法造出方程的新的解，这新的解比已选择的解“严格地小”，由此产生矛盾. 定理 2 的证明便是这样做的，我们选择的量是方程(4) 的解的第三坐标 z.

无穷递降法，并不只是用于否定的方面. 如果方程有解，那么必有一组(或几组)达到“最小”的(正整数)解. 采用递降法，经过有限步后，必然达到最小解. (参考 § 14，定理 1 的证明.)

无穷递降法，不仅限于不定方程. 一个问题，如果能从一种状态产生另一种状态，并且有一个与状态有关的、取正整数值的量严格减少，就可以使用递降法，或者导出矛盾(即问题无解)或者产生所求的解. 例如，§ 2 中的欧氏算法实质上就是一种无穷递降法：经过有限步带余除法达到“最小状态”，产生了最大公约数. (参考 § 15，定理 6 下面的注记 2，以及 § 26，定理 1 的证明.)

习　题　13

1. 证明:两个连续正整数之积不能是完全平方,也不能为完全立方.

2. 求方程 $x^y = 2^z - 1$ 的全部正整数解,其中 x, y 都大于 1.

3. 求方程 $x^y = 2^z + 1$ 的全部正整数解,其中 $y > 1$.

4. 求所有的正整数 m, n,使 $2^m + 3^n$ 是完全平方.

5. 证明:不定方程 $3^x + 4^y = 5^z$ 仅有一组正整数解 $x = y = z = 2$.

6*. 求出单位圆周上的所有有理点(即坐标均为有理数的点).

7*. 证明:边长为整数的等腰三角形的面积不能是完全平方数.

8*. 证明:边长为整数的直角三角形的面积不能是完全平方数.

§14.　两整数的平方和

本节讨论哪些正整数可以表示为两个整数的平方和,即不定方程

$$x^2 + y^2 = n, \quad n > 0 \tag{1}$$

是否有整数解.研究这一问题的基本工具是下面的恒等式,

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2. \tag{2}$$

恒等式(2)蕴含着:如两个整数均可表示成两个整数的平方和,则它们的积也是两个整数的平方和.因此,我们的问题化为研究哪些素数 p 可表为两整数的平方和.由于素数 $2 = 1^2 + 1^2$.从而我们只需考虑 p 为奇素数的情形.

定理 1(欧拉 — 高斯)　设 p 为奇素数,则方程

$$x^2 + y^2 = p \tag{3}$$

有整数解的充分必要条件是 $p \equiv 1 \pmod 4$,并且此时方程(3)恰有一组正整数解(如不计解的次序).

证明　条件显然是必要的.(将方程(3)模4即可看出来,也见§12,例1.)

现在设 $p \equiv 1(\mathrm{mod}\ 4)$,我们分两步证明(3)有解.

第一步,因为 $\left(\frac{-1}{p}\right)=1$,从而同余方程 $x^2 \equiv -1(\mathrm{mod}\ p)$ 有整数解.我们可取其一个解 x,使 $1 \leqslant x \leqslant \frac{p}{2}$. 于是

$$x^2+1=mp. \tag{4}$$

由于

$$0<x^2+1 \leqslant \frac{p^2}{4}+1<p^2,$$

从而 $0<m<p$.

第二步,论证的关键是将(4)看作 p 的某个倍数可表为两整数平方和,即方程

$$x^2+y^2=mp \tag{5}$$

有整数解.设 m_0 是使(5)有解的最小的正整数 m,上面的论证表明 $1 \leqslant m_0<p$. 现在我们采用无穷递降法证明 $m_0=1$,由此就完成了定理的证明.

如 $m_0>1$,设 x_1,y_1 使 $x_1^2+y_1^2=m_0p$.选取 x_0,y_0 满足

$$x_1 \equiv x_0,\quad y_1 \equiv y_0(\mathrm{mod}\ m_0),\quad |x_0|,|y_0| \leqslant \frac{m_0}{2}. \tag{6}$$

如果 $x_0=y_0=0$,则 m_0 是 x_1 和 y_1 的公因子,从而 $m_0 \mid p$,这与 $m_0<p$ 矛盾.所以

$$0<x_0^2+y_0^2 \leqslant \frac{m_0^2}{2}.$$

现在

$$x_0^2+y_0^2 \equiv x_1^2+y_1^2 \equiv 0\ (\mathrm{mod}\ m_0),$$

从而 $x_0^2+y_0^2=m'm_0$,其中 $1 \leqslant m'<m_0$. 由(2)得出

$$m'm_0^2p=(x_1^2+y_1^2)(x_0^2+y_0^2)$$
$$=(x_1x_0+y_1y_0)^2+(x_1y_0-x_0y_1)^2.$$

由(6)得出

$$x_1x_0+y_1y_0\equiv x_1^2+y_1^2\equiv 0\ (\mathrm{mod}\ m_0),$$
$$x_1y_0-x_0y_1\equiv x_1y_1-x_1y_1\equiv 0\ (\mathrm{mod}\ m_0).$$

从而

$$m'p=\left(\frac{x_1x_0+y_1y_0}{m_0}\right)^2+\left(\frac{x_1y_0-x_0y_1}{m_0}\right)^2$$

表明，当 $m=m'$ 时方程(5)也有整数解；但 $0<m'<m_0$，这与 m_0 的定义矛盾.

最后还需证明，在方程(3)有解时，(如不计解的次序)仅有一组正整数解. 设

$$p=a^2+b^2=c^2+d^2,$$

其中 a,b,c,d 都是正整数. 我们要证明 $a=c$ 或者 $a=d$. 由于

$$(ac+bd)(ac-bd)=c^2(a^2+b^2)-b^2(c^2+d^2)$$
$$\equiv 0\ (\mathrm{mod}\ p).$$

故 $p|ac+bd$ 或者 $p|ac-bd$. 结合

$$p^2=(a^2+b^2)(c^2+d^2)=(ac\pm bd)^2+(ad\mp bc)^2,$$

可见 $ad-bc=0$ 或者 $ac-bd=0$. 在第一种情况下，我们有

$$\frac{a^2}{c^2}=\frac{b^2}{d^2}=\frac{a^2+b^2}{c^2+d^2}=1,$$

即 $a=c$(且 $b=d$). 类似地，在第二种情况下有 $a=d$(且 $b=c$). 证毕.

现在我们能对任意正整数 n，给出它是否为两整数平方和的判别法则.

定理2(高斯)　设n为正整数,则n可表为两整数平方和的充分必要条件是:如果n有素因子$q \equiv 3(\mathrm{mod}\ 4)$,则$q$在$n$的标准分解中的方幂为偶数.

证明　我们用S记所有可表为两整数平方和的正整数之集.则S具有性质:$a \in S$, $b \in S$蕴含着$ab \in S$.

首先设n具有定理中所说的性质,其标准分解为

$$n = 2^{\alpha} p_1^{\alpha_1} \cdots p_r^{\alpha_r} q_1^{\beta_1} \cdots q_s^{\beta_s},$$

这里p_i和q_j都是奇素数,且

$$p_i \equiv 1 \ (\mathrm{mod}\ 4)(1 \leqslant i \leqslant r),$$
$$q_j \equiv 3 \ (\mathrm{mod}\ 4) \ (1 \leqslant j \leqslant s).$$

因$\beta_1, \cdots, \beta_s$都是偶数,故$q_j^{\beta_j}$均是完全平方,从而属于S;又$2 \in S$及$p_i \in S$(定理1),反复用S的上述性质即知$n \in S$.

反过来,我们要证明S中每个数都具有定理中所说的性质.显然$1 \in S$,而1(没有素因子)具有所述性质.设S中每个小于n的正整数都具有所述性质,现在考虑n.如果n没有素因子$q \equiv 3 \ (\mathrm{mod}\ 4)$,则已无需证明.我们设有素数$q \equiv 3 \ (\mathrm{mod}\ 4)$使$q \mid n$.令$n = x^2 + y^2$,则

$$x^2 + y^2 \equiv 0(\mathrm{mod}\ q).$$

如果$q \nmid xy$,则

$$\left(\frac{x}{y}\right)^2 \equiv -1(\mathrm{mod}\ q),$$

于是

$$\left(\frac{-1}{q}\right) = 1,$$

这与$q \equiv 3(\mathrm{mod}\ 4)$矛盾.因此$q \mid x$或$q \mid y$.但$q \mid x^2 + y^2$,从而$q$必为$x$和$y$的公因子.于是

$$\frac{n}{q^2} = \left(\frac{x}{q}\right)^2 + \left(\frac{y}{q}\right)^2.$$

即 $\frac{n}{q^2}(<n)$ 为正整数并且属于 S. 由归纳假设，$\frac{n}{q^2}$ 具有定理所述的性质，从而 n 也如此.

注记　关于整数的平方和，有许多有趣和重要的结果. 除了本节中讲的定理 1 和定理 2 外，还有著名的拉格朗日四平方定理，即每个正整数都是四个整数的平方和. 此外，容易证明，形如 $4^a(8k+7)$ 的正整数不能表示成三个整数的平方和(习题 14.3)；反过来的命题也正确，这一困难的结果是勒让德于 1798 年首先证明的. 平方和问题的各种角度的研究与推广，也是现代代数与数论中一项重要内容.

习　题　14

1. 确定下面的整数中哪些可表示为两个整数的平方和：

$$54,171,282,379,487,6291,40003.$$

2*. (i) 确定哪些整数可表示为两个整数的平方差；

(ii) 证明：对任意整数 n，方程 $x^2+y^2-z^2=n$ 有无穷多组正整数解.

3*. 证明：形如 $4^a(8k+7)$ 的整数不能表示为三个整数的平方和.

4. 设 p 是素数，$p\equiv 3 \pmod 4$. 证明：对所有 $k\geqslant 1$，p^{2k} 不能表示为两个正整数的平方和.

5. 证明：对于任意给定的 $n\geqslant 1$，存在 n 个连续的正整数，其中每一个都不是两个整数的平方和.

第二部分

多 项 式

第六章　域上的一元多项式

§15. 带余除法与最大公因式

由引言中的讨论我们知道，系数在(整数环)**Z**、(有理数域)**Q**、(实数域)**R** 或(复数域)**C** 上的一元多项式的全体形成一个环. 类似地，我们可定义系数属于(模素数 p 的剩余类域)$\mathbf{F}_p$ 的多项式，以及加法、乘法、次数、恒为零等概念，并且易于验证所有这样的多项式也成为一个环，记作 $\mathbf{F}_p[x]$. 此外，我们通常将 $\mathbf{F}_p$ 中加法零元 $\bar{0}$ 及 $\mathbf{F}_p[x]$ 中零多项式 $\bar{0}$ 均简记为 0，而不作特别申明. 同样地，$\mathbf{F}_p$ 中乘法单位 $\bar{1}$ 简记为 1(在乘积中略去不写). 这样做的目的是便于统一地表述结论及其论证.

本章中，我们讲述系数属于域 K 的多项式环 $K[x]$ 的基本性质，这里 K 代表 **Q**、**R**、**C** 及 $\mathbf{F}_p$.

每个非零多项式，都对应一个非负整数，即它的次数. 这一简单的事实允许我们能够像在 **Z** 中那样对多项式作归纳论证. 我们将看到，第一章中证明 **Z** 具有唯一分解性的程序对于 $K[x]$ 仍然适用. 读者可对比地看 **Z** 上的论证与本节及下一节的处理手法.

下面的定理 1 是涉及多项式次数的基本结果(可比较 **Z** 上绝对值的性质).

定理 1　设 $f(x), g(x)$ 是 $K[x]$ 中非零多项式.

(i) 如 $f(x)+g(x)$ 非零，则 $\deg(f+g) \leqslant \max(\deg f, \deg g)$；

(ii) $\deg fg = \deg f + \deg g$.

证明　(i) 是显然的. 我们注意，这比绝对值所满足的三角不等式

强.

为了证明(ii),我们设

$$f(x) = a_n x^n + \cdots + a_0, \quad g(x) = b_m x^m + \cdots + b_0,$$

其中 $a_n \neq 0$ 及 $b_m \neq 0$. 由多项式的乘法规则知

$$f(x)g(x) = a_n b_m x^{n+m} + \text{低次项}.$$

因 $a_n b_m \neq 0$,从而

$$\deg fg = n + m = \deg f + \deg g.$$

推论　设 $f(x), g(x)$ 是 $K[x]$ 中非零多项式,则 $f(x)g(x)$ 也是非零多项式. 即 $K[x]$ 是一个无零因子环,从而其中(乘法)消去律成立.

注记　显然,当 K 取为 $\mathbf{Z}$ 时,定理 1 及推论中的结论仍然成立.

$K[x]$ 中的整除概念与 $\mathbf{Z}$ 中的整除性类似. 设 $f(x)$, $g(x) \in K[x]$, $g(x)$ 不为零. 如果存在 $h(x) \in K[x]$,使

$$f(x) = g(x)h(x),$$

则称 $g(x)$(在 $K[x]$ 中)**整除** $f(x)$,记作 $g(x) \mid f(x)$. 我们将 $g(x)$ 称为 $f(x)$ 的一个**因式**,而 $f(x)$ 称为 $g(x)$ 的一个**倍式**. 如不存在上述的 $h(x)$,就说 $g(x)$ **不整除** $f(x)$,记作 $g(x) \nmid f(x)$.

容易看到,对任意 $f(x) \in K[x]$,K 中任意非零常数均是其因式,而如果 $f(x) \neq 0$,则 $f(x)$ 也是它自身的一个因式. 此外,对 $f(x)$ 的任一因式 $g(x)$,唯一地决定了 $f(x)$ 的一个首项系数为 1 的因式 $g^*(x)$,其中 $\deg g = \deg g^*$.

由整除的定义,不难证明下面的结果(可比较 § 1,定理 1).

定理 2　设 $f(x), g(x), h(x) \in K[x]$.

(i) 如 $g(x) \mid f(x)$,且 $h(x) \neq 0$,则 $g(x)h(x) \mid f(x)h(x)$. 反之亦

然；

(ii) 如 $g(x)|h(x)$，且 $h(x)|f(x)$，则 $g(x)|f(x)$；

(iii) 如 $g(x)|f(x)$，$g(x)|h(x)$，则对任意的 $\alpha(x)$，$\beta(x)\in K[x]$，有

$$g(x)|(\alpha(x)f(x)+\beta(x)h(x));$$

(iv) 如 $g(x)|f(x)$，则或者 $f(x)=0$，或者 $\deg g\leqslant\deg f$. 此外，如果 $g(x)|f(x)$ 且 $f(x)|g(x)$，则

$$f(x)=cg(x),$$

这里 $c\in K$，$c\neq 0$.

证明　(i)—(iii)均是显然的，而(iv)可由定理 1(ii)推出来.

下面的定理 3 表明，域上的(一元)多项式环中能够建立带余除法，这是 $\mathbf{Z}$ 上带余除法的类似(§1，定理 2 及其注记)，多项式的次数起着与整数的绝对值相同的作用.

定理 3　设 $f(x)$，$g(x)\in K[x]$，且 $g(x)\neq 0$. 则存在 $K[x]$ 中多项式 $q(x)$ 与 $r(x)$ 使得

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

其中 $r(x)$ 或者为零，或者 $\deg r<\deg g$；并且**商式** $q(x)$ 及**余式** $r(x)$ 由这些条件唯一决定.

证明　如果 $f(x)=0$，或者 $\deg f<\deg g$，则可取 $q(x)=0$，$r(x)=f(x)$. 如 $g(x)$ 是常数，则可取 $q(x)=f(x)$，$r(x)=0$；我们因此设

$$\deg f\geqslant\deg g>0.$$

记 n，m 分别是 $f(x)$ 和 $g(x)$ 的次数，a_n，b_m 分别是 $f(x)$ 和 $g(x)$ 的首项系数. 令 $q_1(x)=a_nb_m^{-1}x^{n-m}$，并记

$$f_1(x) = f(x) - q_1(x)g(x).$$

易见或者 $f_1(x) = 0$ 或 $\deg f_1 < \deg f$. 如 $\deg f_1 \geqslant \deg g$，则对 $f_1(x)$ 重复上面过程. 如此进行，我们得出一列多项式

$$f_1(x), \cdots, f_i(x), \cdots, \quad 及 \quad q_1(x), \cdots, q_i(x), \cdots,$$

使得

$$f_{i+1}(x) = f_i(x) - q_{i+1}(x)g(x),$$

而

$$\deg f > \deg f_1 > \cdots > \deg g.$$

这一过程有限步后必然停止，即存在 l 使

$f_l(x) = 0$ 或 $\deg f_l < \deg g$（参考 §13，定理 2 的注记）.

于是 $q(x) = q_1(x) + \cdots + q_l(x)$ 及 $r(x) = f_l(x)$ 便给出了所说的表示.

为了证明唯一性. 假设 $f(x)$ 有两种符合定理中要求的表示法：

$$f(x) = g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x).$$

那么

$$(q_1(x) - q_2(x))g(x) = r_2(x) - r_1(x).$$

上式右边或者为零，或者次数 $< \deg g$；而左边或者是零，或者次数 $\geqslant \deg g$（参见定理 1）. 因此必须两边均为零，从而

$$q_1(x) = q_2(x) \text{ 及 } r_1(x) = r_2(x).$$

注记　1. 设 K' 是一个域，$K \subset K'$，我们称 K' 是 K 的一个扩张. 显然 $K[x] \subset K'[x]$，故定理 3 中的 $f(x)$ 与 $g(x)$ 可看作 $K'[x]$ 中多项式，且 $g(x)$ 在 $K'[x]$ 中不为零. 由 $K'[x]$ 中带余除法的唯一性可知，在 $K'[x]$ 中以 $g(x)$ 除 $f(x)$ 产生的除法算式与 $K[x]$ 中的算式(1)相同. 因此，带余除法算式不随域的扩张而改变.

2. 由于 $\mathbf{Z}$ 上不能作除法运算，由此易见 $\mathbf{Z}[x]$ 上不能建立像定理 3 那样的带余除法. 然而，如果 $f(x), g(x) \in \mathbf{Z}[x]$，$g(x) \neq 0$，且 $g(x)$

的首项系数为 1. 则与定理 3 相同的论证知，存在唯一确定的 $q_1(x)$，$r_1(x) \in \mathbf{Z}[x]$，使

$$f(x) = g(x)q_1(x) + r_1(x), \tag{2}$$

其中 $r_1(x)$ 或者为零，或者 $\deg r_1 < \deg g$.

对任一包含 $\mathbf{Z}$ 的域 K（例如复域 $\mathbf{C}$），整系数多项式 $f(x)$，$g(x)$ 可看作 $K[x]$ 中多项式，则由定理 3 知，等式(1)必然与(2)相同. 特别地，(1) 中的 $q(x)$ 及 $r(x)$ 分别与 $q_1(x)$ 及 $r_1(x)$ 恒等，均是整系数多项式.

由定理 3 及 §1，定理 3 的相同论证，我们有下面的

定理 4　设 J 是 $K[x]$ 的一个非空子集，具有下面的性质

(i) 对任意 $f(x), g(x) \in J$，有 $f(x) - g(x) \in J$；

(ii) 对任意 $f(x) \in J$ 及 $h(x) \in K[x]$，有 $f(x)h(x) \in J$.

则或者 $J = \{0\}$，或者存在唯一的首项系数是 1 的 $d(x) \in K[x]$，使 $J = (d(x))$. 这里（及以后）记号 $(d(x))$ 表示集合

$$\{d(x)h(x) \mid h(x) \in K[x]\}.$$

证明　如果 $J \neq \{0\}$，则 J 中有非零的多项式，设 $d(x)$ 是其中次数最低的（之一）；并且由(ii)可设 $d(x)$ 首项系数是 1. 我们证明 J 中任一多项式都是 $d(x)$ 的倍式. 事实上，对任意 $f(x) \in J$，由定理 3，存在 $q(x), r(x) \in K[x]$，使得

$$f(x) = d(x)q(x) + r(x),$$

其中 $r(x) = 0$ 或 $\deg r < \deg d$. 如 $r(x) = 0$ 则我们的断言成立. 否则，由于 $q(x)d(x) \in J$，故

$$r(x) = f(x) - d(x)q(x) \in J.$$

但 $\deg r < \deg d$，这与 $d(x)$ 的选取矛盾.

如果 $d_1(x)$ 是另一个首项系数为 1 的多项式，使 $J = (d_1(x))$. 则 $d(x) \mid d_1(x)$ 及 $d_1(x) \mid d(x)$. 从而必有 $d(x) = d_1(x)$（定理 2(iv)）. 因

此 $d(x)$ 是由 J 唯一决定的.

注记　满足定理 4 中条件的集合 J,称为 $K[x]$ 的理想. 定理 4 表明,$K[x]$ 中每个理想都是主理想,即由一个多项式的所有倍式构成. 因此 $K[x]$ 也是主理想环(参考 §1,定理 3 的注记).

由定理 4,我们推出

定理 5　设 $f(x),g(x),\cdots,h(x)$ 是 $K[x]$ 中(有限个)不全为零的多项式. 记

$$J=\{f(x)\alpha(x)+g(x)\beta(x)+\cdots+h(x)\gamma(x)\mid\alpha(x),\beta(x),\cdots,\gamma(x)\in K[x]\}.$$

则存在唯一的首项系数是 1 的多项式 $d(x)\in J$,使 $J=(d(x))$.

容易看出,定理 5 中的 $d(x)$ 整除 $f(x),g(x),\cdots,h(x)$,即 $d(x)$ 是 $f(x),g(x),\cdots,h(x)$ 的一个公因式. 又由于 $d(x)\in J$,故存在 $\alpha(x),\beta(x),\cdots,\gamma(x)\in K[x]$,使得

$$f(x)\alpha(x)+g(x)\beta(x)+\cdots+h(x)\gamma(x)=d(x).$$

因此,如 $d_1(x)$ 是 $f(x),g(x),\cdots,h(x)$ 的任一公因式,则有 $d_1(x)\mid d(x)$,从而

$$\deg d_1\leqslant\deg d.$$

由此易见 $d(x)$ 是 $f(x),g(x),\cdots,h(x)$ 的唯一的次数最高且首项系数是 1 的公因式,我们将它定义为 $f(x),g(x),\cdots,h(x)$ 的**最大公因式**,记作

$$d(x)=(f(x),g(x),\cdots,h(x)).$$

当 $(f(x),g(x),\cdots,h(x))=1$ 时,则称 $f(x),g(x),\cdots,h(x)$ 在 K 上**互素**,换句话说,$f(x),g(x),\cdots,h(x)$ 是互素的,指它们的公因式只有 $K[x]$ 中的非零常数.

由定理 5 推出

推论　设 $f(x),g(x),\cdots,h(x)\in K[x]$ 且不全为零，则存在 $\alpha(x),\beta(x),\cdots,\gamma(x)\in K[x]$，使得

$$\begin{aligned}&f(x)\alpha(x)+g(x)\beta(x)+\cdots+h(x)\gamma(x)\\=&(f(x),g(x),\cdots,h(x)).\end{aligned}$$

这称为 $K[x]$ 上的**裴蜀等式**. 特别地，如果 $f(x),g(x),\cdots,h(x)$ 互素，则存在 $\alpha(x),\beta(x),\cdots,\gamma(x)\in K[x]$，使得

$$f(x)\alpha(x)+g(x)\beta(x)+\cdots+h(x)\gamma(x)=1.$$

由上述推论极易建立(域上的)多项式的最大公因式的基本性质(与整数的最大公约数的性质类似，参见 §2，定理 3 及其证明).

定理 6　(i) $f(x),g(x),\cdots,h(x)$ 的任一公因式一定整除它们的最大公因式；

(ii) 设 $(f(x),r(x))=(g(x),r(x))=1$，则

$$(f(x)g(x),r(x))=1.$$

一般地，如果 $K[x]$ 中若干个多项式均与 $r(x)$ 互素，则它们的积也与 $r(x)$ 互素；

(iii) 设 $g(x)\mid f(x)h(x)$，且 $(g(x),h(x))=1$，则

$$g(x)\mid f(x).$$

注记　1. 上述最大公因式的定义的合理性依赖于定理 5(从而依赖于定理 4)，这与整数中最大公约数的定义不完全相同，因为若干个整数的最大的公约数的存在性与唯一性是不言自明的，但在多项式的情形则并非如此.

2. 设 $f(x),g(x),\cdots,h(x)\in K[x]$，则易知

$$(f(x),g(x),\cdots,h(x))=((f(x),g(x)),\cdots,h(x)).$$

由此可见，求 $K[x]$ 中两个以上的多项式的最大公因式，归结为求两个多项式的最大公因式. 对这一问题，我们有以下的**欧几里德算法**(类似于整数中的手法，参考 §13，定理 2 的注记)：

设 $f(x),g(x)\in K[x],g(x)\neq 0$. 因 $\deg g$ 是一个(有限)整数，于是按下述方式反复作带余除法，有限步后必然停止(即余式为零)：

以 $g(x)$ 除 $f(x)$：

$$f(x)=g(x)q(x)+r_0(x),\ \deg r_0<\deg g;$$

以 $r_0(x)$ 除 $g(x)$：

$$g(x)=r_0(x)q_1(x)+r_1(x),\ \deg r_1<\deg r_0;$$

$$\vdots$$

以 $r_{n-1}(x)$ 除 $r_{n-2}(x)$：

$$r_{n-2}(x)=r_{n-1}(x)q_n(x)+r_n(x),\ \deg r_n<\deg r_{n-1};$$

以 $r_n(x)$ 除 $r_{n-1}(x)$：

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

则易于证明

$$(f(x),g(x))=\frac{1}{a}r_n(x),$$

其中 a 是 $r_n(x)$ 的首项系数.

3. 由欧氏算法可见，$K[x]$ 中多项式的最大公因式可以仅用 K 中元素的四则运算求得(而不依赖于 K 的特殊性质). 此外，$K[x]$ 中带余除法的算式不随域 K 的扩张而改变(参考定理 3 的注记 1). 因此，如 K' 是 K 的一个扩张，则 $K[x]$ 中多项式 $f(x),g(x),\cdots,h(x)$ 在 $K[x]$ 中的最大公因式 $d(x)$，与它们(看作 $K'[x]$ 中多项式)在 $K'[x]$ 中的最大公因式 $d_1(x)$ 相同. 即最大公因式是不随域的扩张而改变的“绝对量”. 例如，若 $\mathbf{Q}[x]$ 中若干多项式在 $\mathbf{Q}$ 上互素，则它们在 $\mathbf{C}$ 上也互素.

证明上述的 $d(x)$ 与 $d_1(x)$ 相等，也可采用下面的方法：由定理 5 的推论知，存在 $\alpha(x),\beta(x),\cdots,\gamma(x)\in K[x]$，使得

$$f(x)\alpha(x)+g(x)\beta(x)+\cdots+h(x)\gamma(x)=d(x).$$

上式在 $K_1[x]$ 中仍成立，故有 $d_1(x)|d(x)$. 另一方面，$d(x)$ 是 $f(x),g(x),\cdots,h(x)$ 在 $K_1[x]$ 中的一个公因式，故 $d(x)|d_1(x)$. 由于 $d(x)$ 与 $d_1(x)$ 首项系数都是 1，因此 $d(x)=d_1(x)$.

习　题　15

1. (i) 设 n 是正整数，$\alpha\in K$. 证明：$x-\alpha$ 整除 $x^n-\alpha^n$；

(ii) 设 n 是正奇数，$\alpha\in K$. 证明：$x+\alpha$ 整除 $x^n+\alpha^n$.

2. 对下面的情形，用欧氏算法求 $(f(x),g(x))$：

(i) $K=\mathbf{Q}$, $f(x)=x^3+x-1$, $g(x)=x^2+1$；

(ii) $K=\mathbf{F}_2$, $f(x)=x^7+\bar{1}$, $g(x)=x^6+x^5+x^4+\bar{1}$；

(iii) $K=\mathbf{F}_3$, $f(x)=x^8+\bar{2}x^5+x^3+x^2+\bar{1}$, $g(x)=\bar{2}x^6+x^5+\bar{2}x^3+\bar{2}x^2+\bar{2}$.

3. 设 m,n 为正整数，证明：$K[x]$ 上多项式 x^m-1 与 x^n-1 的最大公因式是 $x^{(m,n)}-1$.

4. 设 $f(x),g(x)\in K[x]$，且 $f(x)$ 与 $g(x)$ 互素. 则对任意正整数 n，$f(x^n)$ 与 $g(x^n)$ 也互素.

5*. 设 $f(x),g(x)\in K[x]$ 且均非常数，$d(x)=(f(x),g(x))$，则存在 $\alpha(x),\beta(x)\in K[x]$，使得

$$d(x)=f(x)\alpha(x)+g(x)\beta(x);$$

并且 $\deg\alpha<\deg g$，$\deg\beta<\deg f$.

6. 求有理系数多项式 $\alpha(x)$ 和 $\beta(x)$，使得

$$x^3\alpha(x)+(1-x)^2\beta(x)=1.$$

7*. 设 $q(x)\in K[x]$，$q(x)\neq 0$. 证明：对任意 $f(x)\in K[x]$，存在多项式 $\alpha_0(x),\cdots,\alpha_m(x)$，使得

$$f(x)=\alpha_m(x)q^m(x)+\cdots+\alpha_1(x)q(x)+\alpha_0(x),$$

其中 $\alpha_i(x)$ 或者是零，或者 $\deg\alpha_i<\deg q(0\leqslant i\leqslant m)$；并且 $\alpha_0(x),\cdots,$

$a_m(x)$ 由这些条件唯一决定. 上述表达式,称为 $f(x)$ 的 $q(x)$ **进制展开**.

8*. 设 $f(x),g(x),\cdots,h(x)\in K[x]$,且均不为零.

(i) 证明: $f(x)$, $g(x)$, $\cdots$, $h(x)$ 的公倍式中,必有唯一的首项系数是 1 且次数最小的多项式,我们称之为 $f(x)$, $g(x),\cdots,h(x)$ 的最小公倍式,记作 $[f(x),g(x),\cdots,h(x)]$;

(ii) 证明: $f(x),g(x),\cdots,h(x)$ 的最小公倍式整除它们的任一公倍式;

(iii) 如 $f(x),g(x)$ 均不为零,则

$$a^{-1}f(x)g(x)=(f(x),g(x))[f(x),g(x)],$$

这里 a 是 $f(x)g(x)$ 的首项系数;

(iv) 证明: $[f(x),g(x),\cdots,h(x)]=[[f(x),g(x)],\cdots,h(x)]$;

(v) 如果 $f(x),g(x),\cdots,h(x)$ 两两互素,则

$$[f(x),g(x),\cdots,h(x)]=a^{-1}f(x)g(x)\cdots h(x),$$

这里 a 是 $f(x)g(x)\cdots h(x)$ 的首项系数.

9. 设 $m>1$ 且不是素数,记 $\mathbf{Z}_m[x]$ 是以 $\mathbf{Z}_m$ 中元素为系数的全体多项式,并按通常的方式定义其中的加法与乘法. 证明

(i) $\mathbf{Z}_m[x]$ 是一个交换环;

(ii) $\mathbf{Z}_m[x]$ 中有零因子,即存在 $f(x),g(x)\in\mathbf{Z}_m[x]$,且 $f(x)\neq\bar{0},g(x)\neq\bar{0}$,使 $f(x)g(x)=\bar{0}$. 事实上,$\mathbf{Z}_m[x]$ 中有无穷多个零因子;

(iii) $\mathbf{Z}_m[x]$ 中不能作带余除法. 确切地说,存在 $f(x)$, $g(x)\in\mathbf{Z}_m[x]$ 且 $g(x)\neq\bar{0}$,但没有 $q(x),r(x)\in\mathbf{Z}_m[x]$,满足

$$f(x)=g(x)q(x)+r(x),$$

其中 $r(x)$ 或是零,或 $\deg r<\deg g$.

§16. 唯一分解定理

一个多项式 $p(x)\in K[x]$ 称为 **K 上的不可约多项式**,是指

$\deg p \geqslant 1$，而 $p(x)$ 在 K 上仅平凡分解，即如果有一个分解 $p(x) = f(x)g(x)$，其中 $f(x), g(x) \in K[x]$，则

$$\deg f = 0 \quad 或 \quad \deg g = 0.$$

因此，除了一个常数倍数外，$p(x)$ 的因式只有其自身和 1(与 $\mathbf{Z}$ 中素数类似). 显然，如 $p(x) \in K[x]$ 是不可约多项式，则对任意 $a \in K$ $(a \neq 0)$，$ap(x)$ 也是 $K[x]$ 中不可约多项式.

我们注意，与最大公因式不同，多项式的不可约性可能随域的扩张而改变. 例如，$x^2 + 1$ 在 $\mathbf{R}$ 上不可约，但在 $\mathbf{C}$ 上可约.(参考 §15，定理 6 下面的注记 3.)

容易知道，$K[x]$ 中任一非常数多项式必有一个不可约多项式因式；此外，设 $p(x) \in K[x]$ 是一个不可约多项式，则对任意 $f(x) \in K[x]$，或者有 $p(x) \mid f(x)$，或者 $(p(x), f(x)) = 1$. 这些简单的事实可按定义与整数的情形类似地证明(参考 §3).

定理 1　$K[x]$ 中有无穷多个首项系数为 1 的不可约多项式.

证明　当 K 是无限域时，结论显然成立. 因对任意 $a \in K$，一次多项式 $x - a$ 都是 $K[x]$ 中不可约多项式. 如果 K 为有限域 $\mathbf{F}_p$，这一证明不能奏效. 此时我们采用欧几里德关于素数有无穷多个的论证(参考 §3，定理 1)：

设 $\mathbf{F}_p[x]$ 中仅有有限多个首项系数为 1 的不可约多项式，它们的全体是 $p_1(x), \cdots, p_k(x)$. 考虑 $\mathbf{F}_p[x]$ 中非常数多项式

$$f(x) = p_1(x) \cdots p_k(x) + \bar{1}.$$

$f(x)$ 必有首项系数为 1 的不可约因式 $q(x) \in \mathbf{F}_p[x]$，而 $q(x)$ 不同于 $p_i(x)(1 \leqslant i \leqslant k)$；否则 $q(x) \mid \bar{1}$，产生矛盾. 这一证明当然也适用于 K 为无限域的情形.

由 §15，定理 6(iii) 可推出不可约多项式的下述重要性质(类似于 §3，定理 2).

定理 2　设 $p(x)$ 是 $K[x]$ 中不可约多项式，如果 $K[x]$ 中多项式 $f(x),g(x),\cdots,h(x)$ 的积被 $p(x)$ 整除，则 $f(x),g(x),\cdots,h(x)$ 中（至少）有一个被 $p(x)$ 整除.

现在我们叙述并证明本节的主要结果：$K[x]$ 中的唯一分解定理（比较 §3，定理 3）.

定理 3　$K[x]$ 中任一正次数的多项式可分解为 $K[x]$ 中有限个首项系数为 1 的不可约多项式与 K 中常数之积；并且这些不可约多项式是唯一决定的（如不计它们在乘积中的次序）.

证明　分解的存在性是平凡的. 设 $f(x)\in K[x]$ 且 $\deg f\geqslant 1$. 如 $f(x)$ 不可约，则

$$f(x)=a\cdot(\frac{1}{a}f(x))$$

即是所需的分解（这里 a 是 $f(x)$ 的首项系数）. 如 $f(x)$ 可约，设 $f(x)=g(x)h(x)$，其中 $g(x),h(x)\in K[x]$，且 $0<\deg g,\deg h<\deg f$. 由此，所说的结论不难通过对 $\deg f$ 归纳而证明.

为了证明分解的唯一性，我们仍对 $\deg f$ 归纳. 当 $\deg f=1$ 时结论显然成立. 设结论对次数小于 n 的多项式已证明，现考虑 $\deg f=n$ 的情形. 设 $f(x)$ 有两种分解

$$f(x)=ap_1(x)\cdots p_k(x)=aq_1(x)\cdots q_l(x),$$

其中 $p_i(x),q_i(x)$ 均是 $K[x]$ 中首项系数为 1 的不可约多项式，$a\in K$. 由定理 2 知，$p_1(x)$ 整除某个 $q_i(x)(1\leqslant i\leqslant l)$，无妨设 $p_1(x)|q_1(x)$. 但 $q_1(x)$ 是（首项系数为 1 的）不可约多项式，故必须有

$$p_1(x)=q_1(x).$$

设

$$g(x)=ap_2(x)\cdots p_k(x)=aq_2(x)\cdots q_l(x).$$

如 $g(x)$ 是常数，则已证毕；如 $\deg g \geqslant 1$，因 $\deg g < \deg f$，故由归纳假设知，$g(x)$ 的分解唯一，即 $k = l$ 且 $p_2(x), \cdots, p_k(x)$ 是 $q_2(x), \cdots, q_l(x)$ 的一个排列. 证毕.

在 $f(x)$ 的上述分解中，设 $p_1(x), \cdots, p_l(x)$ 是出现的互不相同的首项系数为 1 的不可约多项式，则 $f(x)$ 可表示为乘积

$$f(x) = a p_1^{m_1}(x) \cdots p_l^{m_l}(x), \quad a \in K,$$

其中 $m_1, \cdots, m_l$ 是正整数，由 $p_1(x), \cdots, p_l(x)$ 唯一决定. 上面的分解称为 $f(x)$ 的**标准分解**. 由 §15，定理 1(ii)可见

$$m_1 \deg p_1 + \cdots + m_l \deg p_l = \deg f.$$

注记　§15 与 §16 中的论证与结果可概括为一句话：域上的一元多项式环类似于整数环. 现在我们总结一下两者(主要的)类似性：

首先，$K[x]$ 中的运算与 $\mathbf{Z}$ 中的运算类似(参考引言)；$K[x]$ 中非零多项式的次数，相当于 $\mathbf{Z}$ 中整数的绝对值；$K[x]$ 中的非零常数相当于 $\mathbf{Z}$ 中的数 ± 1；$K[x]$ 中首项系数为 1 的不可约多项式，相当于 $\mathbf{Z}$ 中的素数；并且 $K[x]$ 与 $\mathbf{Z}$ 有相似的带余除法，以此为工具，可以证明：

(i) $\mathbf{Z}$ 中每个非零理想均是主理想，并且由其中绝对值最小的非零数的倍数组成；

(i)′ $K[x]$ 中每个非零理想均是主理想，并且由其中次数最低的多项式的倍式组成.

(参考 §1，定理 3 以及 §15，定理 4.)

由上面的(i)及(i)′可类似地建立 $\mathbf{Z}$ 上最大公约数与 $K[x]$ 上最大公因式的基本性质. 特别地，能够证明：

(ii) 如 p 是 $\mathbf{Z}$ 中的素数，且 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$；

(ii)′ 如 $p(x)$ 是 $K[x]$ 中的不可约多项式，且 $p(x) \mid f(x)g(x)$，则

$$p(x) \mid f(x) \text{ 或 } p(x) \mid g(x).$$

(参考 §3，定理 2 及 §16，定理 2.)

最后，用(ii)及(ii)′可类似地证明 $\mathbf{Z}$ 及 $K[x]$ 均是唯一分解环.

习　题　16

1. 设 $p(x)\in K[x]$ 且 $\deg p\geqslant 1$. 如果对 $K[x]$ 中任意多项式 $f(x)$，或者有 $p(x)\mid f(x)$ 或有 $(p(x),f(x))=1$. 证明：$p(x)$ 是不可约多项式.

2. 设 $f(x),g(x)\in K[x]$ 且均非常数. 用 $f(x),g(x)$ 的标准分解表示它们的最大公因式及最小公倍式.

3*. 设 $f(x),g(x)\in K[x]$ 且 $g(x)\neq 0$. 表达式 $\dfrac{f(x)}{g(x)}$ 称为 K 上的**有理分式**.

(i) 设 $g(x)=a(x)b(x)$，其中 $a(x)$ 与 $b(x)$ 互素且均非常数；假设 $\deg f<\deg g$，则存在唯一确定的 $r(x),s(x)\in K[x]$，$\deg r<\deg a$，$\deg s<\deg b$，使得

$$\frac{f(x)}{g(x)}=\frac{r(x)}{a(x)}+\frac{s(x)}{b(x)};$$

(ii) 设 $g(x)$ 首项系数为 1，其标准分解是 $g(x)=\prod\limits_{i=1}^{l}p_i^{m_i}(x)$. 假设 $\deg f<\deg g$. 则存在唯一确定的多项式 $h_i(x)\in K[x]$，$\deg h_i<m_i\deg p_i(1\leqslant i\leqslant l)$，使得

$$\frac{f(x)}{g(x)}=\frac{h_1(x)}{p_1^{m_1}(x)}+\cdots+\frac{h_l(x)}{p_l^{m_l}(x)};$$

(iii) 设 $p(x)\in K[x]$ 是不可约多项式，m 是正整数. 则对任意 $h(x)\in K[x]$，$h(x)\neq 0$ 且 $\deg h<m\deg p$，存在唯一确定的多项式 $\alpha_i(x)\in K[x]\ (1\leqslant i\leqslant m)$，使得

$$\frac{h(x)}{p^m(x)}=\frac{\alpha_m(x)}{p(x)}+\cdots+\frac{\alpha_1(x)}{p^m(x)},$$

其中 $\alpha_i(x)$ 或者为零，或者 $\deg\alpha_i<\deg p$；

(iv) 证明：每一个分子的次数小于分母的次数，且分母有标准分解

$$f(x) = p_1^{m_1}(x)\cdots p_l^{m_l}(x)$$

的有理分式 $\frac{g(x)}{f(x)}$ 是**部分分式**的和，每个部分分式的分母是 $p_i^{k_i}(x)$ $(k_i = 1,\cdots,m_i,\ i = 1,\cdots,l)$，而分子或者是零，或者其次数小于 $\deg\ p_i$.

4. 将 **R** 上的有理分式

$$\frac{x+3}{(x+1)(x^2+2)},\quad \frac{x^4+2}{x(x^2+1)^2}$$

表示成部分分式的和.

§17. 多项式的零点

本节只需域 K 上的加、减、乘法运算，而无需作除法. 因此我们改用 D 表示环 **Z**,**Q**,**R**,**C** 及 $\mathbf{F}_p$.

设 $f(x) = a_kx^k + \cdots + a_1x + a_0 \in D[x]$. 对任意 $\alpha \in D$，令

$$f(\alpha) = a_k\alpha^k + \cdots + a_1\alpha + a_0. \tag{1}$$

则 $f(\alpha) \in D$. 由此对 $D[x]$ 中每个多项式，联系了一个由 D 映射到自身的**多项式函数**，多项式环 $D[x]$ 中不定元 x 可称为 D 上的变量. 表达式 (1) 称为 $f(x)$ 在 $x = \alpha$ 时的值，也称为 $f(x)$ 中以 α 代入.

由于我们约定了不定元 x 与 D 中元素的(形式)运算适合 D 中元素的运算规律(参考引言)，因此，如果

$$f(x) + g(x) = h(x),\quad f(x)g(x) = k(x),$$

则

$$f(\alpha) + g(\alpha) = h(\alpha),\quad f(\alpha)g(\alpha) = k(\alpha).$$

这些性质可简要地表示为

$$(f+g)(\alpha)=f(\alpha)+g(\alpha)\quad\text{和}\quad(fg)(\alpha)=f(\alpha)g(\alpha).\tag{2}$$

于是多项式之间的通过加、乘运算表示的关系在不定元用 D 中任一个元素代入后，仍保持成立.

如果 D 中的元素 α 使 $f(\alpha)=0$，则称 α 是多项式 $f(x)$ 的**零点**，或 $f(x)$ 的根.（有时也称 α 为方程 $f(x)=0$ 的根. 但我们应当注意，这里的方程是所谓的条件等式，并非指 $f(x)$ 为 $D[x]$ 中零元.）

$K=\mathbf{F}_p$ 的情形值得单独一提. 设 $f(x)=\bar{a}_nx^n+\cdots+\bar{a}_0\in\mathbf{F}_p[x]$，并记 $f^*(x)=a_nx^n+\cdots+a_0\in\mathbf{Z}[x]$，则 $\alpha=\bar{b}\in\mathbf{F}_p$ 是 $f(x)$ 的零点（即 $f(\alpha)=\bar{0}$），等价于说 $f^*(x)\equiv 0(\mathrm{mod}\ p)$ 有解 $x\equiv b(\mathrm{mod}\ p)$. 因此 $\mathbf{F}_p[x]$ 中多项式的零点，与 §7 中说的（整系数多项式）模 p 的同余方程之解（本质上）是一回事.

下面的定理 1，称为因式定理，表现了多项式零点的主要作用：由零点推断（形式）多项式的性状.

定理 1　设 $f(x)\in D[x]$，且 $x=\alpha\in D$ 是 $f(x)$ 的零点，则 $f(x)$ 被 $x-\alpha$ 整除；反之亦然.

证明　以 $x-\alpha$ 除 $f(x)$，得到

$$f(x)=(x-\alpha)q(x)+r,$$

这里 $q(x)\in D[x]$，而 $r\in D$ 是一个常数（参见 §15，定理 3 及其注记 2）. 以 $x=\alpha$ 代入上式，由 (2) 我们有 $r=f(\alpha)$，从而定理中的两个方面都得到了证明.

由定理 1 立即推出

定理 2　设 $f(x)\in D[x]$，$\alpha_1,\cdots,\alpha_k\in D$ 是 $f(x)$ 的不同的零点，则 $f(x)$ 被乘积 $(a-\alpha_1)\cdots(x-\alpha_k)$ 整除.

证明　$k=1$ 时，这就是定理 1；假设结论在 $k-1$ 时已成立，则有

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_{k-1})g(x),$$

其中 $g(x)\in D[x]$. 以 $x=\alpha_k$ 代入上式，得

$$(\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_{k-1})\,g(\alpha_k)=0.$$

由于 $\alpha_k-\alpha_i\neq 0(1\leqslant i\leqslant k-1)$ 且 D 中没有零因子(非零元的积不为零)，故必须 $g(\alpha_k)=0$. 由定理 1 知，$g(x)=(x-\alpha_k)h(x)$，这里 $h(x)\in D[x]$. 于是

$$f(x)=(x-\alpha_1)\cdots(x-\alpha_{k-1})(x-\alpha_k)h(x).$$

这就归纳证明了结论.

推论 1　$D[x]$ 中 n 次多项式至多有 n 个(不同的)零点.

推论 2　设 $D[x]$ 中多项式 $f(x)=a_nx^n+\cdots+a_1x+a_0$ 在 D 中至少有 $n+1$ 个(不同的)零点，则 $f(x)$ 是零多项式.

推论 3　设 D 为无限集合(即 $D=\mathbf{Z},\mathbf{Q},\mathbf{R}$ 或 $\mathbf{C}$)，$f(x)$，$g(x)\in D[x]$. 如果有无穷多个 $\alpha\in D$ 使 $f(\alpha)=g(\alpha)$，则 $f(x)=g(x)$(即 f 和 g 的同次幂的系数相等).

注记　1. 当 $D=\mathbf{F}_p$ 时，容易看到，推论 1 即是 §7 中的拉格朗日定理.

2. 当 D 为无限集合时，推论 3 表明，如 D 上的两个多项式 $f(x)$ 和 $g(x)$ 对所有 $\alpha\in D$ 满足 $f(\alpha)=g(\alpha)$，则 $f(x)=g(x)$. 因此，D 上的两个多项式作为(多项式)函数恒等，与它们作为(形式)多项式相等并无区别.

然而，在 D 为有限环 $\mathbf{F}_p$ 时，情况却很不相同. 例如，多项式 x^p-x 不是 $\mathbf{F}_p[x]$ 中零多项式，但对每个 $x\in\mathbf{F}_p$，它的值恒为零.

现在我们转向多项式的重根. 设 $f(x)\in D[x]$, $\alpha\in D$ 是 $f(x)$ 的一个零点. 如果 $f(x)$ 被 $(x-\alpha)^m$ 整除, 但不能被 $(x-\alpha)^{m+1}$ 整除, 则正整数 m 称为零点 α 的**重数**. 当 $m=1$ 时, 我们称 α 是 $f(x)$ 的**单根**(或单零点); 如 $m>1$ 则称 α 为 $f(x)$ 的(m 重) **重根**.

用多项式的**微商**容易确定其一个根是否为重根.

设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in D[x]$. 定义 $f(x)$ 的(形式的)微商 $f'(x)$ 为

$$f'(x)=na_nx^{n-1}+(n-1)a_{n-1}x^{n-2}+\cdots+a_1.$$

因此 $f'(x)$ 也属于 $D[x]$. 类似于微积分中的结果, 微商有如下的基本性质.

定理 3　设 $f(x),g(x)\in D[x]$, $a\in D$, 则

(i) $(f+g)'=f'+g'$;

(ii) 如 $a\in D$, 则 $a'=0$, 而 $(af)'=af'$;

(iii) $(fg)'=f'g+fg'$.

证明　(i), (ii)由定义易于证明. 为了证明(iii), 我们注意, 如 $f(x)=f_1(x)+f_2(x)$, 则由(i)知

$$\begin{aligned}(fg)'&=((f_1+f_2)g)'=(f_1g+f_2g)'\\&=(f_1g)'+(f_2g)';\end{aligned}$$

如 $g(x)$ 是两个多项式之和, 有类似的结果. 因此, 只需对特殊情形 $f(x)=ax^n$ 及 $g(x)=bx^m(a,b\in D)$ 证明(iii). 此时我们有

$$\begin{aligned}(fg)'&=(ax^n\cdot bx^m)'=(n+m)abx^{n+m-1}\\&=nax^{n-1}\cdot bx^m+ax^n\cdot mbx^{m-1}\\&=f'g+fg'.\end{aligned}$$

定理 4　设 $f(x)\in D[x]$, 且 $\deg f\geqslant 1$, $\alpha\in D$ 是 $f(x)$ 的一个零点, 则 α 是 $f(x)$ 的重零点的充分必要条件是 $f'(\alpha)=0$.

证明　设 α 是 $f(x)$ 的 m 重零点($m>1$)，即

$$f(x)=(x-\alpha)^m g(x),$$

这里 $g(x)\in D[x]$. 则

$$f'(x)=m(x-\alpha)^{m-1}g(x)+(x-\alpha)^m g'(x).$$

以 $x=\alpha$ 代入上式，得出 $f'(\alpha)=0$(注意 $m-1\geqslant 1$). 反过来，(由于 $f(\alpha)=0$) 我们设

$$f(x)=(x-\alpha)^m g(x),$$

其中 $g(\alpha)\neq 0$. 如果 $m=1$，则有

$$f'(x)=g(x)+(x-\alpha)g'(x),$$

于是 $f'(\alpha)=g(\alpha)\neq 0$，与假设矛盾. 从而必须 $m>1$.

习　题　17

1*. 设 $f(x)\in K[x]$，且 $\deg f=2$ 或 3. 则 $f(x)$ 在 K 上不可约的充分必要条件是 $f(x)$ 在 K 中无零点.

2. 确定 $\mathbf{F}_2[x]$ 与 $\mathbf{F}_3[x]$ 中所有 2 次及 3 次的首项系数为 1 的不可约多项式.

3. 设 $f(x)\in\mathbf{Z}[x]$，且 $f(0)\equiv f(1)\equiv 1\pmod 2$. 证明：$f(x)$ 没有整数根.

4*. 设 $f(x)=a_nx^n+\cdots+a_0\in\mathbf{Z}[x]$，$n\geqslant 1$，$a_na_0\neq 0$ 且 $(a_n,\cdots,a_0)=1$. 设 $\frac{b}{c}$ 是 $f(x)$ 的一个有理根，其中 $(b,c)=1$，则 $c\mid a_n$ 及 $b\mid a_0$. 特别地，首项系数为 ± 1 的整系数多项式的有理根必是整数.

5. 设 p 是素数，$f(x)\in\mathbf{Z}[x]$. 证明：$f(a)\equiv 0\pmod p$ 对所有整数 a 成立的充分必要条件是

$$f(x)=(x^p-x)g(x)+ph(x),$$

其中 $g(x),h(x)\in\mathbf{Z}[x]$.

6*. 设 $f(x) \in D[x]$,证明

(i) 如 $D \neq \mathbf{F}_p$,则 $f'(x) = 0$ 的充分必要条件是 $f(x)$ 为常数;

(ii) 如 $D = \mathbf{F}_p$,则 $f'(x) = 0$ 的充分必要条件是 $f(x) \in \mathbf{F}_p[x^p]$,即 $f(x) = g(x^p)$,其中 $g(x) \in \mathbf{F}_p[x]$.

7. 对 $f(x) \in K[x]$, $f(x)$ 的 n 阶微商递推地定义为:$f^{(0)} = f$, $f^{(n)} = (f^{(n-1)})'$(对 $n \geqslant 1$). 证明:对 $f(x), g(x) \in K[x]$, 我们有

$$(fg)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} f^{(n-i)} g^{(i)}.$$

8. 设 $f(x) \in K[x]$, $\alpha \in K$,证明:α 是 $f(x)$ 的 k 重根的充分必要条件是 $f^{(i)}(\alpha) = 0$(对 $0 \leqslant i \leqslant k-1$) 但 $f^{(k)}(\alpha) \neq 0$. 这里 k 是正整数且在 $K = \mathbf{F}_p$ 时 $k < p$.

9*. 当 x 取整数时,复系数多项式 $f(x)$ 之值为整数,则称这样的多项式为**整值多项式**.

(i) 记 $\binom{x}{k} = \dfrac{x(x-1)\cdots(x-k+1)}{k!}$($k$ 为正整数),则 $\binom{x}{k}$ 是 k 次整值多项式;

(ii) 证明:$\binom{x+1}{k} = \binom{x}{k} + \binom{x}{k-1}$;

(iii) 任一个 n 次整值多项式可表示为

$$a_n\binom{x}{n} + a_{n-1}\binom{x}{n-1} + \cdots + a_1\binom{x}{1} + a_0,$$

其中 $a_n, \cdots, a_0$ 均为整数,$a_n \neq 0$;且对任何整数 $a_n, \cdots, a_0$,上述多项式均为整值多项式;

(iv) 若一个 n 次多项式,对于连续 $n+1$ 个整数均取整值,则此多项式必是整值多项式.

§ 18. 多项式的同余式

设 $f(x), g(x), m(x) \in K[x]$ 且 $m(x) \neq 0$,如果

$$m(x)\mid(f(x)-g(x)),$$

则称 $f(x)$ 与 $g(x)$ **模** $m(x)$ **同余**，记作

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

(1) 式称为**模** $m(x)$**的同余式**.

多项式的同余式与整数中的同余式有着类似的性质：

定理 1　设 $f(x),g(x),h(x)\in K[x]$,则有

(i) (**返身性**)　$f(x)\equiv f(x)\pmod{m(x)}$;

(ii) (**对称性**)　如 $f(x)\equiv g(x)\pmod{m(x)}$,则

$$g(x)\equiv f(x)\pmod{m(x)};$$

(iii) (**传递性**)　如果

$$f(x)\equiv g(x)\pmod{m(x)},\ g(x)\equiv h(x)\pmod{m(x)},$$

则

$$f(x)\equiv h(x)\pmod{m(x)}.$$

定理 2　设 $f_i(x),g_i(x)\in K[x]$,且 $f_i(x)\equiv g_i(x)\pmod{m(x)}$ $(i=1,2)$. 则

(i) $f(x)\pm f_2(x)\equiv g_1(x)\pm g_2(x)\pmod{m(x)}$;

(ii) $f_1(x)f_2(x)\equiv g_1(x)g_2(x)\pmod{m(x)}$.

定理 1 表明，“模 $m(x)$ 同余”是 $K[x]$ 中的一个等价关系. 由此，类似于将 $\mathbf{Z}$ 按“模 m 同余”分类，我们可以将 $K[x]$ 中多项式分类：同一个类中的多项式彼此模 $m(x)$ 同余，不同类中的多项式模 $m(x)$ 不同余，每一个类称为模 $m(x)$ 的一个同余类. 与整数中的情形不同的是，模 $m(x)$ 的同余类的类数不必是有限的(参考 §4).

由定理 2，我们也能像在 $\mathbf{Z}_m$ 中作加、减、乘法运算那样，在模 $m(x)$ 的同余类中定义加、减、乘法运算；并且易于知道，这些运算满足通常的运算规律(参考 §5). 进一步，如果 $m(x)$ 是 K 上不可约多项式，则模

$m(x)$ 的同余类中还可以作除法，从而形成一个域（与 $\mathbf{F}_p$ 类似），但这样的域一般不是有限域. 这是代数学中构作域的基本手法，限于本书的目的，我们不作讨论. 这里只给出（整数环中的）中国剩余定理对于域上多项式环的推广.

定理 3　设 $m_1(x),\cdots,m_k(x)$ 是 $K[x]$ 中两两互素的多项式，$b_1(x),\cdots,b_k(x)$ 是 $K[x]$ 中任意多项式，则存在多项式 $f(x)\in K[x]$，使得

$$f(x)\equiv b_1(x)\ (\mathrm{mod}\ m_1(x)),\cdots,\ f(x)\equiv b_k(x)\ (\mathrm{mod}\ m_k(x));\tag{2}$$

所有这样的 $f(x)$ 形成模 $m_1(x)\cdots m_k(x)$ 的一个同余类. 特别地，在(2)的解中，有唯一的 $f(x)$，或为零或 $\deg f<\sum_{i=1}^{k}\deg m_i$.

证明　记 $M(x)=m_1(x)\cdots m_k(x)$，并由 $M(x)=M_i(x)m_i(x)$ $(1\leqslant i\leqslant k)$ 定义 $M_i(x)$. 则 $M_i(x)\in K[x]$，且 $(m_i(x),M_i(x))=1$ 及 $m_i(x)\mid M_j(x)$（对 $j\neq i$）. 由 §15，定理 5 的推论知，对于 $1\leqslant i\leqslant k$，存在 $h_i(x),l_i(x)\in K[x]$，使得

$$M_i(x)h_i(x)+m_i(x)l_i(x)=1.$$

记 $d_i(x)=M_i(x)h_i(x)$，则有

$$d_i(x)\equiv 1\ (\mathrm{mod}\ m_i(x)),\ d_i(x)\equiv 0\ (\mathrm{mod}\ m_j(x))\ (j\neq i).\tag{3}$$

于是

$$f(x)=b_1(x)d_1(x)+\cdots+b_k(x)d_k(x).\tag{4}$$

满足(2)中 k 个同余式（参考 §7，定理 3 的证明）.

如果 $f_1(x)$ 与 $f_2(x)$ 均满足定理中的要求，则 $f_1(x)-f_2(x)$ 被 $m_1(x),\cdots,m_k(x)$ 整除，从而被 $m_1(x)\cdots m_k(x)$ 整除（习题 15.8），即 $f_1(x)$ 与 $f_2(x)$ 在模 $M(x)$ 的一个同余类中.

最后，如果(4)给出的 $f(x)$ 不为零且 $\deg f \geqslant \sum_{i=1}^{k} \deg m_i$. 由带余除法，存在唯一确定的 $q(x), r(x) \in K[x]$，使

$$r(x) = f(x) - M(x)q(x),$$

且 $r(x) = 0$ 或 $\deg r < \deg M \left(= \sum_{i=1}^{k} \deg m_i\right)$. 易知 $r(x)$ 满足(2).

由定理 3 能够推出下面的**拉格朗日插值公式**.

定理 4　设 $a_0, a_1, \cdots, a_n$ 是 K 中 $n+1$ 个不同元素，$b_0, b_1, \cdots, b_n$ 是 K 中任意元素，则存在唯一确定的多项式 $f(x) \in K[x]$，$f(x)$ 或为零或 $\deg f \leqslant n$，满足

$$f(a_i) = b_i, \quad i = 0, 1, \cdots, n.$$

确切地说，$f(x)$ 由下式给出：

$$f(x) = \sum_{i=0}^{n} b_i \prod_{\substack{j=0 \\ j \neq i}}^{n} \frac{x - a_j}{a_i - a_j}. \tag{5}$$

证明　取 $m_i(x) = x - a_i (0 \leqslant i \leqslant n)$，则显然诸 $m_i(x)$ 是 $K[x]$ 中两两互素的多项式. 由定理 3，存在唯一确定的 $f(x) \in K[x]$，$f(x)$ 或为零或 $\deg f \leqslant n$，使得

$$f(x) \equiv b_i (\mathrm{mod}\ x - a_i) \quad (0 \leqslant i \leqslant n),$$

即

$$f(x) = b_i + (x - a_i)\, q_i(x) \quad (0 \leqslant i \leqslant n),$$

其中 $q_i(x) \in K[x]$. 以 $x = a_i$ 代入上式，即得 $f(a_i) = b_i (0 \leqslant i \leqslant n)$.

为了构造符合要求的 $f(x)$. 我们注意，诸 $d_i(x)$ 满足(3)，现在等价于说 $d_i(a_i) = 1$ 及 $d_i(a_j) = 0$ $(j \neq i)$. 由于这里 $\deg d_i \leqslant n$，故应取(参考 §17，定理 2)

$$d_i(x) = \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{x - a_j}{a_i - a_j}, \quad 0 \leqslant i \leqslant n.$$

这可看作定理 4 的特殊情形的解 ($b_i = 1$,而 $b_j = 0$ 对 $j \neq i$),将这些解"叠加"(即作线性组合,参考(4)),即得出(5).

习　题　18

1. 提出并证明 $K[x]$ 中同余式的消去律.

2. 求次数不超过 3 的多项式 $f(x) \in \mathbf{Q}[x]$,使得

$$f(-1) = -1,\ f(0) = 1,\ f(1) = 2,\ f(2) = 6.$$

3. 求出一个多项式 $f(x) \in \mathbf{F}_5[x]$,使得

$$f(\bar{0}) = f(\bar{1}) = f(\bar{4}) = \bar{1},$$

而 $f(\bar{2}) = f(\bar{3}) = \bar{3}$.

4. 设 $f(x) \in \mathbf{Q}[x]$ 是一个 n 次多项式,满足

$$f(k) = \frac{1}{k}(k = 1,2,\cdots,n+1).$$

求 $f(n+2)$.

5. 设 $f(x) \in \mathbf{Q}[x]$ 是一个 n 次多项式,满足

$$f(k) = 2^k(k = 1,2,\cdots,n+1).$$

求 $f(n+2)$.

6*. 设 φ 是 $\mathbf{F}_p$ 到自身的任一映射. 证明:存在 $f(x) \in \mathbf{F}_p[x]$,使得 $f(\alpha) = \varphi(\alpha)$ 对所有 $\alpha \in \mathbf{F}_p$ 成立.

7. 设 $f(x) \in \mathbf{F}_p[x]$, $\deg f = p - 2$. 若对所有 $\alpha \in \mathbf{F}_p(\alpha \neq 0)$ 有 $f(\alpha) = \alpha^{-1}$,试确定 $f(x)$.

8. 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x]$, $a_n \neq 0$,而 $x_0, x_1, \cdots, x_n$ 是互不相同的整数,则 $f(x)$ 在 $x_0, x_1, \cdots, x_n$ 上所取的值中,至少有一个的绝对值 $\geqslant \frac{n!}{2^n}|a_n|$.

第七章　代数基本定理

§19. 代数基本定理

我们知道，$K[x]$ 中首项系数为 1 的不可约多项式有无穷多个. 本节我们将对 $K = \mathbf{C}$ 及 $\mathbf{R}$ 的情形确定 $K[x]$ 中所有不可约的多项式. 这一问题的回答依赖于下面的重要结果：

定理 1(代数基本定理)　$\mathbf{C}[x]$ 中任一非常数的多项式至少有一个复根.

代数基本定理的证明超出了本书的范围，我们不予讨论. 由定理 1 我们有

推论　(i) $\mathbf{C}[x]$ 中不约多项式都是一次多项式.

(ii) $\mathbf{C}[x]$ 中任一 n 次多项式 $f(x)(n \geqslant 1)$，在 $\mathbf{C}$ 上可唯一地分解为

$$f(x) = a_n(x - \alpha_1)\cdots(x - \alpha_n), \tag{1}$$

其中 a_n 是 $f(x)$ 的首项系数；从而 n 次复系数多项式恰有 n 个复根(计入重根).

因此，设 $f(x)$ 互不相同的复根为 $\alpha_1, \cdots, \alpha_l$，它们的重数分别为 $m_1, \cdots, m_l$(于是 $m_1 + \cdots + m_l = n$). 则 $f(x)$ 可唯一地分解为

$$f(x) = a_n(x - \alpha_1)^{m_1}\cdots(x - \alpha_l)^{m_l}.$$

这是复系数多项式的标准分解.

证明　(i) 设 $p(x) \in \mathbf{C}[x]$ 是不可约多项式，$\deg p \geqslant 2$. 由定理 1

知 $p(x)$ 在 $\mathbf{C}$ 中有零点 α,即

$$p(x) = (x - \alpha)q(x)(\S 17,\text{定理 } 1).$$

但 $\deg q = \deg p - 1 \geqslant 1$,这与 $p(x)$ 的不可约性矛盾.

(ii) 这是(i) 及 $\mathbf{C}[x]$ 中唯一分解定理的推论($\S 16$,定理 3).

注记　设 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$,将(恒等式)(1)的右端展开,我们得出

$$\left.\begin{aligned}
&(\text{各根的和})\ \alpha_1 + \cdots + \alpha_n = -\frac{a_{n-1}}{a_n};\\
&(\text{各根两两乘积之和})\ \alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n = \frac{a_{n-2}}{a_n};\\
&\qquad\vdots\\
&(\text{各根之积})\ \alpha_1\cdots\alpha_n = (-1)^n\frac{a_0}{a_n}.
\end{aligned}\right\} \tag{2}$$

公式(2)就是著名的**韦达**(Viete)**定理**,它给出了方程的根与系数之间的关系.

设域 $K \subseteq \mathbf{C}$(即 K 为 $\mathbf{Q}$,$\mathbf{R}$ 或 $\mathbf{C}$),对 $f(x) \in K[x]$ 且非常数,代数基本定理断言其必有复根,却没有提供求根的实效方法.下面的结果使我们能够实际地确定 $f(x)$ 是否有重根,而不必求出根(参考 $\S 15$ 中的欧氏算法).

定理 2　设 $K \subseteq \mathbf{C}$,$f(x) \in K[x]$ 且 $\deg f \geqslant 1$,则 $f(x)$ 的所有复根都是单根的充分必要条件是 $f(x)$ 与 $f'(x)$ 互素.

证明　如果 $f(x)$ 有重根 α,则由 $\S 17$,定理 4 知,$f(x)$ 与 $f'(x)$ 在 $\mathbf{C}[x]$ 中有公因式 $x - \alpha$,从而它们在 $K[x]$ 中不互素.

反过来,如果 $f(x)$ 与 $f'(x)$ 不互素,它们在 $\mathbf{C}[x]$ 中有一个公共的不可约因式,这必然是一次的.从而有一个多项式 $x - \alpha \in \mathbf{C}[x]$ 整除 $f(x)$ 与 $f'(x)$,再由 $\S 17$,定理 4 知,$f(x)$(在 $\mathbf{C}$ 中)有重根.

现在我们确定 $\mathbf{R}[x]$ 中所有不可约多项式.

定理3　设 $f(x)\in\mathbf{R}[x]$ 是不可约多项式,则或者 $f(x)$ 是一次多项式,或者

$$f(x)=ax^2+bx+c,\quad \text{其中 } b^2-4ac<0.$$

证明　一次多项式当然是不可约的. 如果 $b^2-4ac<0$,则二次多项式 $f(x)=ax^2+bx+c$ 在 $\mathbf{C}$ 中有两个非实根,因此在 $\mathbf{R}$ 上不可约.

反过来,设 $f(x)$ 是一个不可约多项式且 $\deg f>1$,则 $f(x)$ 没有实根. 由代数基本定理,我们设 $\alpha=u+v\mathrm{i}$ 是 $f(x)$ 的一个非实根,其中 $u,v\in\mathbf{R}$ 且 $v\neq 0$. 令 $\bar{\alpha}=u-v\mathrm{i}$. 则

$$g(x)=(x-\alpha)(x-\bar{\alpha})=x^2-2ux+(u^2+v^2)$$

是二次实系数多项式. 由带余除法(§15,定理3),我们有

$$f(x)=g(x)q(x)+r(x),\tag{3}$$

这里 $q(x),r(x)\in\mathbf{R}[x]$,且 $r(x)=0$ 或 $\deg r\leqslant 1$. 将(3)看作 $\mathbf{C}$ 上的等式,并代入 $x=\alpha$,产生 $r(\alpha)=0$. 由于 $r(x)=cx+d$,其中 $c,d\in\mathbf{R}$. 于是有 $c\alpha+d=0$,但 α 非实数,故必须 $c=d=0$,进而 $r(x)=0$. 因此 $f(x)=g(x)q(x)$,这意味着 $q(x)$ 为(实)常数. 于是 $f(x)$ 是二次多项式,且没有实根,易知它必具有定理中说的形式.

由定理3及 $\mathbf{R}[x]$ 中多项式的唯一分解定理,我们有

推论　对任意 $f(x)\in\mathbf{R}[x]$,$\deg f\geqslant 1$,$f(x)$ 有标准分解

$$f(x)=a(x-\alpha_1)^{m_1}\cdots(x-\alpha_k)^{m_k}(x^2+a_1x+b_1)^{n_1}\cdots(x^2+a_lx+b_l)^{n_l},$$

其中 a 及诸 α_i,a_i,b_i 都是实数,$a_i^2-4b_i<0(1\leqslant i\leqslant l)$,且

$$m_1+\cdots+m_k+2n_1+\cdots+2n_l=\deg f.$$

我们看到 $\mathbf{C}[x]$ 及 $\mathbf{R}[x]$ 中不可约多项式具有相当简单的形式，其根本原因是每个(非常数的) 复系数多项式在 $\mathbf{C}$ 中必有零点，以及每个复数可唯一地表示为 $a+bi$ 的形式($a,b\in\mathbf{R}$). 然而，关于 $\mathbf{F}_p[x]$ 及 $\mathbf{Q}[x]$ 中的不可约多项式，结果则完全不同. 事实上，在这些情况下问题要复杂和困难得多. 例如，能够证明，对每个正整数 n，$\mathbf{F}_p[x]$ 中都存在 n 次不可约多项式，并且可以给出这样的多项式的个数. 此外，在 § 21 中将看到，$\mathbf{Q}[x]$ 中不可约多项式与 $\mathbf{Z}[x]$ 中不可约多项式本质上是一回事，而我们能给出一些充分条件判别 $\mathbf{Q}[x]$ 中一个多项式不可约. 例如，对每个 n，$\mathbf{Q}[x]$ 中都有 n 次不可约多项式.

另一方面，因为 $\mathbf{Q}\subset\mathbf{C}$，由 $\mathbf{Q}[x]$ 中多项式在 $\mathbf{C}$ 中必有根这一事实，我们能够给出 $\mathbf{Q}[x]$ 中不可约多项式的某些基本性质.

定理 4 设 $f(x)$ 是 $\mathbf{Q}[x]$ 中不可约多项式，则 $f(x)$ 在 $\mathbf{C}$ 中没有重根.

证明 因 $f(x)$ 在 $\mathbf{Q}$ 上不可约，又 $f(x)\nmid f'(x)$ (因 $\deg f'<\deg f$). 因此 $f(x)$ 与 $f'(x)$ 必然互素，由定理 2 即知 $f(x)$ 在 $\mathbf{C}$ 中没有重根.

定理 5 设 $f(x)\in\mathbf{Q}[x]$ 且 $f(x)$ 在 $\mathbf{Q}$ 上不可约. 如果 $g(x)\in\mathbf{Q}[x]$ 且 $f(x)$ 与 $g(x)$ 在 $\mathbf{C}$ 中有公共根，则必然 $f(x)\mid g(x)$.

证明 如果 $f(x)\nmid g(x)$，因 $f(x)$ 不可约，故 $(f(x),g(x))=1$. 于是(由 § 15，定理 5 的推论) 存在 $u(x),v(x)\in\mathbf{Q}[x]$，使

$$f(x)u(x)+g(x)v(x)=1.$$

这一等式在 $\mathbf{C}$ 上仍然成立. 以 $f(x)$ 与 $g(x)$ 的公共复根代入，得出 $1=0$，矛盾！因此必然 $f(x)\mid g(x)$.

我们也可采用下面的论证：因 $f(x)$ 和 $g(x)$ 在 $\mathbf{C}$ 中有公共根，故它

们在 $\mathbf{C}$ 上不互素；从而 $f(x)$ 与 $g(x)$ 在 $\mathbf{Q}$ 上也不互素(参考 §15，定理6 的注记 3)．因此现在必有 $f(x)|g(x)$．

定理 5 表明，$\mathbf{Q}$ 上不可约多项式的根必然是成族出现的：若 $\mathbf{Q}[x]$ 中一个多项式包含了其一个根，则必然包含其所有根．

习　题　19

1*．设 $f(x)\in\mathbf{R}[x]$，$\deg f\geqslant 1$．设 α 是 $f(x)$ 的一个复根，则 α 的共轭 $\bar{\alpha}$ 也是 $f(x)$ 的根．

2．设 $f(x)\in\mathbf{R}[x]$，如果对任意实数 x 有 $f(x)\geqslant 0$，则 $f(x)$ 是两个实系数多项式的平方和．

3*．设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbf{C}[x]$，$a_n\neq 0$，$\alpha$ 是 $f(x)$ 任一根，则

$$|\alpha|\leqslant 1+\max_{0\leqslant i\leqslant n-1}\left|\frac{a_i}{a_n}\right|.$$

4．设 $f(x)=a_nx^n+\cdots+a_1x+a_0\in\mathbf{Z}[x]$，其中 $0\leqslant a_i\leqslant 9$ $(0\leqslant i\leqslant n)$，且 $a_n\neq 0$．如 α 是 $f(x)$ 的一个复根，则 $\mathrm{Re}(\alpha)\leqslant 0$ 或者 $|\alpha|<4$．

§20. 单　位　根

一个复数 ζ 称为(复) **单位根**，如果对某个正整数 n，它满足方程

$$x^n-1=0. \tag{1}$$

方程(1)的 n 个根，记为 $\zeta_1,\cdots,\zeta_n$，称为 ***n* 次单位根**．由 §17，定理 4 知，这些根互不相同．因为，如记 $f(x)=x^n-1$，则 $f'(x)=nx^{n-1}$，从而

$$f'(\zeta_k)=n\zeta_k^{n-1}\neq 0(1\leqslant k\leqslant n).$$

今后我们用 μ_n 记 n 次单位根的集合．

我们熟知，由棣莫弗(De Moivre)公式可导出

$$\zeta_k = \cos\frac{2k\pi}{n} + \mathrm{i}\sin\frac{2k\pi}{n}, \quad k = 1,\cdots,n. \tag{2}$$

由此立即看出，在复平面上，μ_n 中的 n 个复数(对应的点) 恰好将单位圆周 $|z| = 1$ 分成 n 等份，其中一个分点为 $z = 1$.

设 ζ 是一个单位根. 我们将满足 $\zeta^d = 1$ 的最小正整数 d 称为 ζ 的**阶**. 例如，1 的阶是 1，而 -1 的阶是 2(当且仅当 n 为偶数时，$-1 \in \mu_n$).

如果 $\zeta \in \mu_n$ 且 ζ 的阶恰为 n，则称 ζ 是**本原的 n 次单位根**. 本原的 n 次单位根 与(整数中) 模 m 的原根(阶为 $\varphi(m)$) 有许多类似之处. 读者可以对照地看 §8 与这里的结果及论证.

引理 1　设 ζ 是一个单位根，其阶是 d. 如 m 是一个整数，则 $\zeta^m = 1$ 的充分必要条件是 $d|m$. 特别地，μ_n 中任一元素的阶均整除 n.

证明　与 §8，引理 1 的证明类似.

引理 2　设 ζ 是一个单位根，其阶为 d. 如 k 是一个整数，则 ζ^k 是一个阶为 $\frac{d}{(d,k)}$ 的单位根. 特别地，ζ^k 的阶为 d 的充分必要条件是 $(k,d) = 1$.

证明　与 §8，引理 3 的证明类似.

现在我们证明，本原的 n 次单位根“生成”μ_n 中所有单位根.

定理 1　如 ζ 是一个本原的 n 次单位根，则 μ_n 中所有单位根可表示成

$$\zeta^0 = 1, \zeta, \cdots, \zeta^{n-1}; \tag{3}$$

反过来，如果 ζ 是一个 n 次单位根，使 μ_n 中所有单位根可表示为(3) 的形式，则 ζ 是本原的.

证明　设ζ是一个本原的n次单位根. 显然,(3) 给出的n个数都满足方程(1),从而均属于μ_n. 因此我们只需证明它们互不相同. 假设

$$\zeta^i = \zeta^j,$$

其中$0 \leqslant i < j \leqslant n-1$,则$\zeta^{j-i} = 1$. 因$\zeta$的阶是$n$,故由引理 1 知$n \mid (j-i)$; 这不可能,因为$0 < j - i < n$.

反过来,设$\zeta \in \mu_n$,并使μ_n中所有单位根可表示为(3) 的形式. 设ζ的阶为d, 如果ζ不是本原的,即$d < n$,则ζ的任一幂次都是d次单位根. 特别地,(3) 中的n个数都是属于μ_d,即$\mu_n \subset \mu_d$. 这显然不可能,因μ_n中有n个不同的元素,而μ_d仅有d个元素.

注记　容易验证,μ_n中n个数对(复数的)乘法形成群. 定理1表明μ_n是一个循环群,且生成元是本原的n次单位根. (参考 §5 与 §8.)

我们现在确定μ_n中所有的本原单位根.

定理 2　μ_n中共有$\varphi(n)$个n次本原单位根. 确切地说,设

$$\zeta = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$

则全体本原的n次单位根为

$$\{\zeta^k \mid 1 \leqslant k \leqslant n,\quad (k,n) = 1\}. \tag{4}$$

证明　由棣莫弗公式及(2) 可见,μ_n中所有n次单位根ζ_k $(1 \leqslant k \leqslant n)$可表示为

$$\zeta^0, \zeta^1, \cdots, \zeta^{n-1}.$$

故由定理 1 知,ζ是μ_n中的一个本原的n次单位根. 再由定理 1 及引理 2 推出,$\varphi(n)$个数$\zeta^k (1 \leqslant k \leqslant n, (k,n) = 1)$是$\mu_n$中全部的本原的$n$次单位根.

推论　设 $n>1$，对每个正整数 d，$d|n$，在 μ_n 中恰有 $\varphi(d)$ 个阶为 d 的元素. 确切地说，如 ζ 是一个本原 n 次单位根，则 μ_n 中阶为 d 的元素为

$$S_d=\{\zeta^{\frac{n}{d}k}\mid 1\leqslant k\leqslant d,(k,d)=1\},\tag{5}$$

证明　与 §8，定理 4 的证明类似.

注记　对 $d|n$，设 S_d 如(5)所述. 则诸 S_d 显然形成 μ_n 的一个划分，而 μ_n 有 n 个元素，由上面的推论我们顺便导出了

$$\sum_{d|n}\varphi(d)=n.\tag{6}$$

(参考 §8，定理 1 的证明.)

习　题　20

1. 设 $f(x)\in\mathbf{C}[x]$，n 是正整数，如果 $(x-1)|f(x^n)$，则 $(x^n-1)|f(x^n)$.

2. 设 $f(x)\in\mathbf{C}[x]$ 且 $\deg f\geqslant 1$，n 是正整数. 如果 $f(x)|f(x^n)$，则 $f(x)$ 的根只能是零或单位根.

3*. 设 m,n 为整数且 $n>1$. 证明

$$\frac{1}{m}\sum_{x=1}^{m}e^{2\pi i nx/m}=\begin{cases}0, & \text{如果 } m\nmid n;\\ 1, & \text{如果 } m|n.\end{cases}$$

4*. 证明：同余方程 $f(x)\equiv 0(\bmod m)$ 的解数为

$$N=\frac{1}{m}\sum_{y=1}^{m}\sum_{x=1}^{m}e^{2\pi i f(x)y/m}.$$

由此推出同余方程 $ax\equiv b(\bmod m)$ 的解数是 (a,m)(如果 $(a,m)|b$) 或 0(如果 $(a,m)\nmid b$).

5*. 设 n 是整数且 $n>2$.

(i) 求所有 n 次单位根的和与积；

(ii) 求所有本原的 n 次单位根的和与积.

第八章　整系数多项式

§21. 本原多项式与唯一分解

本章研究整系数多项式环 $\mathbf{Z}[x]$.

$\mathbf{Z}[x]$ 中的整除及不可约的概念与 $K[x]$ 中的类似. 设 $f(x)$, $g(x) \in \mathbf{Z}[x]$, 如存在 $h(x) \in \mathbf{Z}[x]$, 使 $f(x) = g(x)h(x)$, 则称 $g(x)$ **整除** $f(x)$; 否则, 便称 $g(x)$ **不整除** $f(x)$. 如 $f(x) \in \mathbf{Z}[x]$, $\deg f \geqslant 1$, 而 $f(x)$ 仅有平凡的分解, 即不能分解为两个低次但非常数的(整系数)多项式之积, 则称 $f(x)$ 为 **$\mathbf{Z}$ 上的不可约多项式**, 否则称 $f(x)$(在 $\mathbf{Z}$ 上)可约(或可分解).

设 $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbf{Z}[x]$ 且 $f(x) \neq 0$, 我们将 $a_0, \cdots, a_n$ 的最大公约数 $(a_0, \cdots, a_n)$ 称为 $f(x)$ 的**容度**; 容度为 1 的多项式称为($\mathbf{Z}$ 上的) **本原多项式**. 显然, $\mathbf{Z}[x]$ 中任一非零多项式可分解为其容度与一个本原多项式的乘积. 我们将证明, $\mathbf{Z}[x]$ 中唯一分解定理也成立, 确切地说, 我们有

定理 1　$\mathbf{Z}[x]$ 中任一非常数的多项式可分解为一个整数与有限个(首项系数为正的)本原不可约多项式的乘积; 并且, 如不计(乘积中)因式的次序, 这些不可约多项式是唯一决定的.

为了证明定理 1, 需作一些准备工作. 我们首先证明下面重要的结果.

引理 1(高斯引理)　$\mathbf{Z}[x]$ 中两个本原多项式的乘积仍是一个本

原多项式.

证明　设有两个本原多项式

$$f(x) = a_n x^n + \cdots + a_0$$

及

$$g(x) = b_m x^m + \cdots + b_0$$

使得 $f(x)g(x)$ 不是本原的. 则有素数 p 整除 $f(x)g(x)$ 中所有系数. 因 $f(x)$ 是本原的，故 p 不能整除所有 a_i. 设 r 是最小下标使 a_r 不被 p 整除；类似地，设 s 是最小的下标使 b_s 不被 p 整除.

$f(x)g(x)$ 中 x^{r+s} 的系数为

$$\begin{aligned} &a_r b_s + a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots \\ &\quad + a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \cdots, \end{aligned}$$

这个和应该被 p 整除. 另一方面，由于对 $i \leqslant r-1, j \leqslant s-1$ 有 $p \mid a_i$ 及 $p \mid b_j$，故和中除第一项外，其余项都能被 p 整除，因此 $p \mid a_r b_s$. 因 p 是素数，故 $p \mid a_r$ 或 $p \mid b_s$，这与我们对 a_r, b_s 的选取相违.

注记　上述论证的最后一步应用了 §3，定理 2. 因此，高斯引理（本质上）依赖于 $\mathbf{Z}$ 上的唯一分解定理（参考 §3，定理 3 的注记 2）.

下面的引理表明，$\mathbf{Q}[x]$ 中每一个非零多项式，都本质上唯一地对应 $\mathbf{Z}[x]$ 中的一个本原多项式.

引理 2　设 $f(x) \in \mathbf{Q}[x]$ 且 $f(x) \neq 0$. 则存在一个有理数 $a \neq 0$，使得 $af(x)$ 是 $\mathbf{Z}[x]$ 中的本原多项式. 此外，如果有理数 $b \neq 0$，使 $bf(x)$ 也是 $\mathbf{Z}[x]$ 中的本原多项式，则 $a = \pm b$.

证明　设

$$f(x) = a_n x^n + \cdots + a_0,$$

这里 $a_0,\cdots,a_n$ 均是有理数且 $a_n \neq 0$. 取整数 e 使 $ea_0,\cdots,ea_n$ 都是整数，并令 $d = (ea_0,\cdots,ea_n)$. 则

$$\frac{e}{d}f(x) = \frac{ea_n}{d}x^n + \cdots + \frac{ea_0}{d}$$

是 $\mathbf{Z}[x]$ 中本原多项式.

此外，如果有理数 $a,b(ab \neq 0)$，使 $af(x)$ 和 $bf(x)$ 都是本原多项式. 设

$$af(x) = g(x),\quad bf(x) = h(x),$$

则有 $g(x) = \frac{b}{a}h(x)$. 因 $g(x),h(x)$ 均是本原的，故 $\frac{b}{a}$ 必须是整数，并且没有素因子，从而 $\frac{b}{a} = \pm 1$ 即 $a = \pm b$.

设 $f(x) \in \mathbf{Z}[x]$ 且非常数. 如果 $f(x)$ 在 $\mathbf{Z}$ 上有非平凡的分解，那么 $f(x)$ 在 $\mathbf{Q}$ 上当然也有非平凡的分解(因 $\mathbf{Z} \subset \mathbf{Q}$). 由引理 1 和引理 2，我们能够证明反过来的结论也成立.

定理 2　设 $f(x)$ 是 $\mathbf{Z}[x]$ 中一个本原多项式，且 $\deg f \geqslant 1$. 如果 $f(x)$ 在 $\mathbf{Q}$ 上有非平凡的分解. 则 $f(x)$ 在 $\mathbf{Z}$ 上也有非平凡的分解. 更确切地说，设 $f(x) = g(x)h(x)$，这里 $g(x),h(x) \in \mathbf{Q}[x]$ 且 $\deg g$，$\deg h \geqslant 1$. 则存在有理数 a 使

$$f(x) = ag(x) \cdot \frac{1}{a}h(x),\quad \text{且 } ag(x),\frac{1}{a}h(x) \in \mathbf{Z}[x].$$

证明　由引理 2 知，存在非零有理数 a,b 使 $ag(x)$ 和 $bh(x)$ 都是本原多项式. 记 $g_1(x) = ag(x),h_1(x) = bh(x)$. 则由 $f(x) = g(x)h(x)$ 产生

$$abf(x) = g_1(x)h_1(x).$$

由引理 1，$g_1(x)h_1(x)$ 是本原多项式，而(按假设)$f(x)$ 也是本原多项式，故 ab 必须是整数且没有素因子，所以 $ab = \pm 1$. 因此，上述的有理

数 a 使 $ag(x)$ 与 $\frac{1}{a}h(x)$ 都是(本原的)整系数多项式,由此得出我们的断言.

现在我们容易证明本节的主要结果.

定理 1 的证明　任一个非常数的整系数多项式 $f(x)$ 可(唯一地)分解为其(正、负)容度与一个首项系数为正的本原多项式的积.故我们只要对 $f(x)$ 为(首项系数是正的)本原多项式的情形证明结论.

(定理 1 中)所说的分解的存在性是显然的(注意,本原多项式的非常数的因式必是本原多项式).

为了证明分解的唯一性,设 $f(x)$ 有两种分解:

$$f(x) = p_1(x)\cdots p_k(x) = q_1(x)\cdots q_l(x),$$

其中 $p_i(x)$ 和 $q_j(x)$ 都是首项系数为正的本原不可约多项式.定理 2 表明,$\mathbf{Z}[x]$ 中一个本原不可约多项式在 $\mathbf{Q}[x]$ 中仍是不可约的,而 $\mathbf{Q}[x]$ 具有唯一分解性(参考 §16,定理 3),因此,将 $f(x)$(在 $\mathbf{Z}$ 上的)上述两种分解放到 $\mathbf{Q}$ 上看,我们便推出 $k = l$,以及对适当的有理数 a_i,使得 $a_1p_1(x),\cdots,a_kp_k(x)$ 是 $q_1(x),\cdots,q_k(x)$ 的一个排列.无妨设

$$a_ip_i(x) = q_i(x)(1 \leqslant i \leqslant k).$$

由于 $p_i(x)$ 和 $q_i(x)$ 均是首项系数为正的本原多项式,故必须 $a_i = 1(1 \leqslant i \leqslant k)$,即

$$p_i(x) = q_i(x) \quad (1 \leqslant i \leqslant k).$$

证毕.

注记　系数属于(整数)环的多项式与域上的多项式很不相同.我们已经看到,$K[x]$ 与 $\mathbf{Z}$ 的唯一分解性能够类似地论证的原因,在于两者都是所谓的主理想整环(参考 §16,定理 3 后面的注记).然而,容易得知,$\mathbf{Z}[x]$ 不是主理想整环(习题 21.4).因此,我们不能采用 §16 的论证来证明 $\mathbf{Z}[x]$ 的唯一分解性.

定理1的上述证明基于两个事实. 其一是 $\mathbf{Z}$ 的唯一分解性(参考引理1的注记);其二是每个有理数均可表示为两个整数之商(即所谓 $\mathbf{Q}$ 是 $\mathbf{Z}$ 的商域),而 $\mathbf{Q}[x]$ 是唯一分解环.

习　题　21

1*. 对 $f(x) \in \mathbf{Z}[x]$ 且 $f(x) \neq 0$,用 $c(f)$ 表示 $f(x)$ 的容度.

(i) 对任意 $a \in \mathbf{Z}, a \neq 0$,证明:$c(af) = |a|c(f)$;

(ii) 证明:$c(fg) = c(f) \cdot c(g)$.

2*. 设 $f(x)$ 是本原多项式,$g(x) \in \mathbf{Q}[x]$,且 $f(x)g(x) \in \mathbf{Z}[x]$,则 $g(x) \in \mathbf{Z}[x]$.

3. 设 $p(x) \in \mathbf{Z}[x]$ 是本原的不可约多项式,证明:对 $f(x)$, $g(x) \in \mathbf{Z}[x]$,若 $p(x) | f(x)g(x)$,则 $p(x) | f(x)$ 或 $p(x) | g(x)$.

4. 设 J 是由常数项为偶数的所有整系数多项式构成的集合.

(i) 证明:J 是 $\mathbf{Z}[x]$ 中的一个理想,即对任意 $f(x), g(x) \in J$,有 $f(x) - g(x) \in J$,并且对任意 $f(x) \in J$ 及 $r(x) \in \mathbf{Z}[x]$,有 $f(x)r(x) \in J$;

(ii) 证明:J 不是 $\mathbf{Z}[x]$ 的主理想,即不存在 $d(x) \in \mathbf{Z}[x]$,使

$$J = (d(x)) = \{d(x)r(x) | r(x) \in \mathbf{Z}[x]\}.$$

§22.　不可约多项式

在§19中我们确定了 $\mathbf{C}[x]$ 及 $\mathbf{R}[x]$ 中的所有不可约多项式. 判定 $\mathbf{Q}[x]$ 中的多项式是否(在 $\mathbf{Q}$ 上)不可约,(按 §21,定理2)等价于判别一个整系数多项式是否在 $\mathbf{Z}$ 上不可约,这一(在代数和数论中)重要的问题相当困难和复杂,我们这里仅提及几个较为基本的原则和手法.

最为经典和著名的判别法是下面的

定理 1(艾森斯坦(Eisenstein)判别法)　设

$$f(x) = a_n x^n + \cdots + a_0$$

是一个整系数多项式,其中 $n \geqslant 1$. 设存在一个素数 p,使得 $p \nmid a_n$, $p \mid a_i$(对 $i < n$) 但 $p^2 \nmid a_0$. 则 $f(x)$ 在 $\mathbf{Z}$ 上不可约(从而在 $\mathbf{Q}$ 上也不可约).

证明　我们讲述两种证明. 第一个证明是 §21,引理 1 中论证的变形. 假设有两个(非常数)整系数多项式

$$g(x) = b_k x^k + \cdots + b_0 \quad 及 \quad h(x) = c_l x^l + \cdots + c_0$$

使 $f(x) = g(x)h(x)$. 因 $a_0 = b_0 c_0$ 被 p 整除但不被 p^2 整除,故 b_0 与 c_0 中恰有一个被 p 整除,无妨设 $p \mid c_0$,又 $a_n = b_k c_l$ 不被 p 整除,故 $p \nmid c_l$. 现在我们可取最小的下标 r 使 $p \nmid c_r$. 显然 $r \neq 0$, 并且

$$a_r = b_0 c_r + b_1 c_{r-1} + \cdots + b_r c_0.$$

因为 $p \nmid b_0 c_r$,而和式中其余项都被 p 整除, 故 $p \nmid a_r$,这与定理中条件矛盾.

由定理 1 推出,对任意正整数 $n \geqslant 1$,多项式 $x^n + 2$ 在 $\mathbf{Z}$ 上均不可约. 因此 $\mathbf{Q}[x]$ 中存在任意次数的不可约多项式.

判断 $\mathbf{Z}[x]$ 中多项式是否不可约的一个基本手法是所谓(整系数多项式) 的模 p 约化(可比较 §12). 设

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{Z}[x].$$

将 $f(x)$ 的系数换为它们所属的模 p 的同余类,这唯一确定了 $\mathbf{F}_p[x]$ 中的一个多项式,记作 $\overline{f}(x)$. 即

$$\overline{f}(x) = \overline{a}_n x^n + \cdots + \overline{a}_1 x + \overline{a}_0 \in \mathbf{F}_p[x].$$

我们将 $\overline{f}(x)$ 称为 $f(x)$ 的**模 p 约化多项式**. 显然, 如果 $p \nmid a_n$, 则 $\deg f = \deg \overline{f}$. 又不难看出,模 p 的约化保持 $\mathbf{Z}[x]$ 中多项式的加法和

乘法，这可简单地表示为

$$\overline{f+g}=\overline{f}+\overline{g},\quad \overline{fg}=\overline{f}\cdot\overline{g}.$$

定理 2　设 $f(x)\in\mathbf{Z}[x]$ 且非常数，p 是一个素数，不整除 $f(x)$ 首项系数. 如果 $f(x)$ 模 p 约化多项式 $\overline{f}(x)$ 是 $\mathbf{F}_p[x]$ 中不可约多项式，则 $f(x)$ 在 $\mathbf{Z}$ 上不可约.

证明　假设 $f(x)$ 在 $\mathbf{Z}$ 上有非平凡的分解 $f(x)=g(x)h(x)$. 模 p 约化，产生

$$\overline{f}(x)=\overline{g}(x)\overline{h}(x).$$

因现在 $\deg f=\deg\overline{f}$，故 $\overline{g}(x)$ 与 $\overline{h}(x)$ 不是 $\mathbf{F}_p[x]$ 中常数. 从而上式给出 $\overline{f}(x)$ 在 $\mathbf{F}_p[x]$ 中一个非平凡的分解，与假设矛盾.

例如，考虑 $f(x)=x^3+2x+1$，我们不能应用定理 1. 然而 $f(x)$ 模 3 的约化为 $\overline{f}(x)=x^3+\overline{2}x+\overline{1}$，易知它在 $\mathbf{F}_3[x]$ 中不可约（习题 17.1），从而由定理 2 知 $f(x)$ 是 $\mathbf{Z}[x]$ 中不可约多项式.

即使 $\overline{f}(x)$ 在 $\mathbf{F}_p$ 上是可约的，因 $\mathbf{F}_p[x]$ 中唯一分解定理成立，有时仍能从 $\overline{f}(x)$ 的分解导出 $f(x)$ 在 $\mathbf{Z}$ 上的不可约性. 我们用这一手法给出定理 1 的另一种证明：

假设有 $f(x)$ 满足定理 1 的条件，但在 $\mathbf{Z}[x]$ 中有非平凡的分解 $f(x)=g(x)h(x)$. 模 p 约化得出

$$\overline{g}(x)\overline{h}(x)=\overline{a}_nx^n.$$

上式右端是（$\mathbf{F}_p[x]$ 中）非零常数与不可约多项式的 n 次幂之积，而 $\mathbf{F}_p[x]$ 具有唯一分解性，故 $\overline{g}(x)$ 与 $\overline{h}(x)$ 均是 $\mathbf{F}_p$ 中常数与 x 的正次幂的积，从而 $\overline{g}(x)$ 与 $\overline{h}(x)$ 的常数项都是 $\overline{0}$. 因此（回到 $\mathbf{Z}$ 看），$f(x)$ 的常数项被 p^2 整除. 矛盾！

另一方面，$f(x)$ 在 $\mathbf{Z}$ 上不可约，并非意味着一定存在一个素数 p，使其模 p 约化在 $\mathbf{F}_p[x]$ 中不可约(试比较 §12，例 1).

例 1　设 $f(x)=x^4+1$，则 $f(x)$ 在 $\mathbf{Z}$ 上不可约；但对每个素数 p，$f(x)$ 模 p 的约化多项式 $\overline{f}(x)$ 在 $\mathbf{F}_p[x]$ 中可约.

证明　$f(x)$ 在 $\mathbf{Z}$ 上不可约甚为容易，我们将这留给读者证明.

下面证明，对每个素数 p，$\overline{f}(x)$ 在 $\mathbf{F}_p[x]$ 中可约. 如 $p=2$，则

$$\overline{f}(x)=(x+\overline{1})^4.$$

当 $p>2$ 时，我们有

$$\begin{aligned}\overline{f}(x)&=(x^2)^2-(\overline{-1})=(x^2+\overline{1})^2-\overline{2}x^2\\&=(x^2-\overline{1})^2-(\overline{-2})x^2.\end{aligned}\tag{1}$$

由于

$$\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{-2}{p}\right)=\left(\frac{4}{p}\right)=1,$$

故

$$\left(\frac{-1}{p}\right),\left(\frac{2}{p}\right)\text{与}\left(\frac{-2}{p}\right)$$

中必有一个为 1，从而 $\overline{-1}$，$\overline{2}$ 与 $\overline{-2}$ 中必有一个是 $\mathbf{F}_p$ 中元素的平方，由(1) 即产生 $\overline{f}(x)$ 在 $\mathbf{F}_p[x]$ 中一个非平凡的分解.

由代数基本定理，$\mathbf{Z}[x]$ 中 $n(>1)$ 次多项式在 $\mathbf{C}$ 中必有 n 个根. 通过整系数多项式在 $\mathbf{C}$ 上分解的信息也能帮助判断其不可约性，这一手法与上面说的模 p 约化几乎“相反”，我们用一个例子说明其基本精神.

例 2　设 p 是一个素数，整数 $n>1$. 设

$$f(x)=a_nx^n+\cdots+a_1x+p\in\mathbf{Z}[x],$$

且 $\sum_{i=1}^{n}|a_i|<p$. 则 $f(x)$ 在 $\mathbf{Z}$ 上不可约.

证明　论证的出发点是 $f(x)$ 的复根之模均大于 1. 事实上，设 x_0 是 $f(x)$ 的一个根，而 $|x_0| \leqslant 1$，则

$$\begin{aligned} p = & |a_n x_0^n + \cdots + a_1 x_0| \leqslant |a_n||x_0|^n + \cdots + |a_1||x_0| \\ & \leqslant |a_n| + \cdots + |a_1|, \end{aligned}$$

与假设矛盾. 现在设 $f(x)$ 在 $\mathbf{Z}$ 上有非平凡的分解 $f(x) = g(x)h(x)$. 则

$$p = |f(0)| = |g(0)| \cdot |h(0)|. \tag{2}$$

($g(0), h(0)$ 实际上分别是 $g(x)$ 与 $h(x)$ 的常数项，从而均是整数). 设 b 是 $g(x)$ 的首项系数，则由韦达定理知，$\frac{g(0)}{b}$ 等于 $g(x)$ 的所有根之积. 但 $g(x)$ 的根都是 $f(x)$ 的根，从而它们的模都大于 1. 因此，$\left|\frac{g(0)}{b}\right| > 1$，故更有 $|g(0)| > 1$；同理 $|h(0)| > 1$. 所以 (2) 不能成立，因 p 是素数.

习　题　22

1. 证明下面的多项式在 $\mathbf{Q}[x]$ 中不可约：

(i) $x^4 + 3x + 5$；

(ii) $x^6 - 4x^3 + 6$；

(iii) $x^4 + 1$；

(iv) $3x^5 + 2x^4 - x^2 + 4x + 5$；

(v) $x^5 + 4x^4 + 2x^3 + 6x^2 - x + 5$.

2*. (i) 设 p 是素数，证明：$x^{p-1} + \cdots + x + 1$ 在 $\mathbf{Q}[x]$ 中不可约；

(ii) 设 $n > 1$ 是整数，证明：如 $x^{n-1} + \cdots + x + 1$ 在 $\mathbf{Q}[x]$ 中不可约，则 n 是素数.

3. 设 $a_1, \cdots, a_n$ 是互不相同的整数，证明：$(x - a_1)\cdots(x - a_n) - 1$ 在 $\mathbf{Q}[x]$ 中不可约.

4. 设 $p = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_0$ 是十进制表示的素数，

则多项式

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$$

在 $\mathbf{Q}[x]$ 中不可约.

5. 设 p 是素数. 证明：$\mathbf{F}_p[x]$ 中形如 $x^2 + \alpha x + \beta$ 的二次多项式中，共有 $\frac{p(p-1)}{2}$ 个不可约多项式.

6. 用模 p 约化的手法证明高斯引理（§21，引理 1）

§23. 分圆多项式

设 n 是正整数，以所有本原的 n 次单位根为根的多项式

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n} (x - \zeta^k), \quad \zeta = e^{\frac{2\pi i}{n}}$$

称为 **n 级分圆多项式**，其次数是 $\varphi(n)$ 且首项系数为 1. 很明显，$\Phi_n(x)$ 不依赖于本原的 n 次单位根 ζ 的选取（参考 §20）.

定理 1　我们有

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

证明　记 μ_n 为 n 次单位根之集. 对每个 $d|n$，设 S_d 是 μ_n 中阶为 d 的元素之集，由 §20，定理 2 的推论知，S_d 恰是 $\varphi(d)$ 个本原的 d 次单位根，故有（参见 §20 中(6)的证明）

$$x^n - 1 = \prod_{\alpha \in \mu_n} (x - \alpha) = \prod_{d|n} \prod_{\alpha \in S_d} (x - \alpha)$$

$$= \prod_{d|n} \Phi_d(x).$$

定理 2　$\Phi_n(x)$ 是整系数多项式.

证明　用归纳法，当 $n=1$ 时，$\Phi_1(x)=x-1\in\mathbf{Z}[x]$. 假设对所有正整数 $d<n$，均有 $\Phi_d(x)\in\mathbf{Z}[x]$. 令

$$g(x)=\prod_{\substack{d\mid n\\ d\neq n}}\Phi_d(x),$$

则 $g(x)\in\mathbf{Z}[x]$. 由定理 1，

$$x^n-1=g(x)\Phi_n(x). \tag{1}$$

由于 $g(x)$ 是首项系数为 1 的整系数多项式，由带余除法知，存在唯一确定的 $q(x),r(x)\in\mathbf{Z}[x]$ 使

$$x^n-1=g(x)q(x)+r(x), \tag{2}$$

其中 $r(x)$ 或者为零，或者 $\deg r<\deg g$. 现在将(2) 看作是 $\mathbf{C}[x]$ 中带余除法，与(1) 比较，由 §15，定理 3 中的唯一性便推出 $r(x)=0$ 及 $q(x)=\Phi_n(x)$(参考 §15，定理 3 的注记 2)，从而 $\Phi_n(x)\in\mathbf{Z}[x]$.

现在我们证明本节的主要结果：

定理 3　$\Phi_n(x)$ 是 $\mathbf{Z}[x]$ 中不可约多项式(从而在 $\mathbf{Q}$ 上也不可约).

由于 $\Phi_n(x)\in\mathbf{Z}[x]$ 且首项系数为 1，故其在 $\mathbf{Z}$ 上的任一不可约因式 $f(x)$ 的首项系数也是 1. 我们将证明 $f(x)$ 以所有本原的 n 次单位根为根，从而必须有 $f(x)=\Phi_n(x)$，即 $\Phi_n(x)$ 在 $\mathbf{Z}$ 上不可约. 论证的关键是下面的

引理　设 $f(x)$ 是 $\Phi_n(x)$ 在 $\mathbf{Z}$ 上的一个首项系数为 1 的不可约因式，p 是素数且 $p\nmid n$. 令 $\omega\in\mathbf{C}$ 是 $f(x)$ 的一个根，则 ω^p 也是 $f(x)$ 的一个根.

如果引理已证明，则不难推出定理 3. 设 ζ 是 $f(x)$ 的一个根，则 ζ 也是 $\Phi_n(x)$ 的根，故 ζ 是一个本原的 n 次单位根. 对任意整数 k，$2\leqslant k\leqslant n$ 且 $(k,n)=1$，将 k 分解为(不必互不相同的)素数的积：

$$k = p_1 \cdots p_s,$$

反复使用引理，我们由 $f(\zeta) = 0$ 推出 $f(\zeta^{p_1}) = 0$，从而 $f(\zeta^{p_1 p_2}) = 0, \cdots$. 最后，$f(\zeta^{p_1 \cdots p_s}) = 0$，即 $f(\zeta^k) = 0$. 由于 $\zeta^k (1 \leqslant k \leqslant n, (k,n) = 1)$ 恰给出所有本原的 n 次单位根（见 §20，定理 2），因此 $f(x)$ 以所有本原的 n 次单位根为根. 从而我们的断言得证.

现在我们证明引理，由假设，存在一个首项系数为 1 的多项式 $g(x) \in \mathbf{Z}[x]$，使得

$$x^n - 1 = f(x)g(x). \tag{3}$$

因 $f(\omega) = 0$，故 $\omega^n = 1$，更有 $(\omega^p)^n = 1$，即 ω^p 是 $x^n - 1$ 的根. 如果 $f(\omega^p) \neq 0$，则由 (3) 推出 $g(\omega^p) = 0$，这意味着 ω 是多项式 $f(x)$ 与 $g(x^p)$ 的公共根. 由于 $f(x)$ 在 $\mathbf{Q}$ 上不可约，故由 §19，定理 5 推出，$f(x)$（在 $\mathbf{Q}$ 上）整除 $g(x^p)$，即有 $h(x) \in \mathbf{Q}[x]$ 使得

$$g(x^p) = f(x)h(x). \tag{4}$$

因 $f(x)$ 的首项系数为 1，当然是本原多项式，由此及高斯引理知 $h(x)$ 实际上是整系数多项式（见习题 21.2）.

现在我们进入多项式环 $\mathbf{F}_p[x]$. 设 $\overline{f}(x), \overline{g}(x), \overline{h}(x)$ 分别是 $f(x)$，$g(x)$ 及 $h(x)$ 模 p 的约化多项式. 则由 (3)，(4) 我们（在 $\mathbf{F}_p[x]$ 中）有

$$x^n - \overline{1} = \overline{f}(x) \cdot \overline{g}(x) \tag{5}$$

和

$$\overline{g}(x^p) = \overline{f}(x) \cdot \overline{h}(x). \tag{6}$$

由于对任意 $\alpha \in \mathbf{F}_p$ 有 $\alpha^p = \alpha$（习题 6.7），因此，如果设

$$\overline{g}(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_1 x + \alpha_0,$$

则 $\overline{g}(x) = x^k + \alpha_{k-1}^p x^{k-1} + \cdots + \alpha_1^p x + \alpha_0^p$. 因此

$$\begin{aligned}\overline{g}(x^p) &= x^{pk} + \alpha_{k-1}^p x^{p(k-1)} + \cdots + \alpha_1^p x^p + \alpha_0^p \\ &= (x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_1 x + \alpha_0)^p \\ &= \overline{g}^{\,p}(x).\end{aligned}$$

现在等式(6)可改写为

$$\overline{g}^{p}(x) = \overline{f}(x) \cdot \overline{h}(x).$$

因 $\mathbf{F}_p[x]$ 具有唯一分解性，故 $\overline{f}(x)$（在 $\mathbf{F}_p[x]$ 中）任一不可约因式必整除 $\overline{g}(x)$，从而 $\overline{f}(x)$ 与 $\overline{g}(x)$ 不互素，任取它们的一个非常数公因式 $\lambda(x)$. 由等式(5) 知，$\lambda^2(x)$ 整除 $x^n - \overline{1}$. 令

$$x^n - \overline{1} = \lambda^2(x) \cdot A(x),$$

其中 $A(x) \in \mathbf{F}_p[x]$. 上式两边求微商，产生

$$nx^{n-1} = \lambda(x)(2\lambda'(x) \cdot A(x) + A(x)\lambda'(x)),$$

由此知 $\lambda(x) | nx^{n-1}$. 但 $\lambda(x)$ 是 $x^n - \overline{1}$ 的因式，因此，nx^{n-1} 与 $x^n - \overline{1}$（在 $\mathbf{F}_p[x]$ 中）有非常数公因式. 这显然导出矛盾：因为 $p \nmid n$，故 $nx^{n-1} \neq \overline{0}$，从而 nx^{n-1} 与 $x^n - \overline{1}$ 事实上是互素的. 引理证毕.

习　题　23

1*. 证明分圆多项式的下述性质：

(i) 如 n 是奇整数，且 $n > 1$，则

$$\Phi_{2n}(x) = \Phi_n(-x);$$

(ii) 如正整数 r 的素因子均整除 n，则

$$\Phi_n(x^r) = \Phi_{nr}(x);$$

(iii) 如 p 是素数，$p \nmid n$；s 为正整数，则

$$\Phi_n(x^{ps}) = \Phi_n(x^s)\Phi_{pn}(x^s);$$

(iv) 如 n 的不同素因子为 $p_1, \cdots, p_k$，则

$$\Phi_n(x) = \Phi_{p_1 \cdots p_k}(x^{np_1^{-1} \cdots p_k^{-1}}).$$

2*. 证明：$\Phi_n(x) = \prod_{d|n} (x^{n/d} - 1)^{\mu(d)}$，这里 μ 是墨比乌斯函数；由此给出 $\Phi_n(x)(n \leqslant 10)$ 的确切表达式.

3*. 设 k 是正整数，$k>1$. 证明：$\Phi_n(x^k)$ 在 $\mathbf{Q}$ 上不可约的充分必要条件是 k 的任一素因子均整除 n.

4. 设 n 是正整数，p 是素数，$p\equiv 1 \pmod{n}$. 证明：同余方程 $\Phi_n(x)\equiv 0 \pmod{p}$ 恰有 $\varphi(n)$ 个解，它们是模 p 的 n 阶元.

第九章　多元多项式

§ 24. 唯一分解与恒等定理

本章中我们考虑环 D 上的多元多项式环 $D[x_1,\cdots,x_n]$. 这里的 D 为 **Z**,**Q**,**R**,**C** 或 $\mathbf{F}_p$.

$D[x_1,\cdots,x_n]$ 中每一个多项式 F 具有形式

$$F(x_1,\cdots,x_n)=\sum_{i_1,\cdots,i_n} a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}, \tag{1}$$

其中系数 $a_{i_1\cdots i_n}\in D$,而 $i_1,\cdots,i_n$ 为非负整数,满足

$$0\leqslant i_1\leqslant d_1,\quad\cdots,\quad 0\leqslant i_n\leqslant d_n.$$

(1)中的表示可改写成

$$F(x_1,\cdots,x_n)=\sum_{i_n=0}^{d_n}\Big(\sum_{i_1,\cdots,i_{n-1}} a_{i_1\cdots i_n}x_1^{i_1}\cdots x_{n-1}^{i_{n-1}}\Big)x_n^{i_n};$$

从而 F 可以表示为

$$F(x_1,\cdots,x_n)=\sum_{j=0}^{d_n}F_j(x_1,\cdots,x_{n-1})x_n^j, \tag{2}$$

其中 F_j 是(不定元为 $x_1,\cdots,x_{n-1}$ 的)$n-1$ 元多项式.

我们称每一项 $a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n}$ 为**单项式**,并且在 $a_{i_1\cdots i_n}\neq 0$ 时,定义这**单项式的次数**为诸 x_i 的幂次之和,即

$$\deg(a_{i_1\cdots i_n}x_1^{i_1}\cdots x_n^{i_n})=i_1+\cdots+i_n.$$

如果一个多项式 F 的所有具有非零系数的单项式均有次数 d,则称 F 为 **d 次齐次多项式**,或 d 次型.

对(1) 给出的 n 元多项式,我们将其次数相同的单项式收集在一

起，可将 F 唯一地表示为齐次部分的和：

$$F = F_{k_1} + \cdots + F_{k_r}, \tag{3}$$

其中 F_{k_i} 是 k_i 次齐次式(称为 F 的一个**齐次部分**)，而 $0 \leqslant k_1 < \cdots < k_r$.

当 F 表示为(3)的形式时，我们将 k_r 定义为 F 的**总次数**(简称次数)，记作 $\deg F = k_r$. 换句话说，F 的次数是指其次数最高的齐次部分的次数.

我们注意，F 的次数与 F 关于某个不定元的次数是两个不同的概念. 例如，将 F 表示为形式(2)，如 d 是最大的下标使 $F_d(x_1, \cdots, x_{n-1})$ 为非零多项式，则我们说 F 关于 x_n 的次数为 d.

我们在引言中已提及 $D[x_1, \cdots, x_n]$ 中的元素可定义加、减与乘法运算，$D[x_1, \cdots, x_n]$ 对这些运算形成一个(交换)环. 此外，我们在 §15 中证明过，D 上的一元多项式环没有零因子，这一结论对 $D[x_1, \cdots, x_n]$ 也成立，从而 $D[x_1, \cdots, x_n]$ 中消去律成立.

定理 1　设 F, G 是 $D[x_1, \cdots, x_n]$ 中两个非零多项式，则 FG 也是非零多项式.

证明　归纳法. 当 $n = 1$ 时结论已得出证明. 假设结论在 $n - 1$ 时已成立，现在设 F, G 均是 n 元(非零多项式)，由(2)，我们将 F, G 表示为

$$F(x_1, \cdots, x_n) = \sum_{j=0}^{k} F_j x_n^j, \quad G(x_1, \cdots, x_n) = \sum_{j=0}^{l} G_j x_n^j.$$

其中 F_j, G_j 均属于 $D[x_1, \cdots, x_{n-1}]$，且 $F_k \neq 0, G_l \neq 0$. 显然，FG 中关于 x_n 的最高次幂为 x_n^{k+l}，其“系数”为 $F_k \cdot G_l \neq 0$(归纳假设). 从而 FG 不是零多项式.

推论　设 F, G 中是 $D[x_1, \cdots, x_n]$ 中两个非零多项式，则

$$\deg FG = \deg F + \deg G.$$

证明　将 F 与 G 表示为齐次部分的和：

$$F=\sum_{i=1}^{r}F_{k_i},\quad G=\sum_{j=1}^{s}G_{l_j},$$

其中 $0\leqslant k_1<\cdots<k_r$，$0\leqslant l_1<\cdots<l_s$. 则

$$FG=\sum_{i,j}F_{k_i}G_{l_j}. \tag{4}$$

由定理 1 知每一项 $F_{k_i}G_{l_j}$ 都非零多项式. 又易见 $F_{k_i}G_{l_j}$ 是齐次式且次数为 k_i+l_j. 于是 $F_{k_r}G_{l_s}$（在(4)式右端只出现一次）是 FG 的次数最高的齐次部分. 从而

$$\deg FG=k_r+l_s=\deg F+\deg G.$$

多元多项式的整除及不可约的概念与一元多项式的情形类似. 设 $F,G\in D[x_1,\cdots,x_n]$ 且 G 非零. 如果存在 $H\in D[x_1,\cdots,x_n]$ 使 $F=GH$，则称 G **整除** F，记作 $G|F$，并且称 G 是 F 的一个**因式**. 按定义不难建立关于多元多项式整除的基本性质（类似于 §15，定理 1），我们略去细节.

设 $P\in D[x_1,\cdots,x_n]$，且 P 非常数，如果 P 在 $D[x_1,\cdots,x_n]$ 中没有除常数之外的因式，则称 P 是 $D[x_1,\cdots,x_n]$ 中的**不可约多项式**. 例如，次数为 1 的多项式是不可约多项式.

下面的唯一分解定理是 §16，定理 3 及 §21，定理 1 的推广.

定理 2　设 $F\in D[x_1,\cdots,x_n]$ 且 $\deg F\geqslant 1$. 则 F 可分解为 $D[x_1,\cdots,x_n]$ 中有限个不可约多项式的积；并且，如果不计常数因子及乘积中因式的次序，这些不可约多项式是唯一决定的.

注记　定理2的第一部分，即 F 具有所说的分解，不难由上述推论通过对 $\deg F$ 归纳来证明. 但分解的唯一性的论证则较为复杂，其细节本书略去. 我们这里仅提及其基本精神：

容易知道，当 $n\geqslant 2$ 时，$D[x_1,\cdots,x_n]$ 没有像 §15，定理 3 那样的带余除法；并且也不是主理想整环. 因此我们不能采用 §16 的方法证明

分解的唯一性.

论证可采用对 n 归纳,并推广 §21 的处理来进行. 当 $n=1$ 时,结论已在前面证明过. 我们归纳地假设 $D[x_1,\cdots,x_{n-1}]$ 是唯一分解环. 注意 $D[x_1,\cdots,x_n]$ 中的 n 元多项式可看作以 $n-1$ 元多项式环 $D[x_1,\cdots,x_{n-1}]$ 中元素为"系数",而以 x_n 为不定元的一元多项式环(参考(2)). 由于 $D[x_1,\cdots,x_{n-1}]$ 具有唯一分解性,我们可定义其中的最大公因式,以及本原多项式等概念,并证明类似的高斯引理(参考 §21,引理 1 的注记). 此外,类似于由 $\mathbf{Z}$ 构作域 $\mathbf{Q}$,我们能够由 $D[x_1,\cdots,x_{n-1}]$ 构作其"商域",其元素为 $D[x_1,\cdots,x_{n-1}]$ 中两个多项式之商(分母不为零),称为不定元 $x_1,\cdots,x_{n-1}$ 的有理函数域,记为 $D(x_1,\cdots,x_{n-1})$. 采用 §15 与 §16 的类似论证,可以证明,以域 $D(x_1,\cdots,x_{n-1})$ 中元素为"系数",x_n 为不定元的多项式环 $D(x_1,\cdots,x_{n-1})[x_n]$ 中可以作带余除法,从而是唯一分解环. 进而,推广 §21 的手法便能够证明 $D[x_1,\cdots,x_n]$ 也是唯一分解环($D[x_1,\cdots,x_{n-1}]$ 相当于 $\mathbf{Z}$,而 $D(x_1,\cdots,x_{n-1})[x_n]$ 则相当于 $\mathbf{Q}[x]$).

对给定的 $F\in D[x_1,\cdots,x_n]$,将 F 分解为不可约多项式的积通常相当困难. 下面的因式定理提供了确定 F 的因式的一种基本方法(比较 §17,定理 1).

定理3　设 $F(x_1,\cdots,x_n)\in D[x_1,\cdots,x_n]$,且关于的 x_n 次数至少是 1. 如果有一个 $n-1$ 元多项式 $G(x_1,\cdots,x_{n-1})\in D[x_1,\cdots,x_{n-1}]$,使得当 x_n 换为 $G(x_1,\cdots,x_{n-1})$ 时,F 为零多项式,则 $F(x_1,\cdots,x_n)$ 有一个因式 $x_n-G(x_1,\cdots,x_{n-1})$.

证明　将 F 表示为

$$F(x_1,\cdots,x_n)=\sum_{j=0}^{d}F_j(x_1,\cdots,x_{n-1})x_n^j,$$

其中 $d\geqslant 1$,而 $F_j\in D[x_1,\cdots,x_{n-1}]$. 由于

$$\sum_{j=0}^{d} F_j(x_1,\cdots,x_{n-1})G^j(x_1,\cdots,x_{n-1}) = 0,$$

因此

$$F(x_1,\cdots,x_n) = \sum_{j=0}^{d} F_j(x_1,\cdots,x_{n-1})(x_n^j - G^j(x_1,\cdots,x_{n-1})).$$

显然,对 $0 \leqslant j \leqslant d$,多项式 $x_n^j - G^j(x_1,\cdots,x_{n-1})$ 有因式

$$x_n - G(x_1,\cdots,x_{n-1}),$$

由此即知 $F(x_1,\cdots,x_n)$ 也如此.

设 $D^n = D \times \cdots \times D = \{(d_1,\cdots,d_n) \mid d_i \in D, 1 \leqslant i \leqslant n\}$. 正如一元多项式的情形,一个多项式 $F(x_1,\cdots,x_n) \in D[x_1,\cdots,x_n]$ 可以看作是 D^n 上的一个函数(其值在 D 中). 设

$$F(x_1,\cdots,x_n) = \sum_{i_1,\cdots,i_n} a_{i_1\cdots i_n} x_1^{i_1}\cdots x_n^{i_n},$$

对任意 $(d_1,\cdots,d_n) \in D^n$, 我们定义

$$F(d_1,\cdots,d_n) = \sum_{i_1,\cdots,i_n} a_{i_1\cdots i_n} d_1^{i_1}\cdots d_n^{i_n} \in D.$$

$F(d_1,\cdots,d_n)$ 称为 F 在 $(d_1,\cdots,d_n)$ 处的值.

定理 4　设 D 有无穷多个元素,$F \in D[x_1,\cdots,x_n]$ 是一个 n 元多项式. 如果对每个 $(d_1,\cdots,d_n) \in D^n$,F 在 $(d_1,\cdots,d_n)$ 处的值都是零,则 F 是零多项式.

证明　采用归纳法. 当 $n = 1$ 时,由 § 17,推论 3 知结论成立. 假设结论在 $n - 1$ 时成立,现在设 $F \in D[x_1,\cdots,x_n]$ 具有定理中说的性质. 记

$$F(x_1,\cdots,x_n) = \sum_{j=0}^{k} F_j(x_1,\cdots,x_{n-1})x_n^j.$$

并设 $(d_1,\cdots,d_{n-1})$ 是 D^{n-1} 中任一元. 考虑一元多项式

$$f(x) = F(d_1,\cdots,d_{n-1},x) = \sum_{j=0}^{k} F_j(d_1,\cdots,d_{n-1})x^j.$$

由假设，对任意 $d \in D$，$f(d)$ 均为零，从而 $f(x)$ 为零多项式. 因此

$$F_j(d_1,\cdots,d_{n-1}) = 0, \quad 0 \leqslant j \leqslant k,$$

对任意 $(d_1,\cdots,d_{n-1}) \in D^{n-1}$ 成立. 由归纳假设，对每一个 j，$F_j(x_1,\cdots,x_{n-1})$ 是零多项式，因此 $F = 0$.

推论　设 D 有无穷多个元素，$F,G \in D[x_1,\cdots,x_n]$，且对所有 $(d_1,\cdots,d_n) \in D^n$ 有 $F(d_1,\cdots,d_n) = G(d_1,\cdots,d_n)$. 则 $F = G$.

上面的推论，称为恒等定理，它表明当 D 有无穷多个元素时，$D[x_1,\cdots,x_n]$ 中的两个多项式作为 D^n 上的(多项式)函数恒等，与它们作为(形式)多项式相等是一致的(参考 §17，推论 3 下面的注记 2).

习　题　24

1. (i) 证明：多项式 $x_1^2 + x_2^2 + x_3^2$ 与 $x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_2x_3 + x_3x_1$ 均是 $\mathbf{R}[x_1,x_2,x_3]$ 中不可约多项式；

(ii) 研究(i) 中的多项式在 $\mathbf{F}_2[x_1,x_2,x_3]$ 中是否可约.

2. 设 n 为正奇数，且不是 3 的倍数. 证明：$\mathbf{R}[x_1,x_2]$ 中多项式 $(x_1 + x_2)^n - x_1^n - x_2^n$ 被 $x_1x_2(x_1^2 + x_1x_2 + x_2^2)$ 整除.

3. 设 D 有无穷多个元素，$F(x_1,\cdots,x_n)$，$G(x_1,\cdots,x_n)$ 是 $D[x_1,\cdots,x_n]$ 中两个多项式，且 G 不为零. 如果对于使 $G(d_1,\cdots,d_n) \neq 0$ 的任一组元素 $d_1,\cdots,d_n \in D$ 都有 $F(d_1,\cdots,d_n) = 0$. 证明 $F(x_1,\cdots,x_n)$ 是零多项式.

4*. 设 D 有无穷多个元素，E 是 D 的一个无限子集，$F(x_1,\cdots,x_n) \in D[x_1,\cdots,x_n]$. 如果对任意 $(d_1,\cdots,d_n) \in E^n$ 有 $F(d_1,\cdots,d_n) = 0$，则 F 是零多项式.

5*. 设 $F(x_1,\cdots,x_n)\in D[x_1,\cdots,x_n]$，并且 F 关于 x_i 的次数至多是 $a_i(1\leqslant i\leqslant k)$. 令 $A_i\subset D$，且 A_i 有 a_i+1 个元素$(1\leqslant i\leqslant n)$. 如果对任意$(d_1,\cdots,d_n)\in A_1\times\cdots\times A_n$，有 $F(d_1,\cdots,d_n)=0$，则 F 是零多项式.

§25. 齐次多项式与对称多项式

本节讲述 n 元齐次多项式与对称多项式的一些基本性质.

齐次多项式的下述性质往往用作其定义.

定理 1　设 $F(x_1,\cdots,x_n)\in D[x_1,\cdots,x_n]$，$F\neq 0$. 则 F 是 k 次的齐次多项式的充分必要条件为：在 $D[x_1,\cdots,x_n,t]$ 内，关系式

$$F(tx_1,\cdots,tx_n)=t^kF(x_1,\cdots,x_n)\tag{1}$$

成立.

证明　所说的条件显然是必要的. 为证其充分性，我们将 F 表示为齐次部分的和：

$$F=F_{k_1}+\cdots+F_{k_r},\quad 0\leqslant k_1<\cdots<k_r,$$

其中 F_{k_i} 是 k_i 次齐次式. 此时等式(1)成为

$$t^{k_1}F_{n_1}+\cdots+t^{k_r}F_{k_r}=t^kF_{k_1}+\cdots+t^kF_{k_r},$$

即

$$(t^k-t^{k_1})F_{n_1}+\cdots+(t^k-t^{k_r})F_{k_r}=0.$$

由于 $F_{k_i}\neq 0(1\leqslant i\leqslant r)$，故必须 $t^k=t^{k_i}$ 对 $i=1,\cdots,r$ 成立. 于是 $r=1$，而 $k_1=k$，即 F 是 k 次齐次式.

齐次多项式的积当然仍是齐次的. 反过来，我们有

定理2　设$F(x_1,\cdots,x_n)$是$D[x_1,\cdots,x_n]$中齐次多项式，则F的任一因式都是齐次的.

证明　设$F=GH$，而G不是齐次式，则G可表示为

$$G=G_i+G_{i+1}+\cdots+G_{i+j},$$

其中$G_l(i\leqslant l\leqslant i+j)$或者是零或者是$l$次齐次式，而$G_i\neq 0,G_{i+j}\neq 0$，且$j>0$；类似地，

$$H=H_k+H_{k+1}+\cdots+H_{k+l},$$

其中$H_k\neq 0,H_{k+l}\neq 0$，而$l\geqslant 0$. 于是

$$F=GH=G_iH_k+(G_{i+1}H_k+G_iH_{k+1})+\cdots+G_{i+j}H_{k+l}.$$

由于$G_iH_k\neq 0,G_{i+j}H_{k+l}\neq 0$（§24，定理1），并且

$$\deg G_iH_k=i+k<i+j+k+l=\deg G_{i+j}H_{k+l},$$

从而F不是齐次多项式，与假设矛盾.

非齐次多项式与齐次多项式有一种紧密地联系.

给定$D[x_1,\cdots,x_n]$中一个k次非齐次多项式$F(x_1,\cdots,x_n)$，我们引入一个新的不定元x_0，将F的各项乘以x_0的适当幂次，使每个单项式的次数为k. 这样产生的$D[x_0,x_1,\cdots,x_n]$中的$(n+1$元$)k$次齐次多项式记作$F^*(x_0,x_1,\cdots,x_n)$，称为(非齐次多项式)$F(x_1,\cdots,x_n)$的**对应多项式**，也称作$F(x_1,\cdots,x_n)$的**齐次化**. 我们称$F(x_1,\cdots,x_n)$与$F^*(x_0,x_1,\cdots,x_n)$相互对应. 不难看出

$$F^*(x_0,x_1,\cdots,x_n)=x_0^kF\left(\frac{x_1}{x_0},\cdots,\frac{x_n}{x_0}\right).\tag{2}$$

对每一个非齐次多项式，显然恰有一个对应的齐次多项式. 反过来，然而，对一个$n+1$元的齐次多项式，若将其一个不定元代之为1，一般对应$n+1$个不同的非齐次多项式. 我们注意，如果某个不定元在一个齐次多项式的每一项中都出现，将其代之为1，产生的多项式并非是一个对应的非齐次多项式，而是一个低次多项式. 考虑极端情形：如一个齐

次多项式的每一项包含所有不定元，则它没有对应的非齐次多项式. 四次齐次多项式

$$x_0^2x_1x_2 + x_0x_1^2x_2 - x_0x_1x_2^2$$

便是这样的例子.

定理 3　设 $F(x_1,\cdots,x_n)$ 与 $F^*(x_0,x_1,\cdots,x_n)$ 是两个(如上所说的) 相互对应的多项式. 如果其中一个是可约的，则另一个也可约.

证明　设齐次多项式 $F^*(x_0,x_1,\cdots,x_n)$ 的次数为 k，并且它可分解为两个次数分别为 r,s 的多项式的积($r,s\geqslant 1$)：

$$F^*(x_0,x_1,\cdots,x_n) = G^*(x_0,x_1,\cdots,x_n)H^*(x_0,x_1,\cdots,x_n).$$

取 $x_0 = 1$，得出

$$F^*(1,x_1,\cdots,x_n) = G^*(1,x_1,\cdots,x_n)H^*(1,x_1,\cdots,x_n). \tag{3}$$

由定理的假设，(3)式左边为 $F(x_1,\cdots,x_n)$，是 k 次多项式(参见(2))，从而(3) 式右边两个多项式的次数必须分别为 r 及 s，因此 $F(x_1,\cdots,x_n)$ 可约.

反过来，设非齐次多项式 $F(x_1,\cdots,x_n)$ 可分解为

$$F(x_1,\cdots,x_n) = G(x_1,\cdots,x_n)H(x_1,\cdots,x_n), \tag{4}$$

G,H 的次数分别是正整数 r,s. 设 F^*,G^*,H^* 分别是 F,G,H 的齐次化多项式(注意 G 和 H 之一可以是齐次的，因此可能出现 $G^* = G$ 或 $H^* = H$，但两者不能都成立.). 由(4)我们有

$$F\left(\frac{x_1}{x_0},\cdots,\frac{x_n}{x_0}\right) = G\left(\frac{x_1}{x_0},\cdots,\frac{x_n}{x_0}\right)H\left(\frac{x_1}{x_0},\cdots,\frac{x_n}{x_0}\right).$$

两边乘以 x_0^{r+s}，产生

$$F^*(x_0,x_1,\cdots,x_n) = G^*(x_0,x_1,\cdots,x_n)H^*(x_0,x_1,\cdots,x_n),$$

于是 $F^*(x_0,x_1,\cdots,x_n)$ 是可约的.

对称多项式是多元多项式中另一类重要的多项式.

设 $F(x_1,\cdots,x_n)\in D[x_1,\cdots,x_n]$，如果任意交换两个不定元均不改变 $F(x_1,\cdots,x_n)$，则称其为（n 元）**对称多项式**，或对称函数. 因此，对称多项式中不定元 $x_1,\cdots,x_n$ 的地位完全平等.

容易验证，两个 n 元对称多项式的和，差，积仍是对称多项式. 但对称多项式的因式不一定是对称的. $\mathbf{Z}[x_1,x_2]$ 中的对称多项式 $(x_1-x_2)^2$ 便是这样的例子. 然而，容易证明

定理 4　设 $F(x_1,\cdots,x_n)\in D[x_1,\cdots,x_n]$，$F\neq 0$，且 F（在 D 上）可分解为 $G\cdot H$. 如果 G 是对称多项式，则 H 也是对称多项式.

由 §24 中定理 1 的推论与定理 3，上面的定理 2 和定理 4，能够作出某些齐次的对称多项式的（标准）分解.

例 1　求 $\mathbf{R}[x_1,x_2,x_3]$ 中多项式

$$(x_1+x_2+x_3)^5-x_1^5-x_2^5-x_3^5$$

的标准分解.

解　将所说的多项式用 F 表示. 当 $x_3=-x_2$ 时，F 为零. 所以 x_2+x_3 是 F 的一个因式；同理，x_3+x_1 与 x_1+x_2 也是 F 的因式. 这三个因式显然两两互素，故 F 以 $G=(x_1+x_2)(x_2+x_3)(x_3+x_1)$ 为其因式.

由于 $\deg F=5$，而 G 是三次的齐次对称多项式，故 F 剩下的因式 H 是二次的齐次对称多项式，从而 H 必为

$$a(x_1^2+x_2^2+x_3^2)+b(x_1x_2+x_2x_3+x_3x_1)$$

的形式，其中 a,b 是不全为零的实数. 在 $F=GH$ 中取

$$x_1=x_2=x_3=1,$$

得出 $a+b=10$；取

$$x_1=2,\quad x_2=1,\quad x_3=0,$$

得 $5a + 2b = 35$. 故 $a = b = 5$. 于是

$$H = 5(x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_2x_3 + x_3x_1).$$

易知这是 **R** 上的不可约多项式(习题 24.1). 由此我们得出了 F 的标准分解为

$$5(x_1 + x_2)(x_2 + x_3)(x_3 + x_1)$$
$$\cdot (x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_2x_3 + x_3x_1).$$

习　题　25

1*. 设 $F(x_1, \cdots, x_n) \in D[x_1, \cdots, x_n]$, F 关于不定元 x_i 的(形式)**偏微商**定义为 F 关于 x_i 的微商,而其余不定元视为常数,记作 $\frac{\partial F}{\partial x_i}$. 证明:

如 $F, G \in D[x_1, \cdots, x_n]$, $a, b \in D$, 则(对 $1 \leqslant i \leqslant n$)

(i) $\frac{\partial(aF + bG)}{\partial x_i} = a\frac{\partial F}{\partial x_i} + b\frac{\partial G}{\partial x_i}$;

(ii) $\frac{\partial(FG)}{\partial x_i} = G\frac{\partial F}{\partial x_i} + F\frac{\partial G}{\partial x_i}$.

2*. (**欧拉定理**)　设 $D \subseteq \mathbf{C}$, $F(x_1, \cdots, x_n) \in D[x_1, \cdots, x_n]$, $F \neq 0$. 则 F 是 k 次齐次式的充分必要条件为

$$\sum_{i=1}^{n} x_i \frac{\partial F}{\partial x_i} = kF.$$

举例说明,上述结论在 $D = \mathbf{F}_p$ 时不成立.

3. 在 $\mathbf{R}[x_1, x_2]$ 中,求 $(x_1 + x_2)^7 - x_1^7 - x_2^7$ 的标准分解.

4. 在 $\mathbf{R}[x_1, x_2, x_3]$ 中,求下列多项式的标准分解:

(i) $x_1(x_2 - x_3)^2 + x_2(x_3 - x_1)^2 + x_3(x_1 - x_2)^2 + 8x_1x_2x_3$;

(ii) $(x_1x_2 + x_2x_3 + x_3x_1)^3 - x_1^3x_2^3 - x_2^3x_3^3 - x_3^3x_1^3$;

(iii) $x_1(x_2^4 - x_3^4) + x_2(x_3^4 - x_1^4) + x_3(x_1^4 - x_2^4)$.

5. 设 $F(x_1, x_2)$ 是 $D[x_1, x_2]$ 中的一个对称多项式,且有一个因式 $x_1 - x_2$. 证明: $(x_1 - x_2)^2$ 整除 $F(x_1, x_2)$.

6*. 设 $F(x_1,\cdots,x_n)\in D[x_1,\cdots,x_n]$ 是对称多项式，则 F 的每个齐次部分也是对称多项式.

§26. 对称多项式基本定理

设 $x_1,\cdots,x_n$ 为不定元. 引入一个新的不定元 x，记

$$\begin{aligned} f(x)&=(x-x_1)\cdots(x-x_n)\\ &=x^n-\sigma_1x^{n-1}+\sigma_2x^{n-2}-\cdots+(-1)^n\sigma_n. \end{aligned}\tag{1}$$

则 x 的幂的系数

$$\begin{cases} \sigma_1=x_1+x_2+\cdots+x_n,\\ \sigma_2=x_1x_2+x_1x_3+\cdots+x_2x_3+\cdots+x_{n-1}x_n,\\ \quad\vdots\\ \sigma_n=x_1x_2\cdots x_n \end{cases}\tag{2}$$

显然是（n 元）对称多项式（任意交换 x_i 与 x_j 不改变(1)式左边，从而也不改变其右端）. $\sigma_1,\sigma_2,\cdots,\sigma_n$ 称为（不定元）$x_1,\cdots,x_n$ 的**初等对称多项式**，或初等对称函数. 很明显，σ_i 是 i 次齐次多项式.

下面的结果，称为**对称多项式基本定理**，表明初等对称多项式在对称多项式中具有基本的重要性.

定理 1　$D[x_1,\cdots,x_n]$ 中任意对称多项式 $F(x_1,\cdots,x_n)$ 可写成初等对称多项式的一个多项式. 即存在 $D[y_1,\cdots,y_n]$ 中的一个多项式 $G(y_1,\cdots,y_n)$，使得

$$F(x_1,\cdots,x_n)=G(\sigma_1,\cdots,\sigma_n).\tag{3}$$

证明　对任意两个（不同类的）n 元单项式，可以**字典式地排列**（顺序）：一项 $x_1^{k_1}\cdots x_n^{k_n}$ 称为在另一项 $x_1^{l_1}\cdots x_n^{l_n}$ 之前，如果数

$$k_1-l_1,\cdots,k_n-l_n$$

中第一个不为零的数是正的.

我们将 $F(x_1,\cdots,x_n)$ (的项)按字典排列法排序,设其首项是

$$ax_1^{k_1}\cdots x_n^{k_n},\quad a\in D,a\neq 0 \tag{4}$$

(注意,它不一定具有最大的次数). 容易看出,(4)作为对称多项式的首项,必有 $k_1\geqslant k_2\geqslant\cdots\geqslant k_n\geqslant 0$. 因若有 i 使 $k_i<k_{i+1}$,则由于 F 是对称的,故 F 在包含(4)的同时必包含

$$ax_1^{k_1}\cdots x_i^{k_{i+1}}x_{i+1}^{k_i}\cdots x_n^{k_n}.$$

但这一项却在(4)中的项之前,从而(4)不是首项.

此外,由(2)可知,(齐次)对称多项式 $\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}$ 中的首项是

$$x^{l_1+\cdots+l_n}x_2^{l_2+\cdots+l_n}\cdots x_n^{l_n},$$

故 $a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\cdots\sigma_n^{k_n}$ 中的首项与 F 中的首项相同. 于是,对称多项式

$$F_1(x_1,\cdots,x_n)=F(x_1,\cdots,x_n)-a\sigma_1^{k_1-k_2}\sigma_2^{k_2-k_3}\cdots\sigma_n^{k_n}$$

(重作字典排列后的)首项在 F 的首项之后. 对 F_1 重复上面的手续,如此进行,便产生 $D[x_1,\cdots,x_n]$ 中一列对称的多项式

$$F_1,F_2,F_3,\cdots,F_l,\cdots,$$

使 F_{i+1} 等于 F_i 减去形如 $a_i\sigma_1^{i_1}\cdots\sigma_n^{i_n}$ 的多项式($a_i\in D$),并且 F_{i+1} 的首项在 F_i 的首项之后. 由于在项(4)之后的(不同类的)单项式只有有限多个,故上述过程有限步后必然停止,即存在 l 使 $F_l(x_1,\cdots,x_n)=0$. 由此即知,存在 D 上的多项式 $G(y_1,\cdots,y_n)$ 使等式(3)成立.

注记　1. 定理1的证明过程提供了一个将给定的对称多项式表示为 σ_i 的多项式的实际表示方法. 这一手法与(域上)一元多项式环的欧氏算法类似. (参考 §15 以及 §13,定理2的注记.)

2. 我们将 $i_1+2i_2+\cdots+ni_n$ 称为单项式 $a\sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$ 的**权**,而多项式 $G(\sigma_1,\cdots,\sigma_n)$ 的权指的是它的各项中所出现的最高权. 由上述证明不难看到,如果 $F(x_1,\cdots,x_n)$ 的次数是 k,则求得的表达式 $G(\sigma_1,\cdots,\sigma_n)$ 的权为 k. 此外,如果 F 是齐次的,则 G 中各项的权相等. 这些观察对实际地作出表示将有所帮助.

现在我们进一步证明，一个对称多项式表示为 σ_i 的多项式的方式是唯一的. 换句话说，表示的形式不依赖于作出表示的方法.

定理 2　设 $G_1(y_1,\cdots,y_n)$ 及 $G_2(y_1,\cdots,y_n)$ 是 $D[y_1,\cdots,y_n]$ 中两个多项式，如果在 $D[x_1,\cdots,x_n]$ 中有

$$G_1(\sigma_1,\cdots,\sigma_n)=G_2(\sigma_1,\cdots,\sigma_n),$$

则 $G_1(y_1,\cdots,y_n)=G_2(y_1,\cdots,y_n)$.

证明　我们只要证明：如果 $G(y_1,\cdots,y_n)$ 不是零多项式，则 $G(\sigma_1,\cdots,\sigma_n)$ 也不是($D[x_1,\cdots,x_n]$ 中的) 零多项式.

我们将 $G(y_1,\cdots,y_n)$ 中任一非零项

$$ay_1^{k_1},\cdots,y_n^{k_n}$$

与 $a\sigma_1^{k_1}\cdots\sigma_n^{k_n}$(作为 $D[x_1,\cdots,x_n]$ 中多项式)按字典排列的首项

$$ax_1^{k_1'}\cdots x_n^{k_n'}$$

对应，这里

$$\begin{aligned}
k_1' &= k_1+k_2+\cdots+k_n,\\
k_2' &= k_2+\cdots+k_n,\\
&\vdots\\
k_n' &= k_n.
\end{aligned}\tag{5}$$

由(5)可见，上述对应是一个单射. 特别地，如果 $ax_1^{k_1'}\cdots x_n^{k_n'}$ 是上述对应的诸首项中最前面的项，则它只出现一次. 所以，当 $\sigma_1,\cdots,\sigma_n$(分别) 代换 $y_1,\cdots,y_n$ 时，作为 $D[x_1,\cdots,x_n]$ 中多项式 $G(\sigma_1,\cdots,\sigma_n)$(字典排列) 的首项，$ax^{k_1'}\cdots x_n^{k_n'}$ 不会被消去. 因此 $G(\sigma_1,\cdots,\sigma_n)$ 不是零多项式. 证毕.

若 x_i 不是不定元，而是 D 中的元素，例如，是 $\mathbf{C}[x]$ 中多项式 $f(x)$ 的根时，对称多项式间的关系仍然保持成立. 因此，由前面的结果知，$f(x)$ 的根的任一对称(多项式) 函数可以用 $f(x)$ 的系数表示，而不必

求出根.

作为一个例子,我们考虑 $\mathbf{Z}[x_1,\cdots,x_n]$ 中多项式

$$\Delta(x_1,\cdots,x_n)=\prod_{1\leqslant i<j\leqslant n}(x_i-x_j)^2.$$

显然,这是一个对称多项式.由定理 1 和定理 2,有唯一的整系数多项式 $D(y_1,\cdots,y_n)$,使得

$$\Delta(x_1,\cdots,x_n)=D(\sigma_1,\cdots,\sigma_n).$$

给定 $\mathbf{C}[x]$ 内一个 n 次多项式

$$f(x)=x^n-a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+(-1)^n a_0,$$

设其 n 个复根为 $\alpha_1,\cdots,\alpha_n$.我们定义 $D(f)=\Delta(\alpha_1,\cdots,\alpha_n)$ 为 $f(x)$ 的**判别式**,显然,$f(x)$ 有重根的充分必要条件是 $D(f)=0$. 由韦达定理知

$$D(f)=D(a_{n-1},a_{n-2},\cdots,a_0).$$

因此,我们实际上不必求出 $f(x)$ 的根,即可由 $f(x)$ 的系数判断 $f(x)$ 是否有重根.

例 1　(i) 二次多项式 $x^2-a_1x+a_0$ 的判别式是

$$a_1^2-4a_0;$$

(ii) 三次多项式 $x^3-a_2x^2+a_1x-a_0$ 的判别式是

$$a_2^2a_1^2-4a_2^3a_0-4a_1^3-27a_0^2+18a_2a_1a_0.$$

解　(i) 因为

$$\begin{aligned}\Delta(x_1,x_2)&=(x_1-x_2)^2=(x_1+x_2)^2-4x_1x_2\\&=\sigma_1^2-4\sigma_2,\end{aligned}$$

由此即得结果.

(ii) 我们注意

$$\Delta(x_1,x_2,x_3)=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$$

是 6 次的齐次式,所以它可(唯一地)表示为 $\sigma_1,\sigma_2,\sigma_3$ 的各项的权均为 6

的多项式(参考定理1及其注记2).易求出方程$i_1+2i_2+3i_3=6$共有7组非负整数解:

$$(i_1,i_2,i_3)=(6,0,0),(4,1,0),(3,0,1),$$
$$(2,2,0),(1,1,1),(0,3,0),(0,0,2);$$

相应地,我们有表示

$$\Delta(x_1,x_2,x_3)=c_1\sigma_1^6+c_2\sigma_1^4\sigma_2+c_3\sigma_1^3\sigma_3$$
$$+c_4\sigma_1^2\sigma_2^2+c_5\sigma_1\sigma_2\sigma_3+c_6\sigma_2^3+c_7\sigma_3^2,\qquad(6)$$

其中$c_i(1\leqslant i\leqslant 7)$是待定的常数.

在恒等式(6)中逐次取x_1,x_2,x_3的特殊值,可以确定这些常数.例如,取$x_1=x_2=0$,得

$$c_1=0;$$

取$x_1=1,x_2=-1,x_3=0$,得

$$c_6=-4.$$

取$x_1=2,x_2=1,x_3=0$,得

$$81c_2+18c_4=18,$$

取$x_1=2,x_2=-1,x_3=0$,得

$$-c_2+4c_4=4.$$

所以$c_2=0,c_4=1$.同样地,我们可求出

$$c_3=-4,\quad c_5=18,\quad c_7=-27.$$

由此即得出所说的结果.

注记　如果$f(x)$是(首项系数为1的)实系数多项式,则$f(x)$的判别式能给出其实根的某些信息.

在$f(x)$为二次及三次的情形,容易证明,$f(x)$的根均为实数的充分必要条件是$D(f)\geqslant 0$.

$f(x)$为二次时,所说的结论是熟知的.

当$f(x)$为三次时,如其三个根均为实数,则显然$D(f)\geqslant 0$.反过

来，设

$$f(x) = (x - x_1)(x - x_2)(x - x_3)$$

的三个根 x_1, x_2, x_3 中有一个非实数，设为 x_1. 则 x_2, x_3 之一为 x_1 的共轭（参考习题 19.1），无妨设 $x_2 = \overline{x_1}$. 那么 $(x - x_1)(x - x_2)$ 为实系数，从而 x_3 是实数. 现在

$$\overline{x_1 - x_2} = -(x_1 - x_2),$$
$$\overline{x_1 - x_3} = x_2 - x_3,$$
$$\overline{x_2 - x_3} = x_1 - x_3.$$

故

$$D(f) = -|(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)|^2 < 0.$$

在 $f(x)$ 的次数大于 3 时，记 r 为其实根的个数，则

$$\deg f \equiv r \pmod 2 \quad (\S 19, \text{定理 3 的推论}).$$

进一步，能够证明，$D(f) \geqslant 0$ 的充分必要条件是

$$\deg f \equiv r \pmod 4.$$

习　题　26

1. 将下面的对称多项式表示为初等对称多项式的多项式：

(i) $x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2$；

(ii) $x_1(x_2^3 + x_3^3) + x_2(x_3^3 + x_1^3) + x_3(x_1^3 + x_2^3)$.

(iii) $(x_1x_2 + x_3)(x_2x_3 + x_1)(x_3x_1 + x_2)$.

2. 设 $F(x_1, \cdots, x_n) \in D[x_1, \cdots, x_n]$ 是对称多项式，满足

$$F(x_1 + a, \cdots, x_n + a) = F(x_1, \cdots, x_n),$$

其中 a 是任意常数. 设 $F(x_1, \cdots, x_n) = G(\sigma_1, \cdots, \sigma_n)$. 证明

$$n\frac{\partial G}{\partial \sigma_1} + (n-1)\sigma_1\frac{\partial G}{\partial \sigma_2} + \cdots + \sigma_{n-1}\frac{\partial G}{\partial \sigma_n} = 0.$$

3. 确定并证明，$\sigma_1,\sigma_2,\cdots,\sigma_n$ 中哪些是不可约多项式.

4*. 设 $f(x)\in\mathbf{C}[x]$，$D(f)$ 是 $f(x)$ 的判别式. 证明：$D(f)=0$ 的充分必要条件是 $f(x)$ 与 $f'(x)$ 不互素.

5*. 记 $s_k=x_1^k+\cdots+x_n^k$，　$k=1,2,\cdots$，这称为 $x_1,\cdots,x_n$ 的方幂和. 下面的结果，称为**牛顿**(Newton)**恒等式**，给出了 s_k 与 σ_i 之间的递推关系：

$$s_k-\sigma_1 s_{k-1}+\sigma_2 s_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}s_1+(-1)^k k\sigma_k=0,$$

如 $k\leqslant n$；

$$s_k-\sigma_1 s_{k-1}+\cdots+(-1)^n\sigma_n s_{k-n}=0,$$

如 $k>n$.

6. 设 $x_1,\cdots,x_n$ 为复系数多项式 $x^n+a_1x^{n-1}+\cdots+a_n$ 的根，定义

$$s_k=x_1^k+\cdots+x_n^k,\quad k=1,2,\cdots.$$

又设 $|s_k|\leqslant 1$ $(k=1,2,\cdots,n)$. 证明：$|a_k|\leqslant 1$ $(k=1,2,\cdots,n)$.

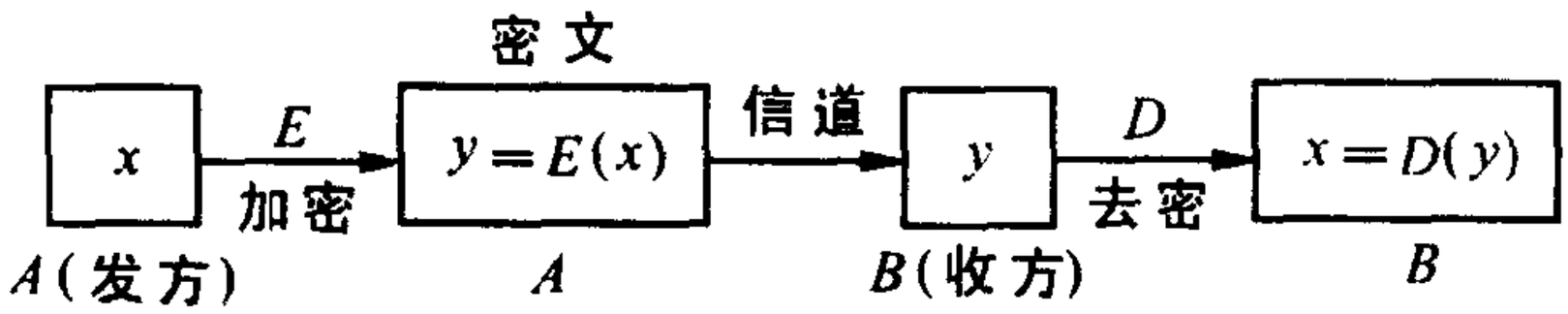
7. 设 x_1,x_2,x_3 是整系数三次方程 $x^3+ax^2+bx+c=0$ 的根，记 $s_n=x_1^n+x_2^n+x_3^n$. 证明：s_n 是整数$(n=1,2,\cdots)$.

附录　应用举例

1. 公开密钥体制

20 世纪 60 年代以来，电子计算机和数字通信技术得到飞速进步，计算机科学和信息科学提出了具有实际应用背景的许多数学问题，数论、代数和组合数学等离散性数学成为解决这些新问题的重要工具. 这里我们以三个具体实例，表现本书中讲述的知识在数字通信和信息安全方面的某些重要应用. 首先，本节中介绍 1976 年出现并已得到广泛应用的新型机密体制：公开密钥体制.

现代无线数字通信系统在运行中，信息很容易被第三者窃取和篡改，所以信息加密和保护非常重要. 保密通信的最简单的模型如附图 1 所示.

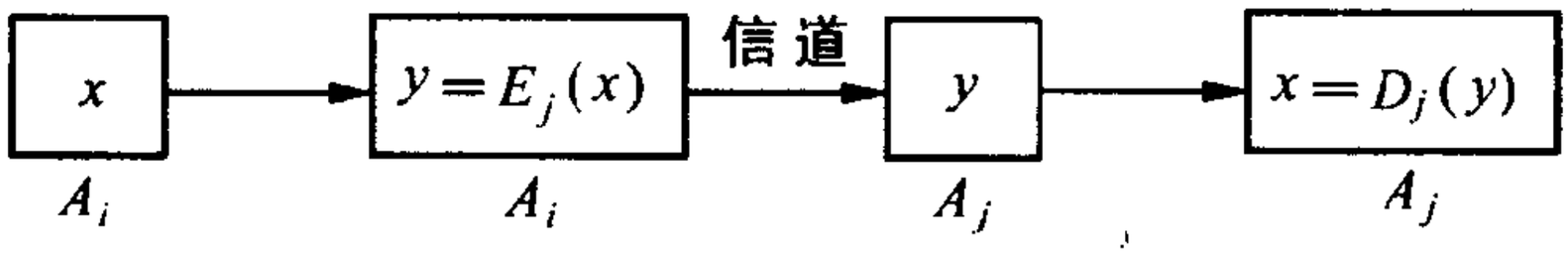


附图 1

发信人 A 把信息(明文)x 通过信道传给收信人 B. A 在传输之前把**明文** x 加密成**密文** $y=E(x)$，然后传给 B. B 在收到密文 y 之后要用 E 的逆运算 D 去密，恢复出明文 $x=D(y)$. 其中 D 和 E 这两个互逆运算只有 A 和 B 知道而对外人保密，分别叫作**加密密钥**和**去密密钥**.

现代网络通信中，每个人都要和许多人通信. 比如某公司有 2000

人，相互通信都需加密，整个公司需要$\binom{2000}{2}=1999000$对密钥，每人都需保存1999对密钥. 大量密钥保存起来很困难，而密钥丢失是非常严重的问题. 1976年，美国年青数学家和计算机专家Diffie和Hellman提出一种新的保密体制，叫作**公开密钥**(public key)体制. 这种系统的关键是使用“**单向**”(one — way)函数E作为加密密钥. 所谓“单向”即指E是可逆函数，但是由E求它的逆函数是非常困难的. 公司每个人A_i都取一个单向函数E_i作为自己的加密密钥并把它公开于众，但是把E_i的逆函数D_i作为A_i自己的去密密钥保存起来，不让别人知道. 公司把2000人的加密密钥$E_i(1\leqslant i\leqslant 2000)$装订成册，就象电话本一样可供大家查找和使用，所以每个人A_i只需保存一个自己的去密密钥D_i即可. 当A_i把信息x传给A_j时，A_i在公司密钥本上查到A_j的加密密钥E_j，A_i把$y=E_j(x)$传给A_j. A_j收到密文y之后，用只有自己知道的去密密钥D_j作用y，就得到明文$x=D_j(y)$(见附图2). 任何外人截获到密文y，即使知道是由A_i传给A_j的，也能查到E_j，但很难求出$D_j=E_j^{-1}$，所以很难恢复明文x.



附图2

公钥体制提出之后，由于解决了保存密钥造成的困难，同时也解决了下节讲述的身份认证问题，引起通信界和数学界很大反响. 一时间人们设计出五花八门的公钥具体方案，随后这些方案又不断被别人攻击和破掉. 所谓具体方案，其核心是设计一批单向函数E. 所谓被破掉，即指寻找出求E^{-1}的好的实用算法，以表示用E作为加密密钥是不可靠的. 迄今为止，基本上只有两个公钥方案被认为是可靠的，并且已普遍

用在电子商务等方面.第一种方案与整数的因子分解有直接关系,它建立在这样一种信念上:大整数的因子分解是件十分困难的事.

纯粹数学家和应用数学家看待数学,往往有不同的美学标准.本书§3 中讲的算术基本定理,在理论上被认为是非常漂亮的.可是注重实际的人会问:给定一个很大的整数 N,是否有实际办法在较短时间内把 N 分解成素数的乘积?事实上,用目前最快的计算机(硬件)和已经发明的大数分解最好算法(软件),要分解100位(十进制)的数 N 需要几分钟,而分解200位的数 N(特别当 N 是两个大约100位的不同素数乘积时)则需要几万年!基于这个事实,就在公钥体制被提出的一年之后,1977年美国麻省理工学院的三位年轻数学家和计算机专家Rivest, Shamir 和 Adleman 提出下面的公钥方案,后人称为 RSA 方案.

取定两个大约 100 位的不同素数 p,q,令 $N = pq$. 则欧拉函数 $\varphi(N) = (p-1)(q-1)$. 再取两个正整数 e 和 d,使得

$$ed \equiv 1 \pmod{\varphi(N)}$$

(当 N 很大时,这样的 (e,d) 有很多,可供不同人使用). 则有如下的简单结果(用本书的知识易于证明).

引理　设 $N = pq$,其中 p 和 q 是不同的素数. 正整数 e 和 d 满足 $ed \equiv 1 \pmod{\varphi(N)}$,则对每个整数 x,均有 $x^{ed} \equiv x \pmod{N}$.

现在我们把信息 x 用 $0,1,2,\cdots,N-1$ 来表示. 加密密钥 E 的作用为 $y = E(x) \equiv x^e \pmod{N}$,$y$ 是 x^e 模 N 的最小非负剩余(目前这种运算已有很快的实用算法). 而去密密钥 D 取为 $D(y) \equiv y^d \pmod{N}$. 由上述引理可知 $D(y) = x$,即 E 和 D 是互逆运算.

在这种方案中 N 和 e 是公开的. 由 e 求 d 需要满足

$$ed \equiv 1 \pmod{\varphi(N)}.$$

但是这必需知道 $\varphi(N) = (p-1)(q-1)$ 的值. 由于分解 $N = pq$ 非常困难,外人无法知道 $\varphi(N)$,所以由 e 不能求出 d 值.

例 1　用户 B 选择两个素数 $p = 11$ 和 $q = 7$，则 $N = pq = 77$，$\varphi(N) = 60$. 用户 B 取加密密钥为与 $\varphi(N)$ 互素的 $e = 7$，则 B 的去密密钥为 $d \equiv e^{-1} \equiv \frac{1}{7} \equiv 43 \pmod{60}$，即 $d = 43$. 用户 B 把 $N = 77, e = 7$ 公开，而对 $d = 43$ 保密. 现在用户 A 想把明文 $x \equiv 2 \pmod{77}$ 发送给用户 B，用户 A 先加密成

$$y = x^e = 2^7 \equiv 51 \pmod{77},$$

把密文 $y = 51$ 传给用户 B. 用户 B 用自己的去密密钥 $d = 43$ 将 y 恢复成明文 x：

$$\begin{aligned} x &= y^d = 51^{43} \\ &\equiv 2 \pmod{77}. \end{aligned}$$

第二个方案是 1985 年提出的 ElGamal 算法，目前也得到广泛应用. 它所采用的工具是 §9 中所述的离散对数. 设 p 为素数，α 是模 p 的一个原根，则对每个不被 p 除尽的整数 β，均存在唯一的整数 a，$0 \leqslant a \leqslant p-2$，使得 $\alpha^a \equiv \beta \pmod{p}$. 对于给定的原根 α，由 a 计算 $\beta \equiv \alpha^a \pmod{p}$ 的指数运算有好的算法，但是当 p 很大(比如大于 130 位)时，由 β 求 a (离散对数)是很困难的. 基于这个想法，ElGamal 给出如下的公开密钥方案.

取定一个大素数 p，模 p 的一个原根 α. 由 B 取一个整数 $a(0 \leqslant a \leqslant p-2)$. 令 $\beta \equiv \alpha^a \pmod{p}$. 将 p, α, β 公开，但是 a 由 B 保密. 设发方 A 将信息传给收方 B，发方 A 秘密地选择一个整数 $k(0 \leqslant k \leqslant p-2)$，计算

$$y_1 \equiv \alpha^k \pmod{p}, \quad y_2 \equiv x\beta^k \pmod{p},$$

然后将 (y_1, y_2) 传给 B. 换句话说，收方 B 的加密密钥 E 是 $E(x, k) = (y_1, y_2)$. 而收方 B 得到此密文 (y_1, y_2) 之后作运算

$$D(y_1, y_2) \equiv y_2 (y_1^a)^{-1} \pmod{p}$$

(只有收方 B 知道 a). 由于

$$y_2 (y_1^a)^{-1} \equiv (x\beta^k)(\alpha^k)^{-a} = x(\beta\alpha^{-a})^k \equiv x \pmod{p},$$

即 $D(y_1,y_2)\equiv x\pmod p$，可知 D 为 B 的去密密钥，将密文恢复出明文 x. 发方 A 每次可秘密地选择不同 k 值，而收方 B 去密时不需知道 k 值，这就使外人在不知道 a(和 k) 时，破译密文 (y_1,y_2) 变得更为困难.

例 2　取素数 $p=2579$ 的一个原根 $\alpha=2$. 取 $a=765$，则

$$\beta\equiv 2^{765}\equiv 949\pmod{2579}.$$

将 p,α,β 公开，而 a 只有收方 B 知道. 现在发方 A 想把信息 $x=1299$ 发给 B. 发方 A 随意取一个整数 $k=853$，计算

$$y_1\equiv 2^{853}\equiv 435\pmod{2579},$$

$$y_2\equiv 1299\cdot 949^{853}\equiv 2396\pmod{2579},$$

然后 A 将密文(435,2396) 发给 B. 而 B 收到密文后计算出明文

$$x\equiv 2396\cdot(435^{765})^{-1}\equiv 1299\pmod{2579}.$$

2. 数字签名

公钥体制所以受到广泛注意，除了大大减少了密钥保存量之外，还解决了另一个重大难题，即数字通信中的签名和身份认证问题.

在外交活动中签署文件，商业上签定合同，日常书信或银行取款的签字，传统方式是用手写签名或印鉴，起到认证或核准的作用. 当人们采用数字通信网络进行电子购物和交换文件时，如何进行签名和身份认证?比如说，A 向 B 发一个电子邮件向 B 借钱，B 如何能判定这个邮件是 A 发来的而不是别人冒名顶替?这是一个长期未能很好解决的问题. 公钥体制解决了这个问题.

先以 RSA 公钥方案为例. 设 $N=pq$，e_A 和 d_A 分别为 A 的加密密钥和去密密钥，$e_Ad_A\equiv 1\pmod{\varphi(N)}$. 其中 N 和 e_A 公开，d_A 由 A 自己保存. 设想 A 向 B 发一个信息 x. 为了向 B 表明 A 的身份，A 将明文 x 用自己的去密密钥作用：$y\equiv x^{d_A}\pmod N$，这就是 A 的签字，A 把 y 发给 B. B 收到 y 后利用公开的 e_A 作用，得到明文 $x\equiv y^{e_A}\pmod N$. 这就

验证了 A 的身份. 由于除 A 之外别人都不知道 d_A，所以外人很难伪造 A 的签名.

RSA 方案还可同时进行签名和加密功能. 设 e_B 和 d_B 分别是 B 的加密密钥和去密密钥($e_Bd_B \equiv 1 \pmod{\varphi(N)}$). A 向 B 发信息 x，则可以按下方式进行.

(1) A 把明文 x 先签名：$y = x^{d_A} \pmod N$，再加密：

$$z \equiv y^{e_B} \pmod N,$$

然后将 z 发给 B；

(2) B 收到 z 之后，先去密：$z^{d_B} \equiv y \pmod N$，再进行

$$y^{e_A} \equiv x \pmod N.$$

B 看到明文 x，从而认证了 A 的身份.

接下来再介绍采用离散对数的 ELGamal 数字签名方案(1985 年). 取大素数 p 和模 p 的一个原根 α. 再取整数 a ($0 \leqslant a \leqslant p-2$)，计算 $\beta \equiv \alpha^a \pmod p$. 把 p，α 和 β 公开，而 a 由 A 自己保守秘密，A 在信息 x 上签名时，先随意取一个与 $p-1$ 互素的整数 k，计算

$$\gamma \equiv \alpha^k \pmod p, \quad \delta \equiv (x - a\gamma)k^{-1} \pmod{p-1}$$

则 (γ, δ) 就是 A 在信息 x 上的签名. 由信息 x 和签名 (γ, δ)，再利用公开的 p、α 和 β，任何人都可验证 A 的签名的正确性，这只需验证同余式 $\beta^\gamma\gamma^\delta \equiv \alpha^x \pmod p$ 成立. 这是因为

$$\beta^\gamma\gamma^\delta \equiv \alpha^{a\gamma+k\delta} \equiv \alpha^x \pmod p,$$

现在考查一下这种签名方案的安全性，即外人不知道 a，对于给定的信息 x 是否能伪造 A 的签名?即外人能否找出一对整数 (γ, δ)，使得 $\beta^\gamma\gamma^\delta \equiv \alpha^x \pmod p$ 成立?如果选了 γ 来求 δ 满足此同余式，这是一个困难的离散对数问题. 如果选了 δ 而求 γ 满足此同余式，目前也没有好的方法. 但是要注意：A 不能用同一个 k 值对两个不同的信息 x_1 和 x_2 ($x_1 \neq x_2$) 进行签名. 因为若 A 对 x_1 和 x_2 的签名为 (γ_1, δ_1) 和 (γ_2, δ_2). 则

$$\gamma_1 \equiv \alpha^k \equiv \gamma_2 (\mathrm{mod}\ p),$$

从而 $\gamma_1 = \gamma_2$，记这个公共值为 γ，则

$$k\delta_1 + a\gamma \equiv x_1, \quad k\delta_2 + a\gamma \equiv x_2 (\mathrm{mod}\ p-1).$$

从而可把方程中外人不知道的 a 消掉而得到

$$k(\delta_1 - \delta_2) \equiv x_1 - x_2 (\mathrm{mod}\ p-1).$$

令 d 是 $\delta_1 - \delta_2$ 和 $p-1$ 的最大公约数，上述方程给出模 $p-1$ 的 d 个解 k. 我们可以用 $\gamma \equiv \alpha^k (\mathrm{mod}\ p)$ 来决定 $k(\mathrm{mod}\ p-1)$ 的正确值，然后可算出

$$a \equiv (x_1 - \delta_1 k)^{\gamma-1} (\mathrm{mod}\ p).$$

一旦 a 被外人知道，外人就可对任意信息 x 仿造 A 的签名，从而破译了 A 的上述签名方案.

注意 A 的签名 (γ, δ) 没有把 a 泄漏出去. 因为在

$$\delta \equiv (x - a\gamma)k^{-1} (\mathrm{mod}\ p-1)$$

中只有 δ, x, γ 公开. 为求 a 需要知道 k. 而从 $\gamma \equiv \alpha^k (\mathrm{mod}\ p)$ 求 k，是一个困难的离散对数问题.

以上我们只举了签名和身份认证的最简单情形. 实际领域还需要解决更复杂的情形. 比如说，如何防止 A 否认自己的签名？当通信双方就签名和身份等问题发生争执时，如何安排仲裁机构，这种仲裁不仅要保障解决争执，而且在仲裁过程中不能泄漏双方任何不应泄漏的信息. 这就需要设计功能更齐全的协议和方案. 此外，我们需要对各种方案的安全性进行更严密的分析. 这些问题的深入研究不仅需要更深刻的数论和代数知识，也需要信息论、计算复杂性理论、概率统计和算法逻辑等方面知识，这些实际问题是对数学家和计算机通信学家的巨大挑战.

3. 密钥分配与共享

保密通信的核心是密钥的设计，此外还有密钥的传输和管理问题. 即使通信双方事先约定的密钥，但使用一段时间之后需要更换. 如果某公司有 n 个用户，彼此使用 $\binom{n}{2}$ 密钥，需要 $\binom{n}{2}$ 个安全的通道传送密钥. 这些密钥的安全性和管理常常是一个严重的问题. 目前常采用由公司设立密钥管理中心的办法，由管理中心设计和更换密钥，只需 n 个安全通道传送(分配) 给 n 个用户. 现在介绍 Blom 于 1985 年提出的一个分配方案.

设某公司有 n 个用户 $A_1,\cdots,A_n$. 取定一个大于 n 的素数 p，再取有限域 $\mathbf{F}_p$ 中 n 个不同的元素 $r_1,r_2,\cdots,r_n$(改变 r_i 的值相当于管理中心更换密钥). p 和 $r_1,r_2,\cdots,r_n$ 均公开.

(1) 管理中心随机地选取 $\mathbf{F}_p$ 中三个元素 a,b,c(它们可以相同). 由此形成一个关于 x,y 的对称多项式

$$f(x,y)=a+b(x+y)+cxy\in\mathbf{F}_p[x,y],$$

系数 a,b,c 只有管理中心知道；

(2) 对每个 $i(1\leqslant i\leqslant n)$，管理中心计算

$$\begin{aligned}g_i(x)&=f(x,r_i)=a+b(x+r_i)+c(xr_i)\\&=\alpha_i+\beta_i x\in\mathbf{F}_p[x],\end{aligned}$$

并把 $g_i(x)=\alpha_i+\beta x_i$ 分配给用户 A_i. 也就是说，用户中只有 A_i 知道 $g_i(x)$ 的系数 α_i 和 β_i，其中 $\alpha_i=a+br_i$，$\beta_i=b+cr_i$；

(3) 如果用户 A_i 和 A_j 通信，则用户 A_i 计算 $g_i(r_j)\in\mathbf{F}_p$(用户 A_i 知道多项式 $g_i(x)$，而 r_j 是公开的)，用户 A_j 计算 $g_j(r_i)$. 由于

$$g_i(r_j)=f(r_j,r_i)=f(r_i,r_j)=g_j(r_i),$$

所以两个用户计算出来同一个值 $k_{ij}=g_i(r_j)=g_j(r_i)$. A_i 和 A_j 就用 k_{ij} 作为通信的密钥. 所以 A_i 和 A_j 之间不再需要传送密钥.

让我们分析一下这种密钥分配方案的安全性.

(1) 对于 A_i 和 A_j 之外的第三个用户 A_k，A_k 得不到 A_i 和 A_j 之间密钥 k_{ij} 的任何信息.

这是因为：A_k 知道管理中心发给自己的

$$g_k(x) = \alpha_k + \beta_k x \in \mathbf{F}_p[x].$$

对于 A_i 和 A_j 的信息，A_k 只知道公开值 r_i 和 r_j，但是不知道

$$g_i(x) = \alpha_i + \beta_i x \quad 和 \quad g_j(x) = \alpha_j + \beta_j x,$$

即不知道 $\alpha_i, \beta_i, \alpha_j, \beta_j$ 的值. 在这种情形下，由一个关系

$$g_i(r_j) = \alpha_i + \beta_i r_j = \alpha_j + \beta_j r_i = g_j(r_i)$$

来决定 k_{ij} 是不可能的. 如果 A_k 试图破译管理中心设计的多项式 $f(x,y) = a + b(x + y) + cxy$，即需要决定三个系数 a,b,c. 但是 A_k 只知道 α_k, β_k 和公开的 r_k，从而只知道 a,b,c 之间的两个关系：$\alpha_k = a + br_k, \beta_k = b + cr_k$，由此也不能决定出 a,b,c 的值. 再进一步，对每个元素 $l \in \mathbf{F}_p$，我们分析一下是否有 a,b,c 使得在上述两个关系之下，l 成为 A_i 和 A_j 之间的密钥. 也就是是问：是否有 $a,b,c \in \mathbf{F}_p$，使得满足如下的三元(a,b,c 为不定元)一次联立方程组

$$\begin{cases} a + b(r_i + r_j) + c(r_i r_j) = l, \\ a + br_k = \alpha_k, \\ b + cr_k = \beta_k. \end{cases}$$

由于这个方程组系数行列式为

$$\begin{vmatrix} 1 & r_i + r_j & r_i r_j \\ 1 & r_k & 0 \\ 0 & 1 & r_k \end{vmatrix} = (r_k - r_i)(r_k - r_j) \neq 0$$

(注意 $r_1, \cdots, r_n$ 是 $\mathbf{F}_p$ 中不同元素)，所以方程组在 $\mathbf{F}_p$ 中有唯一的一组解 a,b,c. 这就表明：根据 A_k 所得信息 $(\alpha_k, \beta_k, r_i, r_j, r_k)$，$A_i$ 和 A_j 之间以 $\mathbf{F}_p$ 中任何元素 l 为密钥的可能性均存在，所以 A_k 得不到 A_i 和 A_j 之间密钥 k_{ij} 的任何信息.

(2) 两个用户 A_k 和 A_t 联系，可以破译管理中心设计的多项式

$f(x,y)$，从而可以破译任意两个用户 A_i 和 A_j 之间的密钥.

这是因为：A_k 和 A_t 可以把管理中心分配给他们的 α_k,β_k 和 α_t,β_t 合在一起. 再加上公开值 r_k 和 r_t，给出关于 a,b,c 的四个关系式

$$\alpha_k = a + br_k, \quad \alpha_t = a + br_t,$$

$$\beta_k = b + cr_k, \quad \beta_t = b + cr_t.$$

由前两个关系给出

$$b = (\alpha_k - \alpha_t)/(r_k - r_t),$$

由后两个等式给出

$$c = (\beta_k - \beta_t)/(r_k - r_t).$$

最后有

$$a = \alpha_k - br_k.$$

所以 A_k 与 A_t 联手可以破译 $f(x,y)$.

现在介绍密钥分配的另一个方案：Diffie-Hellman 方案. 仍设有 n 个用户 $A_1,\cdots,A_n$. 管理中心选取一个大于 n 的素数 p 和模 p 的一个原根 α，再选定 n 个整数 $a_1,\cdots,a_n(0\leqslant a_i\leqslant p-2)$. 然后把 a_i 由安全通道秘密地分配给用户 $A_i(1\leqslant i\leqslant n)$，同时计算 $b_i\equiv\alpha^{a_i}(\mathrm{mod}\ p)$. 把 p,α 和 $b_i(1\leqslant i\leqslant n)$ 均公开. 用户中只有 A_i 知道数 a_i，其他用户只知道 b_i. 要想由 b_i 计算 $a_i(b_i\equiv\alpha^{a_i}(\mathrm{mod}\ p))$，当 p 很大时，这是困难的离散对数问题.

用户 A_i 和 A_j 通信时，A_i 计算 $\mathbf{F}_p$ 中元素 $b_j^{a_i}$（A_i 知道 a_i，而 b_j 是公开的），A_j 计算 $\mathbf{F}_p$ 中元素 $b_i^{a_j}$. 由于 $b_j^{a_i}=\alpha^{a_ja_i}=b_i^{a_j}$，所以 A_i 和 A_j 算出 $\mathbf{F}_p$ 中同一个元素（记为 k_{ij}），它就用作 A_i 和 A_j 通信的密钥.

用户 A_i 和 A_j 之外的第三用户 A_k 能否算出 A_i 和 A_j 之间的密钥 k_{ij}？即给定 $\mathbf{F}_p$ 中元素 $b_i=\alpha^{a_i}$ 和 $b_j=\alpha^{a_j}$，是否可算出 $k_{ij}=\alpha^{a_ia_j}$？这个问题比离散对数问题要弱，但是可以证明这个问题的破译和前节 ElGamal 数字签名方案的破译是等价的.

任意两个用户 A_i 和 A_j 可以更换密钥，方法是：A_i 和 A_j 分别选

取 a_i' 和 $a_j'(0 \leqslant a_i', a_j' \leqslant p-2)$，然后公开 $b_i' = \alpha^{a_i'}$ 和 $b_j' = \alpha^{a_j'}$. 它们可采用新的密钥 $k_{ij}' = \alpha^{a_i' a_j'}$.

我们都知道，发射核武器的控制按钮只由一个人掌握是很危险的. 重要机密常常需要足够多的人意见一致才能开启. 在很多情形下，一个主密钥 k 要分解成一些子密钥 $k_1, \cdots, k_n$，分别由 n 个人 $A_1, \cdots, A_n$ 控制. 只有足够多的人把子密钥放在一起，才能揭示出主密钥. 这叫作**密钥共享问题**. 我们只考虑比较简单的问题：取定一个整数 $t \geqslant 2$. 我们要求：

(1) 任意 t 个子密钥放在一起均可算出主密钥 k，

(2) 任意 $t-1$ 个子密钥放在一起得不到主密钥 k 的任何信息.

这叫门限为 t 的密钥共享问题.

事实上，前节所述的 Blom 密钥分配方案也可看成是 $t=2$ 的密钥共享方案，因为可把 $f(x,y)$ 看成是主密钥，而 $a_1, \cdots, a_n$ 看成是分别发给 $A_1, \cdots, A_n$ 的子密钥. 我们在上节分析 Blom 方案安全性时指出，任意两个人 A_k 和 A_t 在一起可算出主密钥 $f(x,y)$，而每个人则不能得到 $f(x,y)$ 的任何信息. 所以这是门限为 2 的密钥共享方案. 下面，我们介绍 1979 年 Shamir 给出的门限为 t 的密钥共享方案($t \geqslant 2$).

设想把主密钥由 n 个人 $A_1, \cdots, A_n$ 共享. 选定一个大于 n 的素数 p. 由控制中心随机选取 $\mathbf{F}_p$ 中一个元素 k 作为主密钥，并随机地选取 $\mathbf{F}_p[x]$ 中一个 $t-1$ 次的多项式

$$h(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1 x + a_0$$

$$(a_i \in \mathbf{F}_p,\ a_{t-1} \neq 0),$$

其中常数项 a_0 取为主密钥 k；控制中心再取 $\mathbf{F}_p$ 中 n 个不同的非零元素 $x_1, \cdots, x_n$(由 $p > n$ 知这是可能的)，将 $p, x_1, \cdots, x_n$ 均公开. 对每个 $i(1 \leqslant i \leqslant n)$，控制中心把 $y_i = h(x_i) \in \mathbf{F}_p$ 秘密给 A_i，作为 A_i 的子密钥.

现在我们证明这是一个门限为 t 的密钥共享方案.

(1) 设任意 t 个人聚在一起. 为符号简单，不妨设 $A_1, A_2, \cdots, A_t$ 联手. 则知道 $h(x_i) = y_i (1 \leqslant i \leqslant t)$. 由于 $x_1, \cdots, x_n$ 是 $\mathbf{F}_p$ 中不同

的(非零)元素,而 $h(x)$ 是 $\mathbf{F}_p[x]$ 中 $t-1$ 次多项式,我们在 §18 中讲述了:由 $h(x)$ 在 t 个不同点 $x_1,\cdots,x_t$ 的取值 $y_1,\cdots,y_t$ 可唯一决定这个多项式 $h(x)$. 于是算出主密钥 $k=h(0)$. 事实上,我们可以用拉格朗日插值公式给出

$$h(x)=y_1\frac{(x-x_2)\cdots(x-x_t)}{(x_1-x_2)\cdots(x_1-x_t)}+y_2\frac{(x-x_1)\cdots(x-x_t)}{(x_2-x_1)\cdots(x_2-x_t)}+$$

$$\cdots+y_t\frac{(x-x_1)\cdots(x-x_{t-1})}{(x_t-x_1)\cdots(x_t-x_{t-1})}.$$

因此可直接算出主密钥为

$$k=h(0)=y_1(-1)^{t-1}\frac{x_2\cdots x_t}{(x_1-x_2)\cdots(x_1-x_t)}$$

$$+y_2(-1)^{t-1}\frac{x_1x_3\cdots x_t}{(x_2-x_1)\cdots(x_2-x_t)}+$$

$$\cdots+y_t(-1)^{t-1}\frac{x_1\cdots x_{t-1}}{(x_t-x_1)\cdots(x_t-x_{t-1})}.$$

(2) 如果 $t-1$ 个人联手,不妨设 $A_1,\cdots,A_{t-1}$ 联手. 即从 $h(x_i)=y_i$ $(1\leqslant i\leqslant t-1)$ 是否能得到主密钥 k 的任何信息?也就是说,是否能够判定 $\mathbf{F}_p$ 中某个元素比较倾向于为主密钥呢?为此,我们对 $\mathbf{F}_p$ 中任意元素 l,看它是否有 $\mathbf{F}_p[x]$ 中 $t-1$ 次多项式 $h_1(x)$,使得

$$h_1(x_i)=y_i(1\leqslant i\leqslant t-1)$$

并且 $h_1(0)=l$?由于 $x_1,\cdots,x_{t-1}$ 均为非零元素,所以上述条件相当于多项式在 t 个不同点 $x_1,\cdots,x_{t-1},0$ 处的取值. 满足这些条件的 $\mathbf{F}_p[x]$ 中 $t-1$ 次多项式 $h_1(x)$ 是存在并且唯一的. 换句话说,当 $A_1,\cdots,A_{t-1}$ 联手,即在

$$h(x_i)=y_i(1\leqslant i\leqslant t-1)$$

的条件下,每个元素 $l\in\mathbf{F}_p$ 都以同样的可能性成为主密钥. 所以 $t-1$ 个人联手得不到主密钥的任何信息.

部分习题提示和注释

习　题　1

2. 在习题 1.1 中以 $-b$ 代换 b 得出.

3. 连续两个整数中必有一个偶数.

5. 配对.

6. $n \leqslant m$ 时易于证明;当 $n > m$ 时用带余除法化为前一种情形.

9. 反复用带余除法.

10. 对任意整数 n,有 $[x+n]=[x]+n$. 由此易知,可假设 α_i 满足 $0 \leqslant \alpha_i < 1$ 来论证.

习　题　2

1. 证明 a 与 b 互素,最基本的做法是选择 x,y,建立裴蜀等式

$$ax + by = 1.$$

2. 选择适当的 r(及 x,y),建立等式

$$ax + by = r.$$

设 $(a,b)=d$,则 $d \mid r$. 所谓适当的 r 是指:由 $d \mid r$ 能够通过进一步的论证导出 $d=1$;或者 r 的约数很少,进而可以由排除法证得 $d=1$.

3. 上面说的等式等价于 $a \mid (by-r)$ 或 $b \mid (ax-r)$. 利用整除,这些往往更容易导出来.

就本题而言,由于 m 是奇数,故 $(2^n+1) \mid (2^{mn}+1)$;又 $(2^m-1) \mid (2^{mn}-1)$. 从而

$$(2^n+1)\mid((2^m-1)q+2),\ q\text{ 是一个整数.}$$

由此知$(2^m-1,2^n+1)=1$ 或 2,显然这只能为 1.

4. 对指数作欧氏算法.

5. 当 $a\mid b$ 或 $b\mid a$ 时结论显然成立. 下面考虑相反的情形. 由于 $ax+by=d$ 有整数解,这里 $d=(a,b)$. 无妨设 $a>0$,作带余除法,$x=bq+r$,这里 $0<r<|b|$,我们有

$$ar+b(aq+y)=d.$$

易知 $0<|aq+y|=\left|\dfrac{ar-d}{b}\right|<|a|$.

6. 用定理 4(iv) 可得出证明.

7. (i) $(d,mn)=(d,m)\left(\dfrac{d}{(d,m)},\dfrac{mn}{(d,m)}\right)=(d,m)\left(\dfrac{d}{(d,m)},n\right)=(d,m)(d,n)$;

(ii) 利用(i) 即得出证明.

8. (i) 可先对$(a,b)=1$ 的情形证明;

(ii) 设 $d=(a,c)$,则 $d^n=(a^n,c^n)=(a^n,ab)=a$. 同样,$b=(b,c)^n$.

9. 由于$(n,n+1)=1$,可将问题分解为证明 $2(1^k+\cdots+n^k)$ 分别被 n 及 $n+1$ 整除;配对!

10. 用定理 2.

13. 解答习题 2.5 的方法.

14. (i) 全部解是 $x=10-2u-3v,y=u,z=v$,其中 u,v 是任意整数;

(ii) 三元一次不定方程可化为上述特殊情况. 方程中未知数系数的绝对值以 6 为最小,用 6 除方程的两边,得

$$x=-3y+2z+4+\frac{-2y+3z-1}{6}.$$

于是应有整数 u,使得

$$-2y+3z-1=6u. \tag{1}$$

方程(1)中,未知数系数的绝对值最小者为 2(< 6),将(1) 两边同除以

2，得到 $y=z+\frac{z-1}{2}-3u$，于是应有整数 v，使得 $z-1=2v$（有一个未知数的系数为 1），即 $z=2v+1$. 代入(1)式得 $y=3v-3u+1$，于是 $x=10u-5v+3$，(u，v 是任意整数).

也可将三元一次不定方程化为二元一次方程求解（利用习题 2.11）.

习　题　3

1. 当 n 不太大时，这可以实际地判别 n 是否为素数.

4. 例如，$(n+1)!+2,\cdots,(n+1)!+(n+1)$ 符合要求.

5. 修改定理 1 的证法. 注意，形如 $4m+3$ 的数必有一个素因子仍具有这种形式.

9. (i) 如 m 不是 2 的幂，则 m 有一个奇素数因子.

11. 设 $\frac{a}{c}=\frac{d}{b}=\frac{p}{q}$，这里 p，q 是互素的正整数. 则 $a=pu$，$c=qu$，$d=pv$，$b=qv$（u，v 为正整数）. 由此得出

$$a^4+b^4+c^4+d^4=(p^4+q^4)(u^4+v^4).$$

注意这一分解基于整数的性质，而不是代数式的分解.

12. 注意，所说的和中只包含有限个非零项. 在 $1,2,\cdots,n$ 中，被 p 整除的数有 $\left[\frac{n}{p}\right]$ 个，这其中有 $\left[\frac{n}{p^2}\right]$ 个被 p^2 整除，…，有 $\left[\frac{n}{p^l}\right]$ 个被 p^l 整除. 容易看出，p^e 作为 $p,p^2,\cdots,p^e$ 的倍数在和式中恰被计入 e 次.

13. 对任一素数 p，证明 p 在分子中出现的幂次不小于在分母中出现的幂次（用习题 1.10）.

15. 设 $p^\alpha \| n$，证明 $p^\alpha \left| \frac{a^n-b^n}{a-b}\right.$. 如 $p\nmid a-b$，这显然成立；如 $p|a-b$，设 $a-b=pt$. 于是

$$\frac{a^n-b^n}{a-b}=\sum_{i=1}^{n}\binom{n}{i}(pt)^{i-1}b^{n-i}.$$

证明上式右端和式中每一项均被 p^α 整除.(注意

$$\binom{n}{i}=\frac{n(n-1)\cdots(n-i+1)}{i!}$$

的分子被 p^α 整除,应用习题 3.12.)

16. 如果 d 是 n 的正约数,则 $\frac{n}{d}$ 也是 n 的正约数.

17. 用定理 3 的推论 2.

19. (i) 设 2^k 是不超过 n 的 2 的最高次幂,即 $2^k\leqslant n<2^{k+1}$,则 2^k 在 $1,2,\cdots,n$(的标准分解) 中只出现一次;

(ii) 修改(1) 的处理.

习　题　4

2. 特别地,本题给出了整数被 3,9 及 11 整除的一种实用判别法.

4. 对 n 归纳.

5. 如 $(d,n)=1$,则 $(n-d,n)=1$.

10. p 个连续整数 $n,n-1,\cdots,n-p+1$ 构成模 p 的一个完系,所以其中恰有一个被 p 整除. 设 $p\mid n-i(0\leqslant i\leqslant p-1)$,则 $\left[\frac{n}{p}\right]=\frac{n-i}{p}$.

11. 分解 $\frac{a^p+b^p}{a+b}$ 并模 $a+b$,注意 $a\equiv -b\pmod{a+b}$.

12. 设 $p^e\parallel n!$,证明分子中 p 的幂次至少是 e. 如果 $p\mid b$,则因 $e\leqslant n-1$,结论显然成立. 如 $p\nmid b$, 设 b^{-1} 使 $bb^{-1}\equiv 1\pmod{p^e}$, 则

$$\begin{aligned}&b^{-n}a(a+b)\cdots(a+(n-1)b)\\ \equiv&ab^{-1}(ab^{-1}+1)\cdots(ab^{-1}+n-1)\pmod{p^e}.\end{aligned}$$

同余式右端是连续 n 个整数之积,故被 $n!$ 整除,从而 $\equiv 0\pmod{p^e}$. 这一手法,将成算术数列的数,在同余意义下,化为连续的整数.

习 题 5

4. 这可由 $\mathbf{Z}_m^*$ 中没有零因子推出来.

5. 等价于 §4,定理 6(ii).

7. (i) 在 $\bar{a}$ 为乘法单位 $\bar{1}$ 时结论成立. 一般情形由 $\bar{a}=\bar{a}\cdot\bar{1}$ 导出来.

8. 用威尔逊定理.

习 题 6

3. 在欧拉定理中取 $a=-1$.

7. 用费马定理(参考 §5).

8. (i) 是显然的. 当 $n=1$ 时,(ii) 显然成立;如 $n>1$,可设 $n=p_1\cdots p_k$,则所说的和等于

$$\binom{k}{0}-\binom{k}{1}+\cdots+(-1)^k\binom{k}{k}=(1-1)^k=0.$$

(ii) 给出了特征函数 $f(n)=\begin{cases}1, & n=1,\\ 0, & n>1\end{cases}$ 的一种解析表达式.

9. 左边的和等于

$$\sum_{x=1}^{n} f(x)\sum_{d\mid(x,n)}\mu(d)=\sum_{x=1}^{n} f(x)\sum_{\substack{d\mid x\\ d\mid n}}\mu(d)$$

$$=\sum_{d\mid n}\mu(d)\sum_{\substack{x=1\\ d\mid x}}^{n} f(x)=\sum_{d\mid n}\mu(d)S_d.$$

10. 由习题 6.8 的(ii),我们有

$$\sum_{d\mid n}\mu(d)F\left(\frac{n}{d}\right)=\sum_{d\mid n}\mu(d)\sum_{l\mid\frac{n}{d}} f(l)$$

$$= \sum_{l|n} f(l) \sum_{d|\frac{n}{l}} \mu(d) = f(n).$$

反过来，我们有

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{l|d} \mu(l) F\left(\frac{d}{l}\right)$$

$$= \sum_{l|n} \mu(l) \sum_{\substack{l|d \\ d|n}} F\left(\frac{d}{l}\right) \quad (\text{令 } d = lk)$$

$$= \sum_{l|n} \mu(l) \sum_{k|\frac{n}{l}} F(k)$$

$$= \sum_{k|n} F(k) \sum_{l|\frac{n}{k}} \mu(l) = F(n).$$

11. 设 $(m,n) = 1$，对 mn 的任意正约数 d，记 $d_1 = (d,m)$，$d_2 = (d,n)$. 则由习题 2.7 得出，

$$H(mn) = \sum_{d_1|m} \sum_{d_2|n} f\left(\frac{m}{d_1} \cdot \frac{n}{d_2}\right) g(d_1 d_2)$$

$$= \sum_{d_1|m} \sum_{d_2|n} f\left(\frac{m}{d_1}\right) f\left(\frac{n}{d_2}\right) g(d_1 d_2)$$

$$= \sum_{d_1|m} f\left(\frac{m}{d_1}\right) g(d_1) \sum_{d_2|n} f\left(\frac{n}{d_2}\right) g(d_2)$$

$$= H(m)H(n).$$

12. 由定理 1(ii)，习题 6.11 知，等式的左边是积性函数，故只需对 n 为素数幂的情形证明.

习 题 7

6. (i) 易于证明. 由(i)知，(ii)中的必要性是显然的. 为了证明充分性，可用归纳法. 设 $x \equiv b_1 \pmod{m_1}$，$x \equiv b_2 \pmod{m_2}$ 的解是 $x \equiv c \pmod{[m_1,m_2]}$. 对任意 $3 \leqslant i \leqslant k$，易知

$$(m_1,m_i)\mid c-b_i,\quad (m_2,m_i)\mid c-b_i,$$

故 $c-b_i$ 是$[(m_1,m_i),(m_2,m_i)]$的倍数,从而 $c-b_i$ 被$([m_1,m_2],m_i)$ 整除(参考习题 3.17).因此由归纳假设知,同余方程组

$$x\equiv c\ (\mathrm{mod}\ [m_1,m_2]),\cdots,x\equiv b_k(\mathrm{mod}\ m_k)$$

可解;并且解是模 $[m_1,\cdots,m_k]$ 的一个同余类(§2,定理 4(ii)).

7. (i) 首先证明关于完系的结论:所说的数共有 $m_1\cdots m_k$ 个,且任两个模 $m_1\cdots m_k$ 不同余.为了证明关于缩系的结论,现在只要证明,所说的数与 $m_1\cdots m_k$ 互素的充分必要条件是$(x_i,m_i)=1\ (1\leqslant i\leqslant k)$.

9. 设 m' 是 m 的和 b 互素的最大因子.如果 $m'=1$,则 m 的素因子都是b的素因子(注意并不能推出 $m\mid b$).但$(a,b)=1$,从而$(a,m)=1$,结论显然成立.如果 $m'>1$,由孙子定理,同余式组 $x\equiv a\ (\mathrm{mod}\ b)$,$x\equiv 1\ (\mathrm{mod}\ m')$ 有解.易证任一解 $x>0$ 与 m 互素.(m 的素因子或整除 m' 或整除 b.)

习 题 8

4. 设 g 是模 p 的原根,则 $g,g^2,\cdots,g^{p-1}$ 是模 p 的缩系.

5. 比较 §7,例 3.

6. (ii) 设 g 是模 p 的一个原根,则所说的和模 p 同余于 $\sum_{d\mid p-1}\mu(d)S_d$,其中

$$S_d=\sum_{l=1}^{\frac{p-1}{d}}g^{dl}(\text{参考习题 6.9}).$$

易知,当 $d\neq p-1$ 时,$S_d\equiv 0\ (\mathrm{mod}\ p)$;而 $S_{p-1}\equiv 1\ (\mathrm{mod}\ p)$.

7. a 模 a^n-1 的阶是 n.

8. 假设结论不对,设 $n>1$ 是满足 $n\mid 2^n-1$ 的最小整数.设 2 模 n 的阶为 d,则 $1<d<n$.由于 $d\mid n$,故 $2^d\equiv 1\ (\mathrm{mod}\ d)$,这与 n 的最小性矛盾.(参考 §13,定理 2 的注记.)

10. 设 ab 模 m 的阶为 d，则 $a^d \cdot b^d \equiv 1 \pmod{m}$；可应用习题 8.9 及引理 3.

11. 用习题 8.10 及习题 2.6.

13. (i) 对 $a^p - 1$ 的任一素因子 q，考虑 a 模 q 的阶.

14. (i) 对 F_n 的任一素因子 p，证明 2 模 p 的阶是 2^{n+1}；

(ii) $F_n (n \geqslant 1)$ 两两互素.

习　题　9

6. $x^3 \equiv 1 \pmod{p}$ 仅有一个解.

习　题　10

3. (i) $x^2 + 1$ 的素因子或者是 2 或者模 4 同余于 1；

(ii) $x^2 + 2$ 的素因子或者为 2 或者模 8 同余于 1，3. 由此可证明有无穷多个 $8n + 3$ 形式的素数(参考 §3，定理 1 的证明). 其余的结论可采用类似的想法证明.

4. 设所说的素数只有有限个，其全体为 $p_1, \cdots, p_k$. 取 n 使 $\left(\frac{n}{p}\right) = -1$. 由孙子定理，同余式组

$$x \equiv n \pmod{p}, \quad x \equiv 1 \pmod{p_i} \ (1 \leqslant i \leqslant k)$$

有解. x 必有一个素因子 q，使 $\left(\frac{q}{p}\right) = -1$ 且 q 不同于 $p_1, \cdots, p_k$.

6. 如 q 是素数，则 $q \equiv 7 \pmod{8}$，从而 $\left(\frac{2}{q}\right) = 1$. 由欧拉判别法知 $q \mid M_p$. 反过来，考虑 2 模 q 的阶，证明 $\varphi(q) = q - 1$，从而 q 是素数.

7. 可以用模 p 的原根证明，也可用 §5，例 1 中的配对法.

8. (i) 和(ii). 注意，若 a 是模 p 的二次剩余，则 $p - a$ 也是模 p 的

二次剩余；

(iii) 对 $1 \leqslant k \leqslant \frac{p-1}{2}$，由带余除法，$k^2 = p\left[\frac{k^2}{p}\right] + r_k$（习题 1.8），$r_k$ 是模 p 的二次剩余.

9. (i) 用习题 10.8(iii) 的解法.

10. 对 $1 \leqslant x \leqslant p-1$，有 x^{-1} 使 $xx^{-1} \equiv 1 \pmod{p}$. 因此所说的和等于

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

11. (i) 甚为容易. 为证明(ii)，作代换 $u = x+y$，$v = x-y$，则数对 (u,v) 和 (x,y)（模 p）一一对应，得到 $uv \equiv a \pmod{p}$. 如果 $p \mid a$，则解数是 $p+p-1 = 2p-1$；如果 $p \nmid a$，任取 $u(1 \leqslant u \leqslant p-1)$，则模 p 唯一地确定 v，从而解数是 $p-1$.

12. 习题 10.11 中同余式的解数可表示为

$$\sum_{y=0}^{p-1}\left(1+\left(\frac{a+y^2}{p}\right)\right).$$

13. 用习题 10.12.

14. 必要性是显然的. 充分性可对 k 归纳来证明.

习　题　11

1. 用高斯引理中的记号，容易看出

$$\mu = \frac{p-1}{2} - \left[\frac{p}{4}\right].$$

3. (i) $p \equiv 1 \pmod{6}$；(ii) $p \equiv \pm 1 \pmod{5}$.

4. 利用习题 11.3(i).

5. 对 a 的任一素约数 q，证明 $\left(\frac{q}{p}\right) = 1$.（如 $a = \pm 1$ 结论显然成立.）

7. 证明模 p 的二次非剩余都是模 p 的原根；又

$$\frac{p-1}{2} = 2^{n-1} = \varphi(p-1).$$

习　题　12

2. 用习题 4.3(ii).

3. (i) 模 3,推出 x,y,z 都被 3 整除,以 $x = 3x_1, y = 3y_1, z = 3z_1$ 代入方程,重复这一手续可见,x,y,z 被 3 的任意正整数次幂除尽,故都是零.

本题也可采用下面不同形式的处理:问题中的方程是所谓的齐次方程,如果方程有非平凡整数解,可取一组满足$(x,y,z) = 1$ 的解.(参考 §25,定理 1.) 然后如上那样导出 $3|(x,y,z)$,矛盾.

4. 将方程看作 x 的一元二次方程,先寻求它有实数解的条件.

6. 不难验证,$(m,n) = (1,1)$ $(3,3)$ 都是解. 在方程有解时,通常,仅用同余不能求出所有解(除非问题非常特殊,如习题 12.3),而需结合其他方法. 本题中,用同余可以证明,当 $m \geqslant 5$ 时,方程无解. 因此解可通过逐一检验 $m = 1,2,3,4$ 求得.

习　题　13

1. 设正整数 x,y 使 $x(x+1) = y^2$. 两边乘 4,方程可分解为

$$(2x+2y+1)(2x-2y+1) = 1.$$

由此得出 $x = 1, y = 0$,矛盾.

处理不定方程,分解是最为基本的出发点. 上面的分解基于代数式的分解. 应用整数的性质也能产生适用的分解:因$(x,x+1) = 1$,故 x, $x+1$ 必须都是完全平方(习题 2.8),即 $x = u^2, x+1 = v^2$. 因此 $v^2 - u^2 = 1$,推出 $v = 1, u = 0$.(比较习题 3.11 的解答.)

2. x 显然是奇数. 在 y 为奇数时,方程可分解;并且导出此时无解.

当 y 为偶数时，x^y 是奇数的平方，模 4 表明方程也无解.

3. 方程有解 $x=3, y=2, z=3$. 显然 x 应是奇数，将方程变形为

$$(x-1)(x^{y-1}+\cdots+x+1)=2^z.$$

在 y 为奇数时，方程无解. 当 y 为偶数时，设 $y=2y_1$，方程分解为

$$(x^{y_1}-1)(x^{y_1}+1)=2^z.$$

故 $x^{y_1}-1$ 与 $x^{y_1}+1$ 都是 2 的方幂，又它们的最大公约数为 2，因此 $x^{y_1}-1=2$，得出 $x=3, y_1=1$(即 $y=2$)，进而 $z=3$.

当 y 为偶数时，也可采用不同的处理：因 x^{y_1} 是奇数，设为 $2k+1$，则 $x^y=4k(k+1)+1$. 方程成为

$$k(k+1)=2^{z-2}.$$

在 $k>1$ 时，k 和 $k+1$ 中必有一个是大于 1 的奇数，故有奇素因子. 因此必须 $k=1$.

4. 设 $2^m+3^n=x^2$. 显然 x 不被 2 和 3 整除. 模 3，方程化为 $(-1)^m\equiv 1 \pmod 3$. 故 m 是偶数.(这一手续，可看作在 $\mathbf{Z}_3$ 上将原方程消元.) 再模 4 知 n 是偶数.

6. 将有理点中两个坐标的分母化为相同，问题等价于确定方程 $x^2+y^2=z^2$ 的所有整数解.

7. 可由定理 2 推出来.

8. 对直角三角形的面积递降.

习 题 14

2. (i) n 是两整数的平方差的充分必要条件是 n 为奇数，或 n 被 4 整除.

5. 设 $p_1,\cdots,p_n$ 是互不相同的素数，均模 4 同于 3. 由孙子定理，同余方程组

$$x\equiv -p_i-i \pmod{p_i^2}\ (1\leqslant i\leqslant n)$$

有正整数解. 显然 $p_i \| (x+i)$. 由定理 2 知，$x+1,\cdots,x+n$ 都不能表示为两个整数的平方和.

习　题　15

1. 比较习题 1.1.

3. 对指数作欧氏算法. 比较习题 2.4.

5. 比较习题 2.5.

6. 显然，x^3 与 $(1-x)^2$ 互素，故所说的 $\alpha(x)$，$\beta(x)$ 必然存在. 由习题 15.5，可设

$$\alpha(x)=a_1x+a_0,\quad \beta(x)=b_2x^2+b_1x+b_0.$$

比较等式两边同次幂的系数，可确定待定的常数 a_i 和 b_j.

7. 比较习题 1.9.

8. 参考 §2，定理 4.

9. (i) 因 $\mathbf{Z}_m$ 是一个交换环(参考 §5).

(ii) 如 $m>1$ 且不是素数，则 $\mathbf{Z}_m$ 中有零因子.

(iii) 设 $\bar{k}$ 是 $\mathbf{Z}_m$ 中一个零因子，可取 $f(x)=x^m$，$g(x)=\bar{k}x^n$，其中 $m>n>0$. 试比较定理 3 在 $K=\mathbf{F}_p$ 的情形.

习　题　16

1. 比较习题 3.2.

2. 参考 §3，定理 3 的推论 1 与推论 2.

3. (i) 用习题 15.5；(ii) 反复用(i)；(iii) 用习题 15.7.

4. 由习题 16.3(从理论上) 可知所求表示式的形式，为了实际地确定它们，可应用待定系数法(将所作的等式化为多项式等式，并比较两边同次幂的系数；用 §17 中的代值法计算则更为简单).

习　题　17

3. 用定理 1.

4. 由本题可有效地确定一个整系数多项式的所有有理根，因为 a_n 与 a_0 的约数只有有限多个. 此外，本题还提供了证明一个复数为整数的基本出发点：首先证明它是一个有理数；再证明它是一个首项系数为 1 的整系数多项式的根.

5. 用定理 2 的推论 2.

6. (i) 是显然的；(ii) 用习题 5.7.

9. (i) 连续 k 个整数之积被 $k!$ 整除；

(ii) 熟知，当 x 为整数时，所说的等式成立，因此它是一个恒等式(参考定理 2 的推论 3). 这是证明多项式恒等式一种很基本的手法；

(iii) 用带余除法，任一个 n 次复系数多项式 $f(x)$ 均可表示为所说的形式(在 §15，定理 3 中取 $g(x)=\left(\frac{x}{n}\right)$). 如 $f(x)$ 是整值多项式，特别地，$f(0),(1),\cdots,f(n)$ 均是整数，由此逐次地推出 $a_0,a_1,\cdots,a_n$ 为整数；

(iv) 可假定连续 $n+1$ 个整数为 $0,1,\cdots,n$(为什么?)，用(iii)即得出结果.

习　题　18

1. 参考 §4，定理 4.

4. 可以用拉格朗日插值公式，也可采用下面的方法：$n+1$ 次多项式 $g(x)=xf(x)-1$ 在 $x=1,2,\cdots,n+1$ 处为零；又 $g(0)=-1$. 由 §17，定理 2 可确定 $g(x)$.

5. 可以用拉格朗日插值公式，也可用下面的方法：

$$g(x) = 2\left(\binom{x-1}{0} + \binom{x-1}{1} + \cdots + \binom{x-1}{n}\right)$$

是一个 n 次多项式，且

$$g(k) = 2^k (1 \leqslant k \leqslant n+1).$$

因此

$$g(x) - f(x) = 0 (\text{参考 } \S 17, \text{定理 2 的推论 2}).$$

现在易知

$$f(n+2) = 2^{n+2} - 2.$$

6. 这是拉格朗日定理的推论. 也可采用下面的方法(参考定理 4 的证明):对每个 $\alpha \in \mathbf{F}_p$，存在 $f_\alpha(x) \in \mathbf{F}_p[x]$，使得 $f_\alpha(\alpha) = \bar{1}$，而

$$f_\alpha(x) = \bar{0} (\text{对 } x \in \mathbf{F}_p, x \neq \alpha).$$

事实上，可取

$$f_\alpha(x) = \bar{1} - (x-\alpha)^{p-1}.$$

于是

$$f(x) = \sum_{\alpha \in \mathbf{F}_p} \varphi(\alpha) f_\alpha(x)$$

符合要求. 本题表明，$\mathbf{F}_p$ 到自身的映射仅有多项式映射.

7. 显然 $f(x)$ 是唯一确定的，它可用习题 18.6 的解法求出来. 更简单的做法是利用费马定理(习题 6.7) 而得出 $f(x) = x^{p-2}$.

8. 用拉格朗日定理.

习 题 19

2. 如 $f(x) \geqslant 0$(对所有实数 x)，则在 $f(x)$ 的标准分解中，一次不可约因式的幂次都是偶数；又二次不可约多项式 $x^2 + ax + b$ 可表示为 $(x+c)^2 + d^2$(c, d 均是实数). 用 § 14 中恒等式(2).

4. 若 $Re(\alpha) \leqslant 0$，或 $|\alpha| \leqslant 1$，则已无需证明. 对于 $\mathrm{Re}(\alpha) > 0$ 且 $|\alpha| > 1$，我们有 $Re\left(\frac{1}{\alpha}\right) > 0$. 故从

$$0 = \left|\frac{f(\alpha)}{\alpha^n}\right| \geqslant \left|a_0 + \frac{a_1}{\alpha}\right| - \frac{a_2}{|\alpha|^2} - \cdots - \frac{a_n}{|\alpha|^n}$$

$$\geqslant Re\left(a_0 + \frac{a_1}{\alpha}\right) - \frac{9}{|\alpha|^2} - \cdots - \frac{9}{|\alpha|^n}$$

$$> 1 - \frac{9}{|\alpha|^2 - |\alpha|},$$

可导出结论.

习 题 20

1. 条件意味着 $f(1) = 0$. 若 ζ 是任一 n 次单位根，则有 $f(\zeta^n) = 0$，因此 $f(x^n)$ 有因式 $x - \zeta$. 这些因式互不相同，积是 $x^n - 1$.

3. 本题给出了特征函数

$$f(n) = \begin{cases} 0, & \text{如 } m \nmid n \\ 1, & \text{如 } m \mid n \end{cases}$$

的一个解析表达式.

4. 用习题 20.3.

5. (i) 用韦达定理，所求的和是 0，积是 $(-1)^{n-1}$；

(ii) 和是 $\mu(n)$，积是 1. 参考并比较习题 8.6.

习 题 21

1. (ii) 分别用 $c(f)^{-1}f$ 和 $c(g)^{-1}g$ 代替 f 和 g；用高斯引理及(i).

2. 设 d 是一个整数，使 $dg(x)$ 为整系数. 则由 $d \cdot f(x)g(x) = f(x) \cdot dg(x)$ 及习题 21.1 知，$d \mid c(f) \cdot c(dg)$. 因由假设 $c(f) = 1$，故 $d \mid c(dg)$. 因此 $g(x)$ 的系数必须都是整数.

3. 用定理 1.

4. (i) 是显然的；(ii) 如有整系数多项式 $d(x)$ 使 $J = (d(x))$，则

特别地，有整数 a,b 使 $x = ad(x), 2 = bd(x)$，易导出矛盾.

习　题　22

2. (i) 记所说的多项式为 $f(x)$. 则 $f(x)$ 在 $\mathbf{Q}$ 上不可约，等价于 $g(x) = f(x+1)$ 在 $\mathbf{Q}$ 上不可约. 用定理 1 及 § 6 中的引理；

(ii) 比较习题 3.8.

3. 记所说的多项式为 $f(x)$，设

$$f(x) = g(x)h(x), g(x), h(x) \in \mathbf{Z}[x],$$

且 $\deg g, \deg h \geqslant 1$. 用 § 17，定理 2 的推论 2 证明 $g(x) = -h(x)$.

4. 记所说的多项式为 $f(x)$，设

$$f(x) = g(x)h(x), g(x), h(x) \in \mathbf{Z}[x],$$

且 $\deg g, \deg h \geqslant 1$. 一方面，$g(10)$ 是素数；另一方面，由 $f(x)$ 的根的性质可推出 $|g(10)| > 1$(参考习题 19.1，习题 19.4). 同样 $|h(10)|$ 是大于 1 的整数. 产生矛盾.

5. 参考习题 17.1.

习　题　23

2. 由定理 1 及墨比乌斯反转公式(习题 6.10).

3. 不难直接证明；也可用习题 23.1 中的恒等式(ii) 和(iii) 来证明.

4. 用习题 23.2 不难证明，模 p 的任一个 n 阶元都是所说的同余式的解；又解数不能超过 $\varphi(n)$(§ 7，定理 2)，结合 § 8，定理 4 的第二个断言即得出证明.

习 题 24

1. (i) 容易得知，如果 $x_1^2 + x_2^2 + x_3^2$ 在 **R** 上可约，则它必分解为 $(ax_1 + bx_2 + cx_3)(Ax_1 + Bx_2 + Cx_3)$ 的形式(参考 §25，定理 2). 取 x_1, x_2, x_3 适当的特殊值易导出矛盾. 此外，简单的配方表明，$x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_2x_3 + x_3x_1$ 在 **R** 上的不可约性可由前一个结论推出来.

2. 当 $x_1 = 0$ 及 $x_2 = 0$ 时，多项式为零，所以能被 x_1x_2 整除；如果 $x_1 = \omega x_2$ 及 $x_1 = \omega^2 x_2$(ω 是三次单位根，且 $\omega \neq 1$)，则所说的多项式也均为零，故能被 $(x_1 - \omega x_2)(x_1 - \omega^2 x_2) = x_1^2 + x_1x_2 + x_2^2$ 整除(参考定理 3).

3. 用定理 4 和定理 1.

4. 对 n 归纳(参考 §17，定理 2 的推论 3).

5. 对 n 归纳(参考 §17，定理 2 的推论 2).

习 题 25

2. 证明必要性时只需对 k 次单项式证明就够了(习题 25.1(i))；为证明充分性可参考定理 1 的证明.

3. 参考例 1 及习题 24.2.

4. (ii) 当 $x_1 = -x_2$ 时多项式为零.

5. 设 $F(x_1, x_2) = (x_1 - x_2)G(x_1, x_2)$，则 $G(x_1, x_2) + G(x_2, x_1) = 0$，因此 $G(x_1, x_1) = 0$. 故 $x_1 - x_2$ 是 $G(x_1, x_2)$ 的一个因式.

6. 设 F_k 是 F 的一个 k 次齐次部分. 对于 F_k 中任一单项式，任意交换其两个不定元后所得的单项式必在 F 中出现，因它是 k 次的，故它实际上属于 F_k.

习　题　26

1. (iii) 可先将多项式表示为齐次式的和(参考习题 25.6).

3. σ_n 可约,而 $\sigma_1,\cdots,\sigma_{n-1}$ 不可约. 注意 σ_i 关于每个 $x_j(1\leqslant j\leqslant n)$ 都是一次的.

4. 用 §19,定理 2.

5. 对 $i=1,2,\cdots,n$, 我们有

$$x_i^n-\sigma_1x_i^{n-1}+\cdots+(-1)^n\sigma_n=0.$$

将上式乘以 x_i^{k-n},并对 i 求和,即得 $k\geqslant n$ 时的结果.

为了证明当 $1\leqslant k<n$ 时有

$$s_k-\sigma_1s_{k-1}+\sigma_2s_{k-2}+\cdots+(-1)^{k-1}\sigma_{k-1}s_1+(-1)^k k\sigma_k=0. \tag{1}$$

我们注意,前面的结果表明,当 $x_1,\cdots,x_n$ 中有 $n-k$ 个等于零时,(1)式成立. 设 $n>l\geqslant k$,并设(1)在 $x_1,\cdots,x_n$ 中有 $n-l$ 个为零时成立. 下面考虑 $x_1,\cdots,x_n$ 中有 $n-l-1$ 个为零的情况;无妨设 $x_{l+2},\cdots,x_n$ 为零.

由归纳假设,在 $x_1,\cdots,x_{l+1}$ 中任一个为零时,(1)的左边为零,因而(1)的左边被 $l+1$ 次多项式 $x_1\cdots x_{l+1}$ 整除(§24,定理 3). 因此(1)的左边必是零;否则它是一个次数 $\leqslant k(<l+1)$ 的多项式. 故在这种情况下(1)仍成立,这就归纳证明了(1).

6. 对 k 归纳(用习题 26.5).

7. 这是定理 1 的平凡推论. 用牛顿公式及归纳法也可得出证明,并能递推地求 s_n 的值.