格理论与密码学

周福才　徐　剑　著

科学出版社

格理论与密码学

周福才　徐　剑　著

科学出版社

北　京

内 容 简 介

本书主要介绍格理论中的基础理论、关键技术及其在密码学中的典型应用。主要包括三方面内容:格理论与密码学的基础知识,包括数论基础、抽象代数基础、向量空间、对称密码体制、公钥密码体制、哈希函数等;格理论的基础理论和关键技术,包括格的基本定义、格中的计算性难题、最短向量问题、最近向量问题、二维格中的高斯格基约减算法、LLL 格基约减算法及其衍生和变形、LLL 与 apprCVP 问题以及格基约减算法的 MATLAB 实现;格理论在密码学中的典型应用,包括基于格的密码系统分析方法以及基于格理论的哈希函数。

本书可供从事信息安全、密码学、数学、计算机、通信等专业的科技人员参考,也可供高等院校相关专业的师生参考。

图书在版编目(CIP)数据

格理论与密码学/周福才,徐剑著.—北京:科学出版社, 2013
ISBN 978-7-03-036384-8

Ⅰ.格… Ⅱ.①周…②徐… Ⅲ.①格-理论②密码术 Ⅳ.①O153.1
②TN918.1

中国版本图书馆 CIP 数据核字(2012)第 319036 号

责任编辑:孙 芳 张 宇 张海丽 / 责任校对:刘小梅
责任印制:张 倩 / 封面设计:耕者设计工作室

科学出版社出版
北京东黄城根北街 16 号
邮政编码:100717
http://www.sciencep.com

新科印刷有限公司印刷
科学出版社发行 各地新华书店经销
*
2013 年 1 月第 一 版 开本:B5(720×1000)
2013 年 1 月第一次印刷 印张:11 1/2
字数: 227 000

定价: 60.00 元
(如有印装质量问题,我社负责调换)

前　言

信息在当今社会中的地位和作用越来越重要，它已经成为社会发展和进步的重要战略资源。信息技术已经改变了人们的传统生产和生活方式，社会的信息化已成为当今世界发展不可逆转的趋势和潮流。但是，信息技术的飞速发展也带来日益严峻的安全问题。目前，信息安全已成为人们日益关注的社会问题。伴随着计算机技术和网络技术的飞速发展，人们对信息安全的认识也日益深刻，对信息安全的属性要求也从最初的机密性、完整性发展到认证性、不可否认性以及可用性。为了达到人们对信息安全的属性要求，通常需要采用多种管理手段和相应的技术支持，而这其中最为常用，也是最为关键、最为核心的技术则是密码技术。

早期的密码学研究主要集中在机密性方面，即更多的是针对对称密码体制的研究和应用。对称密码体制在加密和解密过程中使用同一个密钥，包括的主要运算是置换和替代运算，因此效率很高，适合大数据量的加解密操作。但对称密码的缺陷是保密通信双方需要事先分配同一个密钥，由此会引起密钥的分配和管理问题；另外，由于对称密码体制难以支持数字签名机制，导致通信双方的身份无法确认。针对对称密码体制存在的问题，1976 年，Diffie 和 Hellman 在《密码学新方向》一文中提出了公钥密码学的思想，即使用两个密钥（公钥和私钥）来实现加解密操作和数字签名。其中，公钥是可以公开的密钥，用于加密数据或验证签名；私钥只能为消息的接收者或者签名者所掌握，用于解密或签名。公钥密码体制解决了对称密码体制中的密钥分发和管理的问题，也提供了数字签名的功能，使得在开放的网络环境中确保信息的机密性、完整性和不可否认性成为可能，开辟了密码学的新纪元，标志着现代密码学的开始。

自从 Diffie 和 Hellman 的公钥密码思想提出以来，先后出现了许多的公钥密码体制，这些体制大多建立在单向陷门函数的基础之上，其安全性往往基于一些复杂的数学难题。例如，RAS 密码体制是基于大整数分解难题，ElGamal 密码体制是基于离散对数问题，椭圆曲线密码体制是基于椭圆曲线点群上的离散对数问题。上述公钥密码体制中都包含各种代数结构（群、环、域）中大整数或多项式的复杂运算，因此，相对于对称密码体制，其运算效率较低，这也是一直制约公钥密码体制发展的重要因素之一。此外，大整数分解和离散对数问题已经被证明无法抵御量子攻击和亚指数攻击。因此，必须寻求更加高效和安全的公钥密码体制。

1996 年，Ajtai 在格问题困难性基础上给出了一个具有里程碑意义的结论，提出了基于格难题构造密码方案的可能性，为构造新型的公钥密码体制提供了一条崭新的研究思路。Ajtai 指出，某一类格中一些问题的平均难度等价于格上一类崭

新的研究思路。Ajtai 指出，某一类格中一些问题的平均难度等价于格上一类 NP 问题的难度。因此，在这些格问题基础上构建的公钥密码体制，其任意一个实例的安全性与其最难实例的安全性相同。这个优良的特性是目前大部分公钥密码体制所不具备的。同时，由于格是一种线性结构，格上的运算大多是线性运算，因此，利用格难题所构建的新型公钥密码体制具有比现有方案更快的运算速度。而且，到目前为止，还不存在解决某些格问题的多项式量子算法，因此，基于格难题所设计的新型公钥密码体制是可以抵御量子攻击的。鉴于上述特性，近几年基于格难题来分析与构造新型公钥密码体制的研究已经成为国际和国内密码学研究的一个热点。本书也将就格理论及其在密码学中的应用进行深入浅出的介绍。

本书共 6 章。第 1 章对密码学和格理论的相关数学基础进行了介绍，主要包括数论基础、抽象代数基础、向量空间等内容；第 2 章对密码学基础知识与相关典型算法进行了介绍，主要包括对称密码体制原理、公钥密码体制原理、DES 算法、AES 算法、Diffie-Hellman 密钥交换协议、RSA 密码系统、ElGamal 密码系统以及椭圆曲线密码系统；第 3 章对格的定义和相关性质进行了介绍，包括格的基本定义、格中的计算性难题、最短向量问题以及最近向量问题；第 4 章介绍了格基约减算法及其实现，包括二维格中的高斯格基约减算法、LLL 格基约减算法及其衍生和变形、LLL 与 apprCVP 问题以及格基约减算法的 MATLAB 实现；第 5 章介绍了基于格难题的密码系统，并利用格理论对同余密码系统、背包密码系统以及 NTRU 密码系统进行了安全性分析；第 6 章介绍了基于格理论的哈希函数 LBH 及应用，包括 LBH 的数学基础、LBH 的基础结构、LBH 的安全性、LBH 的代价分析，并在 LBH 的基础上给出了基于 LBH 的更新优化认证数据结构以及基于 LBH-UOADS 的数据查询认证方案。

本书由东北大学周福才、徐剑共同完成，博士研究生林慕清、李福祥、陈晨参与了本书的撰写和校对工作。在本书撰写过程中，在一些内容讨论和素材提供方面得到了东北大学师生的鼎力支持，他们包括博士研究生岳笑含，硕士研究生季东杰、王磊、陈科、金恒展、韩健、周杨、李宇溪等，在此向他们表示衷心的感谢。

本书得到了沈阳市科技计划项目(NO.F10-205-1-12)的支持，在此表示深深的谢意。

由于应用格理论进行密码学研究是一个崭新的研究方向，相关基础理论和关键技术还不够完善，再加上作者学识、水平有限，书中难免有不妥之处。作者期望本书能够起到抛砖引玉的作用，同时也希望得到读者的批评和指正，以达到不断完善基于格理论的密码学的目的。

作　者

2012 年 6 月于东北大学

目　　录

第1章　数学基础

本章将介绍本书用到的一些基本的数学概念和符号。1.1节和1.2节分别简要介绍数论和抽象代数的基础知识，对这些内容不熟悉的读者可以参考更详细的参考书籍；1.3节主要介绍定义在$\mathbb{R}^m$上的向量空间的概念和性质。充分理解本章内容对于其余各章的学习是非常必要的。

1.1　数论基础

数论和代数学是现代密码学的基础。本节将介绍数论中的一些重要定理和结论。数论是研究整数性质的一个数学分支，其研究对象是整数(自然数)。整数在计算机科学、密码学与信息安全、数字信号处理等领域起到了重要的作用。本节将介绍整除性和整数的分解，带余除法以及求解最大公因子的相关算法；并介绍模运算的运算法则与性质，以及求解线性同余方程组的方法；此外还介绍了素数、有限域、模除法运算的概念；最后介绍了有限域中的乘方和原根的性质。

1.1.1　整除性和最大公因子

若a,b是整数，则可以分别计算$a+b,a-b,a\cdot b$，且所得结果均是整数。这种性质称为对元素运算的封闭性。

但是对除法运算并不能总是满足这种运算封闭性。例如，不能用2去除3，因为3/2并不是整数，由此引出了整除性的基本概念。

定义1.1　设a,b是整数，$b\neq 0$。若存在整数c，满足$a=bc$，则称b整除a或a被b整除，记为$b|a$。

命题1.1　设$a,b,c\in\mathbb{Z}$，则有

(1) 若$a|b,b|c$，则$a|c$；

(2) 若$a|b,b|a$，则$a=\pm b$；

(3) 若$a|b,a|c$，则$a|(b+c)$且$a|(b-c)$。

定义1.2　a和b的公因子是能够同时整除二者的正整数。顾名思义，最大公因子就是满足$d|a,d|b$的最大的正整数d，用$\gcd(a,b)$来表示。在不存在歧义的情况下也可以表示成(a,b)。

最大公因子的概念虽然简单，但有很多应用。下面介绍几种计算最大公因子的方法。

定义 1.3(带余除法) 设 a,b 是正整数,则存在唯一的 q 和 r 满足

$$a=b\cdot q+r,\quad 0\leqslant r<b$$

若求 a 和 b 的最大公因子,首先对 a 作带余除法,即

$$a=b\cdot q+r,\quad 0\leqslant r<b$$

若 d 是 a 和 b 的公因子,则 d 也能够整除 r;若 e 是 b 和 r 的公因子,e 也能够整除 a。换言之,有

$$\gcd(a,b)=\gcd(b,r)$$

重复此过程,对 b 作带余除法,即

$$b=r\cdot q'+r',\quad 0\leqslant r'<r$$

则有

$$\gcd(b,r)=\gcd(r,r')$$

此过程将使余数越来越小,最终为 0,此时有

$$\gcd(s,0)=s=\gcd(a,b)$$

这种方法常称为辗转相除法,或欧几里得算法。

定理 1.1(欧几里得算法) 设 a,b 是正整数($a\geqslant b$),下述算法能够在有限步内计算出 $\gcd(a,b)$:

(1) 设 $r_0=a,r_1=b$;

(2) 令 $i=1$;

(3) 对 r_{i-1} 作带余除法,$r_{i-1}=r_i\cdot q_i+r_{i+1},0\leqslant r_{i+1}<r_i$;

(4) 若 $r_{i+1}=0$,则 $r_i=\gcd(a,b)$,算法结束;

(5) 若 $r_{i+1}>0$,令 $i=i+1$,转到第(3)步。

其中,第(3)步最多执行 $2\log_2 b+1$ 次。

证明 定理 1.1 所进行的带余除法过程可以用下列步骤来表示:

$$\begin{aligned}
a&=b\cdot q_1+r_2,\quad 0\leqslant r_2<b\\
b&=r_2\cdot q_2+r_3,\quad 0\leqslant r_3<r_2\\
r_2&=r_3\cdot q_3+r_4,\quad 0\leqslant r_4<r_3\\
r_3&=r_4\cdot q_4+r_5,\quad 0\leqslant r_5<r_4\\
&\vdots\\
r_{t-2}&=r_{t-1}\cdot q_{t-1}+r_t,\quad 0\leqslant r_t<r_{t-1}\\
r_{t-1}&=r_t\cdot q_t\\
r_t&=\gcd(a,b)
\end{aligned}$$

r_i 的值严格递减,当 $r_{i+1}=0$ 时算法结束。这就证明了算法能够在有限步内结束。

此外,在迭代过程中有

$$r_{i-1}=r_i\cdot q_i+r_{i+1},\quad 0\leqslant r_{i+1}<r_i$$

这表明

$$\gcd(r_{i-1},r_i)=\gcd(r_i,r_{i+1}),\quad i=1,2,3,\cdots$$

当 $r_{t+1}=0$ 时，有 $r_{t-1}=r_t\cdot q_t$，故

$$\gcd(r_{t-1},r_t)=\gcd(r_t\cdot q_t,r_t)=r_t$$

再由迭代等式可知

$$\gcd(a,b)=r_t$$

也就是说最后一个不为零的余数就是 a 和 b 的最大公因子。

证毕

下面分析算法的效率。因为 r_i 的值严格递减，且 $r_1=b$，故算法最多执行 b 步就能够终止。然而，这样求出的只是一个上界。注意，随着步骤(3)的每两次迭代，r_i 的值至少能够减半：$r_{i+2}<\frac{1}{2}r_i$，$i=0,1,2,\cdots$。下面分两种情况证明此不等式。

情况 1：$r_{i+1}\leqslant\frac{1}{2}r_i$。

由于 r_i 严格递减，故

$$r_{i+2}<r_{i+1}\leqslant\frac{1}{2}r_i$$

情况 2：$r_{i+1}>\frac{1}{2}r_i$。

考虑 r_{i+1} 除 r_i，即

$$r_i=r_{i+1}\cdot 1+r_{i+2}$$

则有

$$r_{i+2}=r_i-r_{i+1}<r_i-\frac{1}{2}r_i=\frac{1}{2}r_i$$

综合两种情况，能够证明

$$r_{i+2}<\frac{1}{2}r_i,\quad i=0,1,2,\cdots$$

反复利用这个等式将得

$$r_{2k+1}<\frac{1}{2}r_{2k-1}<\frac{1}{4}r_{2k-3}<\frac{1}{8}r_{2k-5}<\frac{1}{16}r_{2k-7}<\cdots<\frac{1}{2^k}r_1=\frac{1}{2^k}b$$

因此，若有 $2^k\geqslant b$，则

$$r_{2k+1}<1\Rightarrow r_{2k+1}=0$$

算法结束。

在定理证明过程中，$r_{t+1}=0$，则 $t+1\leqslant 2k+1\Rightarrow t\leqslant 2k$，且在上述算法中共执行了 t 次除法，故欧几里得算法至多在 $2k$ 次迭代后结束。选取满足 $2^k\geqslant b>2^{k-1}$ 的最小的 k，则迭代次数$\leqslant 2k=2(k-1)+2<2\log_2 b+2$。

上述定理证明了欧几里得算法至多执行 $2\log_2 b+1$ 次迭代。然而，这个估计

值可以被改进。已有文献证明,迭代次数不超过 $1.45\log_2 b+1.68$,且对于随机选取的 a 和 b,平均迭代次数约为 $0.85\log_2 b+0.14$。

定理 1.2(扩展的欧几里得算法) 设 a,b 是正整数,存在 u,v 满足

$$au+bv=\gcd(a,b)$$

证明 从欧几里得算法得知

$$a=b\cdot q_1+r_2$$

将其代入

$$b=r_2\cdot q_2+r_3$$

可得

$$b=(a-b\cdot q_1)\cdot q_2+r_3$$

故

$$r_3=-a\cdot q_2+b\cdot(1+q_1q_2)$$

再将结果代入

$$r_2=r_3\cdot q_3+r_4$$

最终得

$$a-b\cdot q_1=[-a\cdot q_2+b\cdot(1+q_1q_2)]q_3+r_4$$

整理可得

$$r_4=a\cdot(1+q_2q_3)-b\cdot(q_1+q_3+q_1q_2q_3)$$

即为 $r_4=a\cdot u+b\cdot v$ 的形式。

重复此过程将得

$$r_t=a\cdot u+b\cdot v=\gcd(a,b)$$

证毕

定义 1.4 设 a,b 是整数,当 $\gcd(a,b)=1$ 时,称 a 和 b 互素。

一般地,可以在等式 $Au+Bv=\gcd(A,B)$ 两端同除 $\gcd(A,B)$,得

$$\frac{A}{\gcd(A,B)}u+\frac{B}{\gcd(A,B)}v=1$$

则 $\dfrac{A}{\gcd(A,B)}$ 和 $\dfrac{B}{\gcd(A,B)}$ 互素。

1.1.2 模运算

本小节介绍模运算的概念和相关性质。

定义 1.5 设 m 为自然数,a 和 b 是任意整数,如存在关系 $a=b+km$,其中 k 为整数,则定义 $a\equiv b(\mathrm{mod}\,m)$,其含义为:$b$ 是 a 除以 m 的余数(b 为 a 模 m 的余数,或 a 与 b 模 m 同余)。

定义 1.6 $a\mathrm{mod}\,m$ 表示 a 模 m 运算,表示 a 除以 m 的余数,其值能够取遍 0

到 $m-1$ 之间的整数。

例如，$(7+8)\bmod 12=15\bmod 12=3$，也可表示成：$15\equiv 3 \pmod{12}$。

模运算（$+,-,\times$）满足交换律、结合律和分配律。按模运算原理：对中间结果做模运算，与做完全部运算后再做模运算的所得结果相同。

命题 1.2　设整数 $m\geqslant 1$，则有

（1）若 $a_1\equiv a_2 \pmod m$，$b_1\equiv b_2 \pmod m$，则 $a_1\pm b_1\equiv a_2\pm b_2 \pmod m$，且 $a_1\cdot b_1\equiv a_2\cdot b_2 \pmod m$。

（2）设 a 为整数，当且仅当 $\gcd(a,m)=1$ 时，存在整数 b 满足 $a\cdot b\equiv 1 \pmod m$。若这样的 b 存在，称其为 a 模 m 的乘法逆元，也可以是 a^{-1} 表示 a 的逆元。

证明

（1）设

$$a_1=a_2+k_1 m,\quad b_1=b_2+k_2 m$$

则

$$a_1\pm b_1=a_2\pm b_2+(k_1\pm k_2)m$$

即

$$a_1\pm b_1\equiv a_2\pm b_2 \pmod m$$

对于 $a_1\cdot b_1\equiv a_2\cdot b_2 \pmod m$，有

$$a_1\cdot b_1=(a_2+k_1 m)\cdot(b_2+k_2 m)=a_2\cdot b_2+(k_1 b_2+k_2 a_2+k_1 k_2 m)\cdot m$$

即

$$a_1\cdot b_1\equiv a_2\cdot b_2 \pmod m$$

（2）必要性：设 $\gcd(a,m)=1$，由定理 1.2 知，存在整数 b,v 满足 $ab+mv=1$，即 $ab-1=-mv$，能够被 m 整除，由同余定义知 $ab\equiv 1 \pmod m$。

充分性：设 a 存在模 m 逆元，即 $a\cdot b\equiv 1 \pmod m$，则存在整数 c 使得 $ab-cm=1$。又因为 $\gcd(a,m)$ 能够整除 $ab-cm=1$，故 $\gcd(a,m)=1$。

证毕

当除数与模 m 互素时，可以进行模除法运算。例如，已知 $7^{-1}\equiv 8 \pmod{11}$，计算 $\frac{5}{7}=5\cdot 7^{-1}\equiv 5\cdot 8\equiv 40\equiv 7 \pmod{11}$。

继续讨论模运算的性质。若对 a 做带余除法 $a=m\cdot q+r$，$0\leqslant r<m$。这表明满足 $a\equiv r \pmod m$ 的 r 能够取 0 到 $m-1$ 之间的所有整数。所以，若要研究模 m 的整数，只需要取 $0\leqslant r<m$ 即可。这就引出了同余类的概念。

定义 1.7　记整数模 m 同余类环为

$$\mathbb{Z}/m\mathbb{Z}=\{0,1,2,\cdots,m-1\}$$

注意到在同余类环中所进行的运算，所得结果均需模 m 以保持运算的封闭性。

定义 1.8 命题 1.2 中的命题(2)证明了若 $\gcd(a,m)=1$,则 a 存在模 m 的乘法逆元。这种具有逆元的元素称为单位,用如下记号来表示所有单位构成的集合:

$$(\mathbb{Z}/m\mathbb{Z})^*=\{a\in\mathbb{Z}/m\mathbb{Z}:\gcd(a,m)=1\}$$

集合$(\mathbb{Z}/m\mathbb{Z})^*$称为整数模 m 单位群。

例 1.1 整数模 24 单位群为$(\mathbb{Z}/24\mathbb{Z})^*=\{1,5,7,11,13,17,19,23\}$;整数模 7 单位群为$(\mathbb{Z}/7\mathbb{Z})^*=\{1,2,3,4,5,6\}$。

密码学领域中很重要的一个问题就是如何表示$(\mathbb{Z}/m\mathbb{Z})^*$中的元素个数。定义这个量为欧拉函数。

定义 1.9 欧拉函数表示$(\mathbb{Z}/m\mathbb{Z})^*$中元素的个数,记为

$$\phi(m)=\#(\mathbb{Z}/m\mathbb{Z})^*=\#\{0\leqslant a<m:\gcd(a,m)=1\}$$

从例 1.1 中可得,$\phi(24)=8$,$\phi(7)=6$。

1.1.3 中国剩余定理

在一千多年前的《孙子算经》中,有这样一道算术题: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?按照今天的话来说就是:一个数除以 3 余 2,除以 5 余 3,除以 7 余 2,求这个数。

这样的问题,也有人称为“韩信点兵”。它形成了一类问题:初等数论中如何解线性同余式。这类问题的有解条件和解的方法被称为“中国剩余定理”或“孙子定理”。

最简单的情形是只有两个同余式

$$x\equiv a(\mathrm{mod}\,m)\text{和 }x\equiv b(\mathrm{mod}\,n)\ \gcd(m,n)=1$$

则由中国剩余定理可得上述方程组有唯一解。下面来看一个简单的例子。

例 1.2 求下面同余方程组的解:

$$\begin{cases}x\equiv 1(\mathrm{mod}5)\\ x\equiv 9(\mathrm{mod}11)\end{cases}\tag{1.1}$$

解 由模运算的定义可知第一个等式的解具有以下形式:

$$x=1+5y,\quad y\in\mathbb{Z}\tag{1.2}$$

将式(1.2)代入式(1.1)的第 2 个等式可得

$$1+5y\equiv 9(\mathrm{mod}11)$$

因此

$$5y\equiv 8(\mathrm{mod}11)\tag{1.3}$$

为了解出 y,将式(1.3)两端乘以 5(mod11)的乘法逆元 9,即

$$y\equiv 9\cdot 8\equiv 72\equiv 6(\mathrm{mod}11)$$

将 y 的值代入到式(1.2)中,最终算出

$$x=1+5\cdot 6=31$$

定理 1.3(中国剩余定理)　设 $m_1,m_2,\cdots,m_k$ 两两互素,$a_1,a_2,\cdots,a_k$ 是任意整数,则线性同余方程组

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ x\equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x\equiv a_k \pmod{m_k} \end{cases}$$

存在唯一解 $x=c$。

若 $x=c$ 和 $x=c'$ 都是方程组的解,则 $c=c' \pmod{m_1 m_2\cdots m_k}$。

证明　利用数学归纳法证明存在性。假设对于某个 i,已经找到满足前 i 个同余式

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ x\equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x\equiv a_i \pmod{m_i} \end{cases}$$

的解 $x=c_i$,下面证明如何找到满足前 $i+1$ 个同余式

$$\begin{cases} x\equiv a_1 \pmod{m_1} \\ x\equiv a_2 \pmod{m_2} \\ \quad\vdots \\ x\equiv a_{i+1} \pmod{m_{i+1}} \end{cases}$$

的解。显然这个解应该具有 $x=c_i+m_1 m_2\cdots m_i y$ 的形式。

由于这个解一定满足前 i 个同余式,故实际上需要寻找 y 满足

$$c_i+m_1 m_2\cdots m_i y\equiv a_{i+1} \pmod{m_{i+1}}$$

因为 $\gcd(m_{i+1},m_1 m_2\cdots m_i)=1$,由命题 1.2 中命题(2)可知这样的 y 一定存在。

证毕

上述中国剩余定理的证明过程就是一个求解同余方程组的算法,下面用一个例子来说明。

例 1.3　求解下面的同余方程组:

$$\begin{cases} x\equiv 2 \pmod 3 \\ x\equiv 3 \pmod 7 \\ x\equiv 4 \pmod{16} \end{cases}$$

解　由中国剩余定理可知,上述方程组存在模 $336=3\cdot 7\cdot 16$ 的唯一解。首先求解第 1 个方程 $x\equiv 2 \pmod 3$,$x=2+3y$,代入第 2 个方程可得

$$2+3y\equiv 3 \pmod 7$$

化简得 $3y\equiv 1 \pmod 7$,等式两端乘以 3mod7 的乘法逆元 5,得到 $y\equiv$

$5(\mathrm{mod}7)$,则有

$$x=2+3y=2+3\cdot 5=17$$

得到了第 1 个方程的解。从而满足前两个方程的解具有如下形式:

$$x=17+21z \tag{1.4}$$

将式(1.4)代入第 3 个方程得

$$17+21z\equiv 4(\mathrm{mod}16)$$

化简得 $5z\equiv 3(\mathrm{mod}16)$,两端再乘以 $5\mathrm{mod}16$ 的乘法逆元 13,得

$$z\equiv 3\cdot 13\equiv 39\equiv 7(\mathrm{mod}16)$$

最后代入 $x=17+21z$,可得方程组的解为

$$x=17+21\cdot 7=164$$

1.1.4 利用中国剩余定理求解二次同余式

利用中国剩余定理能够很容易求解大合数模的同余方程组:首先将大合数模作素数分解,然后求解素数模同余式构成的方程组,最后再利用中国剩余定理求出方程组的解。本小节讨论利用中国剩余定理求解模 m 的二次同余式的方法。当 m 为模 4 余 3 的素数时,求解最为简单,故首先介绍这种情况。

命题 1.3 设 p 是满足 $p\equiv 3(\mathrm{mod}4)$ 的素数,$a\in\mathbb{C}$,且二次同余式 $x^2\equiv a(\mathrm{mod}p)$ 有解,即 a 存在模 p 的平方根,则解具有形式

$$b\equiv a^{(p+1)/4}(\mathrm{mod}p)$$

证明 设 g 是模 p 的原根,则 a 等于 g 的乘方,且 a 存在模 p 的平方根意味着 a 是 g 的偶数乘方,即 $a\equiv g^{2k}(\mathrm{mod}p)$。下面计算解 b:

$$\begin{aligned}b^2&\equiv a^{\frac{p+1}{2}}(\mathrm{mod}p)\\&\equiv (g^{2k})^{\frac{p+1}{2}}(\mathrm{mod}p)\\&\equiv g^{(p+1)k}(\mathrm{mod}p)\\&\equiv g^{2k+(p-1)k}(\mathrm{mod}p)\\&\equiv a\cdot (g^{p-1})^k(\mathrm{mod}p)\\&\equiv a\end{aligned}$$

例 1.4 计算 $a=2201$ 模素数 $p=4127$ 的平方根。

解 $b\equiv a^{(p+1)/4}=2201^{4128/4}\equiv 2201^{1032}\equiv 3718(\mathrm{mod}4127)$

可以验证:$3718^2=13823524\equiv 2201(\mathrm{mod}4127)$。

当 m 为合数求解平方根时,需要将 m 做因子分解,并利用中国剩余定理计算同余方程组的解。下面是一个例子。

例 1.5 解二次同余式:

$$x^2 \equiv 197 (\mathrm{mod} 437)$$

解　对 437 做因子分解 $437 = 19 \cdot 23$，首先解同余方程组

$$\begin{cases} y^2 \equiv 197 \equiv 7 (\mathrm{mod} 19) \\ z^2 \equiv 197 \equiv 13 (\mathrm{mod} 23) \end{cases}$$

因为 19 和 23 均模 4 余 3，故由命题 1.3 能够算出

$$y \equiv \pm 8 (\mathrm{mod} 19), \quad z \equiv \pm 6 (\mathrm{mod} 23)$$

下面选择两个正值来求解同余方程组

$$\begin{cases} x \equiv 8 (\mathrm{mod} 19) \\ x \equiv 6 (\mathrm{mod} 23) \end{cases}$$

由中国剩余定理计算出解 $x \equiv 236 (\mathrm{mod} 437)$。

从上例可以看出，若已知 m 的素因子分解，计算模 m 的平方根是比较简单的。然而，若 m 是一个不容易被分解的大整数时，求解模 m 的平方根就十分困难了。实际上，此时分解 m 与求解模 m 的平方根的困难程度相当。

若 m 是一个分解式未知的大合数，则确定给定的整数 a 是否存在模 m 的平方根是一个困难问题。著名的 Goldwasser-Micali 公钥密码系统就是基于此困难问题的。求解难题的陷门就是 m 的分解式。

1.1.5　唯一分解性和有限域

1.1.2 小节介绍了模运算的性质，并了解如何进行加法、减法和乘法运算。随之而来的问题是如何在模条件下进行除法运算。因为只有当 $\gcd(a, m) = 1$ 时，才可以在 $\mathbb{Z}/m\mathbb{Z}$ 中除以 a。但是，注意到，若 m 是素数，就可以在 $\mathbb{Z}/m\mathbb{Z}$ 中除以任意的非零元。因此，本小节首先介绍素数的概念。

定义 1.10　若整数 $p \geqslant 2$，且其所有的正因子只有 1 和 p，则称 p 为素数。

例如，前 10 个素数分别为 2，3，5，7，11，13，17，19，23，29，第十万个素数是 1299709，第一百万个素数是 15485863。素数个数是无限的。

命题 1.4　设 p 为素数，假设 p 能够整除 ab，则 p 至少能够整除 a 和 b 其中的一个。一般地，若有 $p \mid a_1 a_2 \cdots a_n$，则 p 至少能够整除一个 a_i。

证明　令

$$g = \gcd(a, p)$$

则

$$g \mid p \Rightarrow g = 1 \text{ 或 } g = p$$

若 $g = p$，则 $p \mid a$；否则 $g = 1$，由定理 1.2 知存在 u 和 v 满足

$$au + pv = 1$$

两端乘以 b 得

$$abu + pbv = b$$

因为 p 整除 ab,故等式左端能够被 p 整除,即 $p \mid b$。

证毕

为了证明一般结论,可以将乘积写为

$$a_1(a_2 a_3 \cdots a_n)$$

将 a_1 视为 a,$a_2 a_3 \cdots a_n$ 视为 b,按照上段步骤进行证明。

若 $p \mid a_1$,则证明结束;否则,若 $p \mid a_2 \cdots a_n$,将其写成

$$a_2 \cdots a_n = a_2(a_3 \cdots a_n)$$

重复上段证明过程,直至找到 a_i 能够被 p 整除。

命题 1.4 能够证明每个正整数都能够唯一分解成一些素数的乘积(代数学基本定理)。

定理 1.4(代数学基本定理) 设整数 $a \geqslant 2$,则 a 能够写成如下形式:

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdots p_r^{e_r}$$

其中,p_i 均为素数。在不考虑各素数排列顺序的条件下,分解式是唯一确定的。

证明 首先证明分解的存在性。

若 a 为素数,定理显然成立。若 a 不是素数,设 p_1 是 a 的最小真因子,则 p_1 一定为素数,因为 p_1 的真因子也是 a 的真因子,所以 p_1 不能有真因子。设 $a = p_1 a_1$,对 a_1 重复上述过程,则至多 n 步后可以得到 $a = p_1 p_2 \cdots p_k$,再将相同的因子写到一起,就证明了分解的存在性。

下面证明唯一性。设 a 可分解为 $a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$,其中 p_i 和 q_j 都是素数。因为 $p_1 \mid a$,故 $p_1 \mid q_1 q_2 \cdots q_t$。由命题 1.4 知,$p_1$ 能够整除某个 q_i。重新排列顺序后不妨假设 $p_1 \mid q_1$,但由于 p_1 和 q_1 都是素数,故有 $p_1 = q_1$。等式变成 $p_2 \cdots p_s = q_2 \cdots q_t$。重复以上步骤 s 次,将得到 $1 = q_{t-s} q_{t-s+1} \cdots q_t$,故有 $t = s$。这就证明了在不考虑各素数排列顺序的条件下分解式是唯一确定的。

证毕

定义 1.11 代数学基本定理说明当正整数 a 被分解为素数乘积时,每个素数 p 都有唯一确定的指数。称这个指数为 a 中素数 p 的阶,用 $\mathrm{ord}_p(a)$ 表示(为了简便起见,对所有的素数记 $\mathrm{ord}_p(1) = 0$)。

例如,$1728 = 2^6 \cdot 3^3$,故 $\mathrm{ord}_2(1728) = 6$,$\mathrm{ord}_3(1728) = 3$,$\mathrm{ord}_p(1728) = 0$($p \geqslant 5$),利用符号 ord_p 可以简洁地将 a 的分解式表示为

$$a = \prod_{\text{primes } p} p^{\mathrm{ord}_p(a)}$$

通常将 ord_p 视为一个函数:

$$\mathrm{ord}_p : \{1,2,3,\cdots\} \to \{0,1,2,3,\cdots\}$$

通过上述讨论能够观察到,若 p 为素数,则任意的非零元模 p 都存在乘法逆元。这就意味着在模 p 条件下不仅可以进行加、减、乘法运算,也可以进行除法

运算。

命题 1.5　设 p 为素数，则$\mathbb{Z}/p\mathbb{Z}$中的非零元存在乘法逆元，即存在 b 满足

$$ab\equiv 1(\mathrm{mod}\,p)$$

记 b 为 $a^{-1}\,\mathrm{mod}\,p$。

证明　由命题 1.2 中(2)知，若模为素数 p，显然对非零元 $a\in\mathbb{Z}/p\mathbb{Z}$，有 $\gcd(a,p)=1$。

证毕

利用扩展的欧几里得算法(定理 1.2)可以计算 $a^{-1}\,\mathrm{mod}\,p$，只需得到等式 $au+pv=1$，并令 $u=a^{-1}\,\mathrm{mod}\,p$。

命题 1.5 也可以用另一种方式来表述：若 p 为素数，则

$$(\mathbb{Z}/p\mathbb{Z})^*=\{1,2,3,4,\cdots,p-1\}$$

换言之，$(\mathbb{Z}/p\mathbb{Z})^*$ 中元素都是单位，并且在除法运算下封闭。

定义 1.12　若 p 为素数，则集合$\mathbb{Z}/p\mathbb{Z}$连同其上的加、减、乘、除运算构成一个域。如用抽象代数的知识表达，域就是每个非零元都存在乘法逆元的一个(交换)环。例如，实数域 $\mathbb{R}$，有理数域 $\mathbb{Q}$和复数域 $\mathbb{C}$。元素个数有限的域称为有限域，有限域在密码学研究领域具有极其重要的应用。

尽管$\mathbb{Z}/p\mathbb{Z}$和F_p表示同一个概念，但在两个系统中元素相等的表示方法略有不同。对于 $a,b\in\mathrm{F}_p$，两者相等表示为 $a=b$；但若 $a,b\in\mathbb{Z}/p\mathbb{Z}$，相等则用模等式来表示，即 $a\equiv b(\mathrm{mod}\,p)$。

1.1.6　有限域中的乘方和原根

在密码学领域中应用的有限域经常会涉及元素的乘方运算。本小节将从纯数学的角度讨论这个问题。

先给出一个例子：当 $a=1,2,\cdots,6$ 时，分别计算 $a^6\,\mathrm{mod}7$，可以得到 $a^6\equiv 1(\mathrm{mod}7)$；但是当 a 是 7 的倍数时，显然有 $a^6\equiv 0(\mathrm{mod}7)$。因此，有

$$a^6\equiv\begin{cases}1(\mathrm{mod}7), & 7\nmid a\\ 0(\mathrm{mod}7), & 7\mid a\end{cases}$$

定理 1.5(Fermat 小定理)　设 p 为素数，a 为任意整数，则有

$$a^{p-1}\equiv\begin{cases}1(\mathrm{mod}\,p), & p\nmid a\\ 0(\mathrm{mod}\,p), & p\mid a\end{cases}$$

证明　若读者熟悉群论，可以观察到F_p中的非零元构成阶为 $p-1$ 的群F_p^*，由 Lagrange 定理知，F_p^* 中元素的阶都能整除 $p-1$。

若不利用群论知识，可以给出以下更为直接的证明。

若 $p\mid a$，显然有

$$a^{p-1}\equiv 0(\mathrm{mod}\,p)$$

故只需证明的 $p\nmid a$ 情况。在 mod$p$ 条件下考虑以下各数：

$$a,2a,3a,\cdots,(p-1)a$$

首先用反证法证明这 $p-1$ 个数各不相同，若

$$ja\equiv ka(\mathrm{mod}\,p)\Rightarrow(j-k)a\equiv 0(\mathrm{mod}\,p)$$

则有 $p|(j-k)a$。因为 $p\nmid a$，故 $p|(j-k)$。

但由于 j 和 k 都是 1 到 $p-1$ 间的整数，故

$$j-k=0\Rightarrow j=k$$

与假设矛盾。故这 $p-1$ 个数各不相同。

也就是说模 p 条件下

$$a,2a,3a,\cdots,(p-1)a$$

能够取遍 1 到 $p-1$ 间的整数，所以

$$a\cdot 2a\cdot 3a\cdots(p-1)a\equiv 1\cdot 2\cdot 3\cdots(p-1)(\mathrm{mod}\,p)$$

又因为

$$\gcd((p-1)!,p)=1$$

所以等式两端约掉$(p-1)!$，即得 $a^{p-1}\equiv 1(\mathrm{mod}\,p)$。

证毕

利用 Fermat 小定理可以快速地计算模 p 的乘法逆元，因为 $a^{-1}\equiv a^{p-2}(\mathrm{mod}\,p)$。这种方法的计算量与扩展的欧几里得算法大概相同。

例 1.6 分别用 Fermat 小定理和扩展的欧几里得算法计算 $7814^{-1}\,\mathrm{mod}17449$。

解 由 Fermat 小定理得

$$7814^{-1}\equiv 7814^{17447}\equiv 1284(\mathrm{mod}17449)$$

由扩展的欧几里得算法解 $7814u+17449v=1$，得$(u,v)=(1284,-575)$。故 $7814^{-1}\equiv 1284(\mathrm{mod}17449)$。

例 1.7 判断整数 $m=15485207$ 是否为素数。

利用快速乘方算法不难算出：

$$2^{m-1}=2^{15485206}\equiv 4136685(\mathrm{mod}1548207)$$

由 Fermat 小定理知，若 m 为素数，则同余式的结果应该为 1。也就是说若结果不为 1，m 一定不是素数。

上述例子说明了只要进行简单的计算就可以在不知道 m 分解式的情况下得知 m 是否为素数。

Fermat 小定理表明，若 a 不是 p 的倍数，则有 $a^{p-1}\equiv 1(\mathrm{mod}\,p)$。然而，对于 a 来说是否存在一个最小的指数使其模 p 余 1？答案是肯定的，并称这个最小的指数为 a 模 p 的阶。

命题 1.6 设 p 为素数，整数 a 不能被 p 整除。假设 $a^n\equiv 1(\mathrm{mod}\,p)$，则 a 模 p 的阶 k 能够整除 n，特别地有 $k|(p-1)$。

证明　由阶的定义知，k 满足 $a^k \equiv 1 \pmod{p}$，而且是最小的正指数。设 n 满足

$$a^n \equiv 1 \pmod{p}$$

对 n 做带余除法得

$$n = kq + r, \qquad 0 \leqslant r < k$$

则

$$1 \equiv a^n \equiv a^{kq+r} \equiv (a^k)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{p}$$

但 $r < k$，而 k 又是满足与 1 同余的最小的正指数，故

$$r = 0, n = kq, \Rightarrow k \mid n$$

再由 Fermat 小定理知

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

故

$$k \mid (p-1)$$

Fermat 小定理描述了有限域中单位的特殊性质。下面将讨论另一个在理论和实践中都十分重要的定理。

定理 1.6(原根定理)　设 p 为素数，则存在元素 $g \in \mathrm{F}_p^*$，满足 g 的乘方能够生成整个 F_p^*，即

$$\mathrm{F}_p^* = \{1, g, g^2, g^3, \cdots, g^{p-2}\}$$

称 g 为 F_p 的原根或 F_p^* 的生成元，它是 F_p^* 中阶为 $p-1$ 的元。

例 1.8　2 是有限域 F_{11} 的原根：

$$2^0 = 1 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 8 \quad 2^4 = 5$$
$$2^5 = 10 \quad 2^6 = 9 \quad 2^7 = 7 \quad 2^8 = 3 \quad 2^9 = 6$$

3 是有限域 F_{17} 的原根：

$$3^0 = 1 \quad 3^1 = 3 \quad 3^2 = 9 \quad 3^3 = 10 \quad 3^4 = 13 \quad 3^5 = 5 \quad 3^6 = 15 \quad 3^7 = 11$$
$$3^8 = 16 \quad 3^9 = 14 \quad 3^{10} = 8 \quad 3^{11} = 7 \quad 3^{12} = 4 \quad 3^{13} = 12 \quad 3^{14} = 2 \quad 3^{15} = 6$$

若 p 是大素数，则有限域 F_p 存在很多原根。确切的数量可以用欧拉函数来表示：F_p 中存在 $\phi(p-1)$ 个原根。例如，$\{2,3,8,10,11,14,15,18,19,21,26,27\}$ 是 F_{29} 的所有原根的集合。这与 $\phi(28)=12$ 的结果是一致的。一般地，若 $k \mid (p-1)$，则 F_p^* 中存在 $\phi(k)$ 个元素的阶为 k。

1.2　抽象代数基础

1.2.1　群

群是一种抽象的代数结构。简单地说，一个集合和在集合上满足某些性质的运算就构成了一个群。对于不熟悉群论的读者，本小节将简要介绍群论的基本概

念，此外还将讨论F_p^*中元素的指数运算。由于指数运算只是简单的重复乘法，所以首先强调一些F_p^*中乘法的重要性质。其性质如下：

（1）单位元：任取 $a\in F_p^*$，存在 $1\in F_p^*$，满足 $1\cdot a=a$。

（2）逆元：任取 $a\in F_p^*$，存在 $a^{-1}\in F_p^*$，满足 $a\cdot a^{-1}=a^{-1}\cdot a=1$。

（3）结合律：任取 $a,b,c\in F_p^*$，有 $a\cdot(b\cdot c)=(a\cdot b)\cdot c$。

（4）交换律：任取 $a,b\in F_p^*$，有 $a\cdot b=b\cdot a$。

若用F_p中的加法运算代替F_p^*中的乘法运算，那么上述性质中的 1 对应于 0，a^{-1}则对应于$-a$，四条性质依然成立：

（1）单位元：任取 $a\in F_p$，存在 $0\in F_p$，满足 $0+a=a$。

（2）负元：任取 $a\in F_p$，存在$-a\in F_p$，满足 $a+(-a)=(-a)+a=0$。

（3）结合律：任取 $a,b,c\in F_p$，有 $a+(b+c)=(a+b)+c$。

（4）交换律：任取 $a,b\in F_p$，有 $a+b=b+a$。

若不考虑具体的集合与运算，只提取出相应的性质，能够抽象出这类代数系统的一般概念——群。

定义 1.13 群包含一个非空集合 G 和一个运算 $*$，运算保持封闭性，即对于 $a,b\in G$，有 $a*b\in G$，并且要求运算 $*$ 满足下述性质：

（1）单位元：任取 $a\in G$，存在 $e\in G$，满足 $e*a=a*e=a$。

（2）逆元：任取 $a\in G$，存在唯一的 $a^{-1}\in G$，满足 $a*a^{-1}=a^{-1}*a=e$。

（3）结合律：任取 $a,b,c\in G$，有 $a*(b*c)=(a*b)*c$。

此外，若也满足交换律：任取 $a,b\in G$，有 $a*b=b*a$，则称 G 为交换群或阿贝尔群。

若 G 包含有限个元素，则称 G 为有限群。用 $|G|$ 或 $\sharp G$ 来表示群中元素的数量，称为 G 的阶。

下面举出一些与群相关的例子：

（1）$G=F_p^*$，$*$ =乘法，单位元 $e=1$，则 G 是阶为 $p-1$ 的有限群。

（2）$G=Z/NZ$，$*$ =加法，单位元 $e=0$，a 的逆元是$-a$，则 G 是阶为 N 的有限群。

（3）$G=Z$，$*$ =加法，单位元 $e=0$，a 的逆元是$-a$，则 G 是无限群。

（4）$G=Z$，$*$ =乘法，则 G 不是群，因为 Z 的大多数元素在 Z 中并不存在乘法逆元。

（5）当 $G=R^*$，$*$ =乘法时，G 是一个群，因为所有的元素在 R^* 中均有逆。

（6）给出一个非交换群的例子：$*$ =矩阵乘法，定义

$$G=\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d\in R \text{ 且 } ad-bc\neq 0\right\}$$

单位元

$$\boldsymbol{e}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$$

逆元

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}^{-1}=\begin{bmatrix}\dfrac{d}{ad-bc} & \dfrac{-b}{ad-bc}\\ \dfrac{-c}{ad-bc} & \dfrac{a}{ad-bc}\end{bmatrix}$$

注意到 G 是非交换的，如

$$\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\neq\begin{bmatrix}1 & 0\\ 1 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$$

(7) 更一般地，可以给出一般线性群的定义：$*$ =矩阵乘法，且

$$GL_n(¡)=\{\text{所有满足 } \det(\boldsymbol{A})\neq 0 \text{ 的实系数 } n\times n \text{ 矩阵 } \boldsymbol{A}\}$$

其中，¡ 也可以用其他的域来代替，如有限域F_p。

设 $g\in G$，x 为正整数，则 g^x 表示对 g 进行 x 次群运算，即

$$g^x=g*g*g*\cdots*g$$

例如，F_p^* 中的 g^x 表示 x 个 g 相乘。¢/N¢ 中的 g^x 表示 x 个 g 相加。虽然加法通常表示成 $x\cdot g$，但这只是符号表示的区别，关键要理解 g^x 的含义是对 g 重复进行 x 次群运算。

当 x 是负数时，$g^x=(g^{-1})^{|x|}$；当 $x=0$ 时，$g^0=e$，即群中的单位元。

下面定义群中元素的阶的概念。

定义 1.14　设 G 是群，$a\in G$，假设存在正整数 d 满足 $a^d=e$，则其中最小的 d 称为元素 a 的阶。若这样的 d 不存在，则称 a 的阶为无穷大。

下面将介绍元素阶的两个重要性质。

命题 1.7　设 G 是有限群，则群中元素的阶都有限。此外，设 $a\in G$ 且 a 的阶为 d，当 $a^k=e$ 成立时，有 $d|k$。

证明　因为 G 是有限群，所以序列 $a,a^2,a^3,a^4,\cdots$ 最终会出现重复的元素。也就是说，存在正整数 $i,j(i<j)$ 使得 $a^i=a^j$。两端乘以 a^{-i}，则有 $a^{i-j}=e$。因为 $i-j>0$，说明了存在某些正整数使得 a 的幂为单位元。设其中最小的一个正整数为 d，则有 $a^d=e$。

假设存在 $k\geqslant d$ 也满足 $a^k=e$，对 k 作带余除法得

$$k=dq+r,\quad 0\leqslant r<d$$

因为

$$a^k=a^d=e$$

则

$$e=a^k=a^{dq+r}=(a^d)^q*a^r=e^q*a^r=a^r$$

但因为 d 是使得 $a^d=e$ 成立的最小的正整数，所以 $r=0$。因此有

$$k=dq,\quad d\mid k$$

定理 1.7（Lagrange 定理） 设 G 是有限群，$a\in G$，则 a 的阶能够整除 G 的阶。确切来说，设群 G 的阶为 n，元素 a 的阶为 d，则有 $a^n=e$，$d\mid n$。

证明 给出当 G 为交换群时的证明。因为 G 的阶有限，则

$$G=\{g_1,g_2,\cdots,g_n\}$$

将其中每个元素都乘以 a，得到一个新的集合

$$S_a=\{a*g_1,a*g_2,\cdots,a*g_n\}$$

并且，S_a 中的元素各不相同。如若不然，不妨设

$$a*g_i=a*g_j$$

两端左乘 a^{-1} 得 $g_i=g_j$。与 G 的定义矛盾。因此 $S_a=G$，并且

$$(a*g_1)*(a*g_2)*\cdots*(a*g_n)=g_1*g_2*\cdots*g_n$$

又因为 G 是交换群，所以

$$a^n*g_1*g_2*\cdots*g_n=g_1*g_2*\cdots*g_n$$

两端分别乘以 $(g_1*g_2*\cdots*g_n)^{-1}$，得

$$a^n=e$$

再根据命题 1.6 可以得出 $d\mid n$。

1.2.2 环

群是在一个集合上定义了一种运算，这种运算可以令两个元素“相乘”并得到第三个元素。而环是在一个集合上定义“加法”和“乘法”两种运算，并存在分配律将它们联系起来。

定义 1.15 环 R 就是在一个集合上定义两种运算，分别用 $+$，$*$ 来表示，并满足如下运算性质：

1）加法

（1）单位元：任取 $a\in R$，存在加法单位元 $0\in R$，满足 $0+a=a+0=a$。

（2）负元：任取 $a\in R$，存在加法负元 $b\in R$，满足 $a+b=b+a=0$。

（3）结合律：任取 $a,b,c\in R$，有 $a+(b+c)=(a+b)+c$。

（4）交换律：任取 $a,b\in R$，有 $a+b=b+a$。

简言之，在加法运算的意义下，R 可视为单位元为 0 的交换群。

2）乘法

（1）单位元：任取 $a\in R$，存在乘法单位元 $1\in R$，满足 $1*a=a*1=a$。

（2）结合律：任取 $a,b,c\in R$，有 $a*(b*c)=(a*b)*c$。

（3）交换律：任取 $a,b\in R$，有 $a*b=b*a$。

注意到并未要求元素具有乘法逆元。此外，加法和乘法之间还满足分配律：

任取 $a,b,c\in R$,有 $a*(b+c)=a*b+a*c$。

通常来说,环的定义中并不要求乘法运算具有单位元和交换律,但在本书中讨论的环都是具有单位元的交换环,这一点请读者注意。

定义 1.16　若环 R 中每个非零元都有乘法逆元,则称 R 为域。

下面列举一些环和域的相关例子:

(1) $R=\mathbb{Q}$, $*$ =乘法,+=加法。乘法单位元是 1,且每个非零元都有乘法逆元,所以 $\mathbb{Q}$ 是一个域。

(2) $R=\mathbb{Z}$, $*$ =乘法,+=加法。乘法单位元是 1,但只有 1 和 −1 有乘法逆元,所以 $\mathbb{Z}$ 只是环而不是域。

(3) $R=\mathbb{Z}/n\mathbb{Z}$, n 是正整数, $*$ =乘法,+=加法。乘法单位元是 1。

(4) $R=\mathrm{F}_p$, p 是素数, $*$ =乘法,+=加法。乘法单位元是 1,由命题 1.5 可知,每个非零元都有乘法逆元,所以 F_p 是域。

(5) 整系数多项式的集合在通常的多项式加法和乘法意义下构成一个环 $\mathbb{Z}[x]$,可以表示为

$$\mathbb{Z}[x]=\{a_0+a_1x+a_2x^2+\cdots+a_nx^n : n\geqslant 0, a_0,a_1,\cdots,a_n\in\mathbb{Z}\}$$

(6) 一般地,若 R 是环,则可以构成系数取自 R 中的多项式环。例如,R 可以是 $\mathbb{Z}/q\mathbb{Z}$ 或有限域 F_p。

1.2.3　可约性和商环

1.1 节介绍的整数集 $\mathbb{Z}$ 中的可约性概念可以推广到任意环中。

定义 1.17　设 $a,b\in R$, $b\neq 0$,当存在 $c\in R$ 使得 $a=b*c$ 成立时,称 b 整除 a,或 a 能够被 b 整除,表示为 $b\mid a$。

命题 1.1 给出的可约性性质和证明对于环也同样满足。相类似的,在环中有 $b\mid 0$, $b\neq 0$。然而,并非所有的环都具有和 $\mathbb{Z}$ 一样好的性质。

例如,在环中就存在两个非零元的乘积是零的情况:在 $\mathbb{Z}/6\mathbb{Z}$ 中,$\overline{2}\cdot\overline{3}=\overline{6}=\overline{0}$。

素数被定义为没有非平凡因子的整数。通过将整数 a 表示为 $a=1\cdot a$ 或 $a=(-1)(-a)$ 的形式可以分解任意的整数,这些就是平凡分解。之所以称为平凡是因为 1 和 −1 具有乘法逆元。若 R 是环,且 $u\in R$ 有乘法逆元 $u^{-1}\in R$,则任给 $a\in R$ 都可分解成 $a=u^{-1}\cdot(ua)$。具有乘法逆元的元素和只能够进行平凡分解的元素都是环中的特殊元,下面将介绍其定义。

定义 1.18　设 R 是环,若 $u\in R$ 有乘法逆元,则称 u 为单位。即存在 $v\in R$,满足 $u*v=1$。设 $a\in R$,若 a 不是单位并且对于 a 的每个分解 $a=b*c$,都有 b 或 c 是单位,则称 a 是不可约的。

整数具有唯一因子分解性质,但并非所有的环都具有这种重要的性质,如系数在域中的多项式环是唯一因子分解环。

整数中的同余概念是一个十分重要且有力的数学工具。利用可约性的概念可以将同余的概念扩展到任意的环。

定义 1.19 设 R 是环，$a,b,m\in R,m\neq 0$。若 $a-b$ 能够被 m 整除，则称 a 和 b 模 m 同余，记为 $a\equiv b(\mathrm{mod}\,m)$。

命题 1.8 设 R 是环，$m\in R,m\neq 0$。若 $a_1\equiv a_2(\mathrm{mod}\,m)$且 $b_1\equiv b_2(\mathrm{mod}\,m)$，则 $a_1\pm b_1\equiv a_1\pm b_2(\mathrm{mod}\,m)$，且 $a_1 * b_1\equiv a_2 * b_2(\mathrm{mod}\,m)$。

定义 1.20 设 R 是环，$m\in R,m\neq 0$。对于任意的 $a\in R$，用 $\bar{a}$ 表示所有满足 $a'\equiv a(\mathrm{mod}\,m)$的 a'的集合，则集合 $\bar{a}$ 称为 a 的同余类，并用 $R/(m)$或 R/mR 来表示所有同余类的集合。即

$$R/(m)=R/mR=\{\bar{a}:a\in R\}$$

显然有以下性质成立：

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

称 $R/(m)$为 R 除 m 的商环。

1.2.4 多项式环与欧几里得算法

若 R 是环，则可以构成系数取自 R 中的多项式环

$$R[x]=\{a_0+a_1x+a_2x^2+\cdots+a_nx^n:n\geqslant 0,a_0,a_1,\cdots,a_n\in R\}$$

非零多项式最高次项的次数称为多项式的次数，记为 $\deg(f)$。若

$$f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n,\qquad a_n\neq 0$$

则有 $\deg(f)=n$，并称 a_n 为首项系数。当非零多项式首项系数为 1 时，称 $f(x)$为首一多项式。

尤为重要的一种情况是：当环 R 满足域的条件，如 $R=\mathbb{Q},\mathbb{R},\mathbb{C},\mathbb{F}_p$，在密码学领域，最重要的一种情形就是有限域$\mathbb{F}_p$。之所以将 R 限定为域 F，是因为$\mathbb{C}$中的所有性质在多项式环 $\mathrm{F}[x]$中都能够满足。本书将讨论 $\mathrm{F}[x]$的相关性质。

首先做多项式除法：x^5+2x^4+7 除以 x^3-5。利用多项式的除法，很容易得出

$$x^5+2x^4+7=(x^2+2x)\cdot(x^3-5)+(5x^2+10x+7)$$

注意到余式 $5x^2+10x+7$ 的次数严格小于除式 x^3-5 的次数。

只要 F 为域，就可以在多项式环$\mathrm{F}[x]$中做上述多项式运算。这种具有带余除法的多项式环称为欧几里得环，简称欧式环。

命题 1.9(欧式环) 设F 为域，$a,b\in \mathrm{F}[x],b\neq 0$，则存在

$$k,r\in \mathrm{F}[x],\qquad \deg r<\deg b$$

可以将多项式 a 表示为 $a=b\cdot k+r$，称为对 a 作带余除法。

证明 若能找到满足 $\deg r<\deg b$ 的 r 和 b，使得 $a=b\cdot k+r$ 成立，则证明结束。

否则，设

$$\boldsymbol{b}=b_0+b_1x+\cdots+b_dx^d$$

$$\boldsymbol{r}=r_0+r_1x+\cdots+r_ex^e$$

$$b_d\neq 0,\quad r_e\neq 0,\quad e\geqslant d$$

则 $\boldsymbol{a}=\boldsymbol{b}\cdot\boldsymbol{k}+\boldsymbol{r}$ 可以重新写成

$$\boldsymbol{a}=\boldsymbol{b}\cdot\left(\boldsymbol{k}+\frac{r_e}{b_d}x^{e-d}\right)+\left(\boldsymbol{r}-\frac{r_e}{b_d}x^{e-d}\cdot\boldsymbol{b}\right)=\boldsymbol{b}\cdot\boldsymbol{k}'+\boldsymbol{r}'$$

这样相当于降低了 $\boldsymbol{r}$ 的次数，所以有

$$\deg\boldsymbol{r}'<\deg\boldsymbol{r}$$

若

$$\deg\boldsymbol{r}'<\deg\boldsymbol{b}$$

则证明结束。

否则继续此过程。最终将会得到次数严格小于 $\boldsymbol{b}$ 的多项式 $\boldsymbol{r}$，即

$$\deg\boldsymbol{r}<\deg\boldsymbol{b}$$

下面定义 $F[x]$ 中公因式和最大公因式的概念。

定义 1.21　设 $\boldsymbol{a},\boldsymbol{b},\boldsymbol{d}\in F[x]$，若 $\boldsymbol{d}$ 能够同时整除 $\boldsymbol{a}$ 和 $\boldsymbol{b}$，则称 $\boldsymbol{d}$ 为 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的公因式。若同时 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的每个公因式都能够整除 $\boldsymbol{d}$，则称 $\boldsymbol{d}$ 为 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的最大公因式。

下面将看到 $F[x]$ 中的每两个多项式都存在最大公因式，用 $\gcd(\boldsymbol{a},\boldsymbol{b})$ 表示其中的首一多项式，则 $\gcd(\boldsymbol{a},\boldsymbol{b})$ 唯一。

随之而来的问题就是每两个多项式是否都存在最大公因式？这并非一个显而易见的问题，实际上，在很多环中最大公因式并不存在，如 $\not\subset[x]$。但当 F 是域时，多项式环 $F[\boldsymbol{x}]$ 中一定存在最大公因式。

命题 1.10（扩展的欧几里得算法）　设 F 是域，多项式 $\boldsymbol{a},\boldsymbol{b}\in F[x]$，$\boldsymbol{b}\neq 0$，则 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 的最大公因式 $\boldsymbol{d}$ 存在，并存在多项式 $\boldsymbol{u},\boldsymbol{v}\in F[x]$，满足 $\boldsymbol{a}\cdot\boldsymbol{u}+\boldsymbol{b}\cdot\boldsymbol{v}=\boldsymbol{d}$。

证明　同定理 1.1 的证明，$\gcd(\boldsymbol{a},\boldsymbol{b})$ 可以通过反复应用命题 1.9 得到，同理，$\boldsymbol{u},\boldsymbol{v}$ 的计算过程同定理 1.2。

证毕

例 1.9　利用欧几里得算法在 $F_{13}[x]$ 中计算 $\gcd(x^5-1,x^3+2x-3)$。

解

$$x^5-1=(x^3+2x-3)\cdot(x^2+11)+(3x^2+4x+6)$$

$$x^3+2x-3=(3x^2+4x+6)\cdot(9x+1)+(9x+4)$$

$$3x^2+4x+6=(9x+4)\cdot(9x+8)+0$$

因此 $9x+4$ 是 x^5-1 和 x^3+2x-3 在 $F_{13}[x]$ 中的一个最大公因式。为了得到首一多项式，将 $9x+4$ 乘以 $3\equiv 9^{-1}(\mathrm{mod}13)$ 得到 $\gcd(x^5-1,x^3+2x-3)=x-1$。

$$\begin{aligned}
&\boldsymbol{a}=\boldsymbol{b}\cdot\boldsymbol{k}_1+\boldsymbol{r}_2, \quad 0\leqslant\deg\boldsymbol{r}_2<\deg\boldsymbol{b}\\
&\boldsymbol{b}=\boldsymbol{r}_2\cdot\boldsymbol{k}_2+\boldsymbol{r}_3, \quad 0\leqslant\deg\boldsymbol{r}_3<\deg\boldsymbol{r}_2\\
&\boldsymbol{r}_2=\boldsymbol{r}_3\cdot\boldsymbol{k}_3+\boldsymbol{r}_4, \quad 0\leqslant\deg\boldsymbol{r}_4<\deg\boldsymbol{r}_3\\
&\boldsymbol{r}_3=\boldsymbol{r}_4\cdot\boldsymbol{k}_4+\boldsymbol{r}_5, \quad 0\leqslant\deg\boldsymbol{r}_5<\deg\boldsymbol{r}_4\\
&\vdots \qquad\qquad \vdots \qquad\qquad \vdots\\
&\boldsymbol{r}_{t-2}=\boldsymbol{r}_{t-1}\cdot\boldsymbol{k}_{t-1}+\boldsymbol{r}_t, \quad 0\leqslant\deg\boldsymbol{r}_t<\deg\boldsymbol{r}_{t-1}\\
&\boldsymbol{r}_{t-1}=\boldsymbol{r}_t\cdot\boldsymbol{k}_t\\
&\boldsymbol{d}=\boldsymbol{r}_t=\gcd(\boldsymbol{a},\boldsymbol{b})
\end{aligned}$$

在 1.2.3 小节中提到了单位和不可约元的概念。在多项式环 $F[x]$ 中，不难看出，单位一定是非零常数多项式，即 F 中的非零元。

例 1.10 多项式 $x^5-4x^3+3x^2-x+2$ 在 $\not\in[x]$ 中是不可约的，但是作为 $F_3[x]$ 中的多项式，它可以分解为

$$x^5-4x^3+3x^2-x+2\equiv(x+1)(x^4+2x^3+2)(\mathrm{mod}3)$$

作为 $F_5[x]$ 中的多项式时，分解式为

$$x^5-4x^3+3x^2-x+2\equiv(x^2+4x+2)(x^3+x^2+1)(\mathrm{mod}5)$$

作为 $F_{13}[x]$ 中的多项式时，它又是不可约的。

每个整数都可以唯一分解成一些素数的乘积。当系数是域中元素时，这个性质对于多项式环也成立。证明过程同整数类似，都是利用扩展的欧几里得算法。

命题 1.11 设 F 是域，则 $F[x]$ 中的每个非零多项式可以唯一分解成首一不可约多项式的乘积，也就是说，设 $\boldsymbol{a}\in F[x]$，常数 $\alpha,\beta\in F$，$\boldsymbol{p}_1,\cdots,\boldsymbol{p}_m,\boldsymbol{q}_1,\cdots,\boldsymbol{q}_n$ 是首一不可约多项式，若有以下两种分解式：

$$\boldsymbol{a}=\alpha\boldsymbol{p}_1\cdot\boldsymbol{p}_2\cdots\boldsymbol{p}_m,\boldsymbol{a}=\beta\boldsymbol{q}_1\cdot\boldsymbol{q}_2\cdots\boldsymbol{q}_n$$

则通过重排 $\boldsymbol{q}_1,\cdots,\boldsymbol{q}_n$ 的顺序，可得

$$\alpha=\beta, m=n, \boldsymbol{p}_i=\boldsymbol{q}_i, \qquad 1\leqslant i\leqslant m$$

证明

存在性证明：若 $\boldsymbol{a}=\boldsymbol{b}\cdot\boldsymbol{c}$，则 $\deg\boldsymbol{a}=\deg\boldsymbol{b}+\deg\boldsymbol{c}$。

唯一性证明：证明过程同定理 1.3。证明的关键在于若 $\boldsymbol{p}\in F[x]$ 不可约且可分解为 $\boldsymbol{p}=\boldsymbol{a}\cdot\boldsymbol{b}$，则有 $\boldsymbol{p}\mid\boldsymbol{a}$ 或 $\boldsymbol{p}\mid\boldsymbol{b}$（或同时满足）。

证毕

1.2.5 多项式环的商和素数阶有限域

1.2.3 小节和 1.2.4 小节分别介绍了多项式环和商环，本小节将这两者相结合，考虑多项式商环的概念。

在讨论整数的模运算时，模 m 的同余类可以表示为 0 到 $m-1$ 之间的一个整数，而多项式的带余除法则表明在多项式商环中也可以做类似的运算。

命题 1.12 设F是域，非零多项式 $\boldsymbol{m}\in \mathrm{F}[x]$，则每个非零同余类 $\overline{\boldsymbol{a}}\in \mathrm{F}[x]/(\boldsymbol{m})$都存在唯一的代表元 $\boldsymbol{r}$，满足

$$\deg \boldsymbol{r}<\deg \boldsymbol{m},\qquad \boldsymbol{a}\equiv \boldsymbol{r}(\bmod \boldsymbol{m})$$

证明 利用命题 1.9 对 $\boldsymbol{a}$ 作带余除法 $\boldsymbol{a}=\boldsymbol{m}\cdot \boldsymbol{k}+\boldsymbol{r}$，则有 $\boldsymbol{r}=0$ 或 $\deg \boldsymbol{r}<\deg \boldsymbol{m}$。若 $\boldsymbol{r}=0$，则 $\boldsymbol{a}\equiv 0(\bmod \boldsymbol{m})$，故 $\overline{\boldsymbol{a}}=0$。

若 $\deg \boldsymbol{r}<\deg \boldsymbol{m}$，由带余除法可知这样的 $\boldsymbol{r}$ 存在。为了证明其唯一性，假设存在 $\boldsymbol{r}'$ 也满足条件，则有

$$\boldsymbol{r}-\boldsymbol{r}'\equiv \boldsymbol{a}-\boldsymbol{a}\equiv 0(\bmod \boldsymbol{m})$$

故

$$\boldsymbol{m}\mid(\boldsymbol{r}-\boldsymbol{r}')$$

又因为

$$\deg \boldsymbol{r}<\deg \boldsymbol{m}$$

故

$$\boldsymbol{r}-\boldsymbol{r}'=0$$

例 1.11 考虑环 $\mathrm{F}[x]/(x^2+1)$。由命题 1.12 可知，商环中的每个元素都可以被唯一表示成 $\overline{\alpha+\beta x}$ 的形式，其中 $\alpha,\beta\in \mathrm{F}$。加法运算如下：

$$\overline{\alpha_1+\beta_1 x}+\overline{\alpha_2+\beta_2 x}=\overline{(\alpha_1+\alpha_2)+(\beta_1+\beta_2)x}$$

乘法运算类似，但是需要将相乘结果除以 x^2+1 并取余式，因此有

$$\overline{\alpha_1+\beta_1 x}\cdot\overline{\alpha_2+\beta_2 x}=\overline{\alpha_1\alpha_2+(\alpha_1\beta_2+\alpha_2\beta_1)x+\beta_1\beta_2 x^2}=\overline{(\alpha_1\alpha_2-\beta_1\beta_2)+(\alpha_1\beta_2+\alpha_2\beta_1)x}$$

注意除以 x^2+1 相当于用 -1 来替代 x^2，因为在商环 $\mathrm{F}[x]/(x^2+1)$ 中，需要将 x^2+1 视为 0。若令 $\mathrm{F}=¡$，则 $¡[x]/(x^2+1)$ 就是复数域£。

当F是有限域时，可以利用命题 1.11 来计算多项式商环中元素的数量。

推论 1.1 设 F_p 是有限域，非零多项式 $\boldsymbol{m}\in \mathrm{F}_p[x]$，其次数 $d\geqslant 1$。则商环 $\mathrm{F}_p[x]/(\boldsymbol{m})$ 包含 p^d 个元素。

证明 由命题 1.12 可知，$\mathrm{F}_p[x]/(\boldsymbol{m})$ 中每个元素可以唯一表示成

$$a_0+a_1 x+a_2 x^2+\cdots+a_{d-1}x^{d-1},\ a_0,a_1,\cdots,a_{d-1}\in \mathrm{F}_p$$

则每个 a_i 的值都有 p 种选择，故 $a_0,a_1,\cdots,a_{d-1}$ 共有 p^d 种选择。

证毕

下面给出多项式商环中单位的一个重要性质。

命题 1.13 设 F 是域，多项式 $\boldsymbol{a},\boldsymbol{m}\in \mathrm{F}[x]$ 且 $\boldsymbol{m}\neq 0$。当且仅当 $\gcd(\boldsymbol{a},\boldsymbol{m})=1$ 时，$\overline{\boldsymbol{a}}$ 是商环 $\mathrm{F}[x]/(\boldsymbol{m})$ 中的一个单位。

证明

必要性：设 $\overline{\boldsymbol{a}}$ 是 $\mathrm{F}[x]/(\boldsymbol{m})$ 中的一个单位。由定义可知，存在 $\overline{\boldsymbol{b}}\in \mathrm{F}[x]/(\boldsymbol{m})$ 使得 $\overline{\boldsymbol{a}}\times\overline{\boldsymbol{b}}=\overline{1}$。用模来表示即 $\boldsymbol{a}\cdot\boldsymbol{b}\equiv 1(\bmod \boldsymbol{m})$，则存在 $\boldsymbol{c}\in \mathrm{F}[x]$，使得 $\boldsymbol{a}\cdot\boldsymbol{b}-1=\boldsymbol{c}\cdot\boldsymbol{m}$。故 $\boldsymbol{a}$ 和 $\boldsymbol{m}$ 的公因式一定能够整除 1，即 $\gcd(\boldsymbol{a},\boldsymbol{m})=1$。

充分性:设 $\gcd(\boldsymbol{a},\boldsymbol{m})=1$。由命题 1.10 可知存在 $\boldsymbol{u},\boldsymbol{v}\in \mathrm{F}[x]$,满足 $\boldsymbol{a}\cdot\boldsymbol{u}+\boldsymbol{m}\cdot\boldsymbol{v}=1$。两端分别模 $\boldsymbol{m}$ 得 $\boldsymbol{a}\cdot\boldsymbol{u}\equiv 1(\mathrm{mod}\boldsymbol{m})$。故 $\bar{\boldsymbol{u}}$ 是 $\bar{\boldsymbol{a}}$ 在 $\mathrm{F}[x]/(\boldsymbol{m})$中的乘法逆元。

证毕

命题 1.13 的一个重要情况是模为不可约多项式。

推论 1.2 设F 是域,不可约多项式 $\boldsymbol{m}\in \mathrm{F}[x]$,则商环$\mathrm{F}[x]/(\boldsymbol{m})$是域,即$\mathrm{F}[x]/(\boldsymbol{m})$中每个非零元都有乘法逆元。

证明 不妨假设 $\boldsymbol{m}$是首一多项式,$\bar{\boldsymbol{a}}\in \mathrm{F}[x]/(\boldsymbol{m})$。

分两种情况讨论:若 $\gcd(\boldsymbol{a},\boldsymbol{m})=1$,由命题 1.13 可知 $\bar{\boldsymbol{a}}$是单位,故存在乘法逆元。

若 $\gcd(\boldsymbol{a},\boldsymbol{m})=\boldsymbol{d}\neq 1$,则 $\boldsymbol{d}\mid\boldsymbol{m}$。但 $\boldsymbol{m}$是不可约的首一多项式且 $\boldsymbol{d}\neq 1$,则 $\boldsymbol{d}=\boldsymbol{m}$,所以 $\boldsymbol{m}\mid\boldsymbol{a}$,即 $\bar{\boldsymbol{a}}=0$。

证毕

例 1.12 多项式 x^2+1 在¡[x]中不可约,则商环¡[x]/(x^2+1)是域。事实上,¡[x]/(x^2+1)就是复数域£。因为$(\bar{x})^2=-1$,故 $\bar{x}$ 相当于 $i=\sqrt{-1}$。

另外,x^2-1 显然在¡[x]中可约,所以¡[x]/(x^2-1)不是域。因为$\overline{(x-1)}\cdot\overline{(x+1)}=0$,故在¡[x]/($x^2-1$)中存在非零元的乘积是零,这意味着它们不是单位。(环中乘积为零的非零元称为零因子。)

若将推论 1.2 应用于系数取自有限域F_p的多项式环,可以构造出具有素数个元素的有限域。

推论 1.3 设F_p是有限域,不可约项式 $\boldsymbol{m}\in \mathrm{F}_p[x]$,其次数 $d\geqslant 1$,则商环$\mathrm{F}_p[x]/(\boldsymbol{m})$包含 p^d 个元素。

证明 推论 1.2 说明$\mathrm{F}_p[x]/(\boldsymbol{m})$是域,推论 1.1 说明$\mathrm{F}_p[x]/(\boldsymbol{m})$包含 p^d 个元素。

证毕

例 1.13 x^3+x+1 在$\mathrm{F}_2[x]$中不可约,故$\mathrm{F}_2[x]/(x^3+x+1)$包含 8 个元素。由命题 1.12 可知这 8 个代表元为

$$0,1,x,1+x,x^2,1+x^2,x+x^2,1+x+x^2$$

加法是系数模 2 的加法,如

$$(1+x)+(x+x^2)=1+x^2$$

乘法将结果除以 x^3+x+1 取余式即可,如

$$(1+x)\cdot(x+x^2)=x+2x^2+x^3=1$$

故 $1+x$ 和 $x+x^2$ 互为乘法逆元。

为了构造包含 p^d 个元素的有限域,需要在$\mathrm{F}_p[x]$中寻找一个次数为 d 的不可约多项式。在纯抽象代数意义上,这样的不可约多项式可以随意选取,只要满足