

# 信道编码

刘玉君 编著

河南科学技术出版社

# 前 言

信道编码是本世纪40年代末提出、60年代发展起来的一门提高数据传输可靠性的理论与技术，至今已有40余年的历史。随着数字通信的发展，特别是70年代以来，随着卫星通信和高速数据网的飞速发展，对数据传输的可靠性提出了越来越高的要求，因此，如何提高数据传输的可靠性已成为一个迫切需要解决的问题。

在有扰信道上传输数字数据时，所收到的数据将不可避免地含有差错。通常，用户提出一个差错率，当超出此差错率时，接收数据即不予使用。若采用信道编码技术，则可将差错减少到容许的限度以内。因此说，信道编码是用来改善数字通信可靠性的一种信号处理技术。

代数理论为信道编码提供了理论基础，大规模集成电路和微型计算机的发展为信道编码技术的应用开拓了广阔的前景，我们将会看到，随着我国四化建设的飞速发展，信道编码技术将得到更加广泛的应用。

本书是在笔者所编的《信道编码分析》和《信道编码》两套教材的基础上，经过多年试用修改并加进了笔者近年来的研究成果编写而成的。全书共分九章，包括以下内容：

第一、二两章分别介绍了学习“信道编码”所需要的数学知识和信道编码理论中的一些基本概念。

线性分组码是信道编码中最基本的一类码，它有明显的数学结构，是讨论各类码的基础，因此我们首先在第三章中介绍了线性分组码，并讨论了三个基本码限和两类基本线性分组码——汉明码和RM码。

为了使编、译码手续更为简单，多年来人们一直致力于分组码的研究，希望找到一种编、译码较易实现的分组码，而循环码就是这样的码。因此，我们在第四章介绍了循环码的基本理论及其编、译码实现电路。

BCH码是一类纠多个随机错误的循环码，它纠错能力强，构造方便，编码简单，译码也较易实现，在编码理论中起着重要作用。因此我们在第五章对BCH码作了较为详细的论述，对主要的译码算法的原理和实现方法以及改进意见进行了深入的讨论，并对RS码的频域编、译码方法作了简单介绍。

1954年里德(Reed)在译RM码时首先提出了大数逻辑译码的思想，以后许多编码工作者推广并发展了这一算法。1963年梅西(Massey)首先把大数逻辑译码算法予以系统化，并提出了软判决的大数逻辑译码。因此，我们在第六章中对循环码的大数逻辑译码作了系统的介绍。

卷积码是区别于分组码的又一种新型信道编码，它广泛应用于卫星通信中，从性能上讲优于一般的分组码。因此，我们在第七章中详细论述了卷积码的有关概念，对卷积码的代数译码和维特比译码算法进行了较为深入的讨论，并对非系统卷积码的译码恢复问题进行了系统研究。

许多实际信道中所产生的错误大部分是突发性的，或是突发错误与随机错误并存的。针对这类信道，需要设计专门用来纠突发错误的码类。因此，我们在第八章着重讨论了针对突发错误的编码技术，其中包括各种交错技术，如矩阵交错、卷积交错以及伪随机交错等。

实际数字通信系统的设计通常都受待传送的数据序列统计特性的影响，为了改善数据序列的统计特性，需要调制前的预编码，这就构成了数字通信系统设计中的一种专门技术——扰乱技术。本书最后一章首先介绍了与扰乱技术有关的线性移位寄存器和 $m$ 序列理论，然后对几种主要扰乱器作了详细讨论。扰乱技术已用于PCM数字通信和保密通信中，所以介绍这方面的有关内容对于读者拓宽知识面和理论联系实际都是有益的。

笔者由衷地感谢窦瑞华、聂涛、党明瑞等教授以及我院、系、教研室、教保处的领导和同志们对本书的写作和出版所给予的支持、鼓励和帮助。特别是窦瑞华教授在百忙中认真审阅了初稿全文，改正了其中一些错误，并提出了许多具体的修改意见，笔者再次表示深切谢意。在本书写作和定稿过程中，我院宋惠元副教授以及左金明、张水莲等同志审阅了全部或部分章节初稿，提出了许多宝贵意见，在此一并致谢。

由于笔者水平有限，书中缺点在所难免，敬请广大读者批评指正。

**刘玉君**

1992年5月于解放军信息工程学院

# 目 录

第一章 数学预备知识 .....	(1)
1.1 整数的可除性 .....	(1)
1.1.1 整除的概念 .....	(1)
1.1.2 最大公因数和最小公倍数 .....	(1)
1.1.3 欧几里德算法 .....	(2)
1.2 同余式和欧拉-费尔马定理 .....	(3)
1.2.1 整数按模运算 .....	(3)
1.2.2 同余式 .....	(3)
1.2.3 模 $n$ 剩余系和剩余缩系 .....	(4)
1.2.4 欧拉-费尔马定理 .....	(4)
1.3 群 .....	(4)
1.3.1 群的概念 .....	(4)
1.3.2 有限群 .....	(5)
1.3.3 循环群 .....	(5)
1.4 域 .....	(6)
1.4.1 域的概念 .....	(6)
1.4.2 域的性质 .....	(7)
1.4.3 域的同构 .....	(7)
1.4.4 域的特征和素域 .....	(8)
1.5 交换环 .....	(9)
1.5.1 交换环的概念 .....	(9)
1.5.2 理想的观念 .....	(10)
习 题 .....	(10)
参考文献 .....	(10)
第二章 数字通信与信道编码 .....	(11)
2.1 差错控制与信道编码 .....	(11)
2.1.1 信道编码的基本思想 .....	(11)
2.1.2 突发错误和随机错误 .....	(13)
2.1.3 差错控制的基本方式 .....	(13)
2.1.4 信道编码的分类 .....	(14)
2.2 信道模型和译码 .....	(15)
2.2.1 信道模型 .....	(15)
2.2.2 纠错译码 .....	(16)

2.2.3	最大似然译码	(16)
2.2.4	最小距离译码	(17)
2.2.5	分组码的检、纠错能力	(18)
2.3	常用检错码	(20)
2.3.1	奇偶监督码	(20)
2.3.2	水平一致监督码	(21)
2.3.3	水平垂直一致监督码	(21)
2.3.4	群计数码	(22)
2.3.5	水平群计数码	(22)
2.3.6	等比码	(23)
	习 题	(23)
	参考文献	(24)
第三章	线性分组码	(25)
3.1	线性分组码的基本概念	(25)
3.1.1	线性分组码的生成	(25)
3.1.2	$(n, k)$ 线性分组码的一致监督矩阵	(27)
3.2	线性分组码的数学描述	(29)
3.2.1	线性分组码的代数结构	(29)
3.2.2	等价码	(30)
3.2.3	零化空间和对偶码	(30)
3.2.4	线性分组码的主要性质	(31)
3.3	线性分组码的译码	(31)
3.3.1	监督矩阵与最小距离的关系	(31)
3.3.2	标准阵列译码表	(32)
3.3.3	伴随式纠错译码	(33)
3.4	纠错能力与码限	(36)
3.4.1	辛格尔顿 (Singleton) 限	(36)
3.4.2	普洛特金 (Plotkin) 限	(36)
3.4.3	汉明 (Hamming) 限	(37)
3.5	汉明码及扩展汉明码	(38)
3.5.1	汉明码的构造	(38)
3.5.2	扩展汉明码	(40)
3.6	由已知码构造新码	(41)
3.6.1	对偶码	(41)
3.6.2	扩展码	(42)
3.6.3	删余码	(42)
3.6.4	增信删余码	(42)
3.6.5	增余删信码	(43)
3.7	RM 码及里德译码算法的改进	(44)

3.7.1 RM 码的概念	(44)
3.7.2 RM 码的里德译码算法	(46)
3.7.3 里德译码算法的改进	(47)
3.7.4 小数逻辑译码	(48)
习 题	(50)
参考文献	(52)
<b>第四章 循环码</b>	<b>(53)</b>
4.1 $F_p[x]$ 中多项式的同余式	(53)
4.1.1 $F[x]$ 中的一元多项式	(53)
4.1.2 带余除法	(54)
4.1.3 多项式的同余式	(54)
4.1.4 $F_p[x] \bmod f(x)$ 的同余类环	(55)
4.2 循环码的数学描述	(56)
4.2.1 循环码的基本概念	(56)
4.2.2 循环码的多项式表示	(57)
4.2.3 循环码与理想	(58)
4.3 循环码的矩阵描述和对偶码	(61)
4.3.1 循环码的生成矩阵	(61)
4.3.2 循环码的监督矩阵	(62)
4.3.3 对偶码	(64)
4.4 由生成多项式的根定义循环码	(64)
4.4.1 欧拉-费尔马定理的推广	(64)
4.4.2 多项式的周期	(65)
4.4.3 本原多项式	(66)
4.4.4 同余类域和极小多项式	(68)
4.4.5 由生成多项式的根定义循环码	(69)
4.5 平方剩余码	(73)
4.5.1 平方剩余的概念	(74)
4.5.2 平方剩余码	(74)
4.6 多项式的乘除运算电路	(76)
4.6.1 乘法电路	(76)
4.6.2 除法电路	(77)
4.6.3 乘除电路	(78)
4.7 循环码的编码电路	(78)
4.7.1 $r$ 级编码电路	(78)
4.7.2 $k$ 级编码电路	(80)
4.8 循环码的译码电路	(81)
4.8.1 伴随式计算电路	(81)
4.8.2 错误图样检测器	(82)

4.8.3 梅吉特 (Meggitt) 译码器的设计 .....	(83)
4.9 缩短循环码 .....	(86)
4.9.1 缩短循环码的代数结构 .....	(86)
4.9.2 缩短循环码的生成矩阵和监督矩阵 .....	(87)
4.9.3 缩短循环码的编码和译码电路 .....	(87)
4.10 循环码的性质及其应用 .....	(88)
4.10.1 循环码的主要性质 .....	(88)
4.10.2 循环码性质的应用 .....	(89)
习 题 .....	(90)
参考文献 .....	(91)
<b>第五章 BCH 码</b> .....	(92)
5.1 BCH 码的基本概念 .....	(92)
5.1.1 BCH 码的定义 .....	(92)
5.1.2 BCH 码的进一步讨论 .....	(93)
5.1.3 BCH 码的扩展 .....	(94)
5.2 BCH 码的纠错能力 .....	(95)
5.3 RS 码 .....	(99)
5.3.1 RS 码的基本概念 .....	(99)
5.3.2 非系统 RS 码的编码 .....	(100)
5.3.3 RS 码的扩展 .....	(101)
5.3.4 系统 RS 码的编码电路 .....	(102)
5.4 彼得森 (Peterson) 译码算法 .....	(104)
5.4.1 彼得森译码原理 .....	(104)
5.4.2 彼得森译码算法的计算机实现 .....	(108)
5.5 BCH 码译码电路的设计 .....	(110)
5.5.1 计算伴随式的电路设计 .....	(110)
5.5.2 求错位多项式 $\sigma(x)$ 的根的电路设计 .....	(110)
5.6 BCH 码迭代译码原理 .....	(112)
5.6.1 关键方程的建立 .....	(112)
5.6.2 迭代算法 .....	(113)
5.6.3 迭代算法的计算机实现 .....	(117)
5.7 快速迭代译码 .....	(119)
5.7.1 二元 BCH 码迭代译码算法的简化 .....	(119)
5.7.2 BCH 码的快速迭代译码 .....	(120)
5.8 快速迭代译码的进一步改进 .....	(122)
5.9 错误值计算和福尼 (Forney) 算法 .....	(126)
5.9.1 福尼算法 .....	(126)
5.9.2 福尼算法的简化 .....	(127)
5.10 欧几里德译码算法 .....	(128)

5.10.1	欧几里德译码算法原理	(128)
5.10.2	欧几里德算法的计算机实现和性能比较	(131)
5.11	RS 码的变换编码和译码	(132)
5.11.1	MS 多项式和有限域上的傅氏变换	(132)
5.11.2	RS 码的变换编码	(134)
5.11.3	RS 码的变换译码	(136)
	习 题	(138)
	参考文献	(139)
<b>第六章 循环码的大数逻辑译码</b>		(140)
6.1	一步大数逻辑译码	(140)
6.1.1	大数逻辑译码的基本原理	(140)
6.1.2	一步大数逻辑译码的纠错能力	(141)
6.2	一步大数逻辑译码电路	(142)
6.2.1	I 型大数逻辑译码器	(143)
6.2.2	II 型大数逻辑译码器	(144)
6.3	某些一步大数逻辑可译码	(145)
6.3.1	极长码	(145)
6.3.2	差集循环码	(147)
6.4	L 步大数逻辑译码	(150)
6.4.1	L 步大数逻辑译码的概念	(150)
6.4.2	L 步大数逻辑译码电路的设计	(152)
6.5	欧氏几何码	(155)
6.5.1	欧氏几何的基本概念	(155)
6.5.2	欧氏几何码	(156)
6.5.3	欧氏几何码译码和 SCR 译码电路	(159)
6.6	APP 门限译码	(161)
6.6.1	离散无记忆信道 (DMC) 和距离函数	(162)
6.6.2	APP 门限译码	(164)
6.6.3	APP 门限译码器的实现	(167)
6.6.4	L 步 APP 门限译码	(167)
	习 题	(170)
	参考文献	(171)
<b>第七章 卷积码</b>		(172)
7.1	$(n_0, 1, m)$ 卷积码的概念	(172)
7.1.1	卷积码的一般概念	(172)
7.1.2	$(n_0, 1, m)$ 系统码的矩阵描述	(173)
7.2	$(n_0, 1, m)$ 卷积码的多项式表示	(176)
7.2.1	子生成多项式和生成多项式矩阵	(176)
7.2.2	卷积码的生成多项式	(177)



7.3	$(n_0, k_0, m)$ 卷积码	(178)
7.3.1	$(n_0, k_0, m)$ 卷积码的矩阵描述	(178)
7.3.2	$(n_0, k_0, m)$ 卷积码的多项式表示	(182)
7.3.3	$(n_0, k_0, m)$ 系统卷积码	(182)
7.4	不变因子分解定理与监督矩阵	(184)
7.4.1	系统码的监督矩阵	(184)
7.4.2	非系统卷积码的监督矩阵	(187)
7.4.3	不变因子分解定理和监督多项式矩阵	(188)
7.5	$(n_0, k_0, m)$ 卷积码的编码电路	(190)
7.6	卷积码的译码	(192)
7.6.1	伴随式计算与实现电路	(192)
7.6.2	反馈译码电路的设计	(193)
7.7	卷积码的距离特性和纠错能力	(196)
7.7.1	初始截短码	(196)
7.7.2	距离特性和纠错能力	(198)
7.8	卷积码的大数逻辑译码	(200)
7.8.1	自正交码	(201)
7.8.2	可正交码	(203)
7.8.3	卷积码的软判决大数逻辑译码	(207)
7.9	卷积码的定译码	(212)
7.9.1	误差传播	(212)
7.9.2	定译码	(214)
7.10	怀纳-阿什 (WA) 纠一个错误卷积码	(215)
7.11	非系统卷积码的大数逻辑译码	(217)
7.11.1	伴随式计算和大数逻辑译码	(217)
7.11.2	$(n_0, 1, m)$ 卷积码的译码恢复电路	(219)
7.11.3	$(n_0, k_0, m)$ 卷积码的译码恢复电路	(221)
7.11.4	不变因子分解定理与译码恢复电路	(222)
7.12	卷积码的树图描述和栅格图	(223)
7.12.1	卷积码的树图描述	(223)
7.12.2	状态图与栅格图	(225)
7.13	卷积码的维特比译码	(227)
7.13.1	维特比译码算法的基本原理	(227)
7.13.2	维特比译码算法的修改	(230)
7.13.3	软判决的维特比译码	(231)
7.13.4	BSC 中维特比译码算法的性能和所适用的码	(233)
7.14	删除卷积码	(238)
	习 题	(241)
	参考文献	(242)

第八章 纠突发错误码 .....	(243)
8.1 循环码的纠突发错误能力 .....	(243)
8.2 几类纠突发错误码 .....	(246)
8.2.1 艾布拉姆森码和法尔码 .....	(246)
8.2.2 巴顿码的构造 .....	(247)
8.2.3 RS 码的纠突发错误性能 .....	(248)
8.3 循环码的捕错译码 .....	(248)
8.3.1 捕错译码的一般原理 .....	(249)
8.3.2 纠单个突发错误码的捕错译码 .....	(252)
8.4 循环码的矩阵交错编码 .....	(255)
8.4.1 矩阵交错编码的原理 .....	(255)
8.4.2 矩阵交错码的编、译码电路 .....	(257)
8.5 分组码的卷积交错编码 .....	(257)
8.5.1 交错次数 $m = pn + 1$ 的卷积交错编码 .....	(257)
8.5.2 交错次数 $m = pn - 1$ 的卷积交错编码 .....	(259)
8.5.3 交错次数 $m$ 与码长 $n$ 互素的卷积交错编码 .....	(261)
8.6 乘积码 .....	(263)
8.6.1 乘积码及其纠错能力 .....	(263)
8.6.2 循环乘积码 .....	(264)
8.7 级连码 .....	(265)
8.8 伪随机交错编码 .....	(267)
8.8.1 线性同余序列交错编码 .....	(267)
8.8.2 伪随机序列交错编码 .....	(269)
8.9 纠突发错误卷积码 .....	(272)
8.9.1 基本概念 .....	(272)
8.9.2 岩垂 (Iwadare) 码 .....	(274)
8.10 扩散卷积码 .....	(276)
8.10.1 自正交扩散卷积码 .....	(276)
8.10.2 可正交扩散卷积码 .....	(278)
8.11 卷积码的交错编码 .....	(279)
8.11.1 卷积码的矩阵交错 .....	(279)
8.11.2 卷积码的卷积交错 .....	(280)
习 题 .....	(284)
参考文献 .....	(284)
第九章 数字数据扰乱器 .....	(285)
9.1 线性移位寄存器序列的数学描述 .....	(285)
9.1.1 线性移位寄存器序列与递推关系式 .....	(285)
9.1.2 生成函数与生成多项式 .....	(288)
9.1.3 状态转移矩阵和特征多项式 .....	(289)

9.2	线性移位寄存器序列的周期性	(290)
9.3	$G(f)$ 中的平移等价类	(294)
9.4	$m$ 序列及其伪随机性	(296)
9.4.1	$m$ 序列的定义	(296)
9.4.2	$m$ 序列的伪随机性	(297)
9.5	$m$ 序列的移加特性和抽样特性	(300)
9.5.1	$m$ 序列的移加特性	(300)
9.5.2	$m$ 序列的抽样特性	(303)
9.6	线性移位寄存器的综合	(305)
9.6.1	解方程组法	(305)
9.6.2	迭代算法	(306)
9.7	伪随机扰乱器	(308)
9.8	自同步扰乱器	(311)
9.8.1	自同步扰乱器的基本原理	(311)
9.8.2	循环输入扰乱器的线性变换矩阵	(314)
9.8.3	自同步扰乱器的临界状态	(316)
9.8.4	带有特殊循环输入的扰乱器	(317)
9.9	自同步式伪随机扰乱器	(319)
9.10	扰乱器的主要特性	(321)
	习 题	(322)
	参考文献	(323)
附录	英汉信道编码词汇	(324)

# 第一章 数学预备知识

信道编码理论与代数学有着密切的关系。多项式、向量、矩阵运算以及近世代数的有关理论等是研究信道编码必不可少的数学工具。鉴于这些数学知识在有关教科书中都有详尽论述，这里仅对本书常用到的一些重要数学概念给以简要介绍，许多严格证明都已略去。

## 1.1 整数的可除性

### 1.1.1 整除的概念

我们把  $1, 2, 3, \dots, n, \dots$  称为自然数，并用  $N$  表示自然数全体所成的集合，即

$$N = \{1, 2, \dots, n, \dots\}.$$

自然数、负整数的全体与零所成的集合称为整数集合，并用  $Z$  表示，即

$$Z = \{\dots, -n, \dots, -2, -1, 0, 1, 2, \dots, n, \dots\}.$$

在整数集合  $Z$  中可以作加、减和乘法等运算，但除法不总是可以进行的，因为任意两个整数作除法，结果可能不再是整数。

**定义 1.1** 整数集合  $Z$  中任意两个数  $a$  和  $b$ ，如果存在一个  $q \in Z$ ，使得  $a = bq$ ，则称  $b$  整除  $a$ ，记为  $b \mid a$ 。否则称  $b$  不能整除  $a$ 。若  $b \mid a$ ，也称  $b$  是  $a$  的因数，或  $a$  是  $b$  的倍数。

既然除法运算在整数集合中不总是可以进行的，那么用整数集合  $Z$  中一个非零整数去除  $Z$  中任一整数，就有除得尽与除不尽两种可能。下面定理给出了用  $b$  去除  $Z$  中任一整数  $a$  所得的结果，这就是带余除法定理。

**定理 1.1** 设  $a, b$  是整数集合  $Z$  中任意两个数，且  $b \neq 0$ ，则一定存在唯一的两个整数  $q$  和  $r$ ，使得

$$a = bq + r, \quad 0 \leq r < |b|. \quad (1.1.1)$$

### 1.1.2 最大公因数和最小公倍数

若  $b \mid a$ ，则  $-b \mid a$  及  $b \mid (-a)$ ，因此我们只讨论正整数和零的正因数和正倍数。

**定义 1.2** 若  $d$  是  $a$  的因数，又是  $b$  的因数，则称  $d$  是  $a$  与  $b$  的公因数。若  $m$  是  $a$  的倍数，又是  $b$  的倍数，则称  $m$  为  $a$  与  $b$  的公倍数。

一般地， $a$  与  $b$  的公因数不是唯一的，它有有限多个。当然这些公因数中一定有一个最大的。然而，两个数的公倍数有无限多个，因而  $a$  与  $b$  的公倍数中一定有一个最小的。

**定义 1.3** 设  $a$  与  $b$  不全为零，如果有一个  $d$  满足

$$1^\circ d \mid a, d \mid b;$$

$$2^\circ \text{若 } e \text{ 是 } a \text{ 与 } b \text{ 的任一公因数，则有 } e \mid d;$$

那么就称  $d$  是  $a$  与  $b$  的最大公因数，记为  $d = (a, b)$ ，或者  $d = \text{GCD}(a, b)$ 。

**定义 1.4** 设  $a$  与  $b$  不全为零，如果  $a$  与  $b$  的一个公倍数有如下性质： $a$  与  $b$  的任一公倍

数都是 $m$ 的倍数, 则 $m$ 称为 $a$ 与 $b$ 的最小公倍数, 记为 $m=[a, b]$ , 或者 $m=\text{LCM}(a, b)$ 。

最大公因数是我们今后经常用到的, 这里我们列举有关它的一些简单性质。

1°  $d \mid a$  与  $d \mid b$  的充分必要条件是  $d \mid (a, b)$ ;

2°  $(a, b)=d$  的充分必要条件是  $(\frac{a}{d}, \frac{b}{d})=1$ ;

3° 如果  $d=(a, b)$ , 则一定存在一对整数  $u, v$  使得  $ua+vb=d$ , 而且还可以进一步要求  $u, v$  适合条件:  $0 \leq u < b/d, 0 \leq |v| < a/d$ , 其中  $a$  与  $b$  均不为 0,  $a \neq b$ . 且适合上述条件的  $u$  和  $v$  是唯一的。

**定义 1.5** 如果一个大于 1 的整数  $a$ , 除了 1 和它本身以外没有其它因数, 则  $a$  称为素数或质数。大于 1 不是素数的数称为合数。

**定义 1.6** 如果两个数  $a$  与  $b$  的最大公因数是 1, 即  $(a, b)=1$ , 则称  $a$  与  $b$  互素。

类似性质 3°, 我们有

4° 如果  $(a, b)=1$ , 则存在一对整数  $u$  和  $v$ , 使得  $ua+vb=1$ , 其中  $0 < u < b, 0 < |v| < a$ , 而且  $u$  与  $v$  是唯一确定的 ( $a \neq 0, b \neq 0$ , 且  $a, b$  不全为 1)。

5° 如果  $a \mid bc$ , 且  $(a, b)=1$ , 则  $a \mid c$ ;

6° 如果  $(a, c)=1, (b, c)=1$ , 则  $(ab, c)=1$ 。

### 1.1.3 欧几里德算法

求两个数的最大公因数的常用方法是辗转相除法。该算法是以下面定理为基础的。

**定理 1.2** 若  $a > b > 0$ , 且

$$a = bq + r, \quad 0 < r < b, \quad (1.1.2)$$

则  $(a, b) = (b, r)$ 。

根据这个定理可以把求两个较大数  $a$  与  $b$  的最大公因数的问题化成求两个较小数  $b$  与  $r$  的最大公因数的问题。由此得到辗转相除求最大公因数的方法, 即欧几里德算法。

**定理 1.3 (欧几里德算法)** 设  $a > b > 0$ ,

$$a = bq_1 + r_1, \quad 0 < r_1 < b;$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1;$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2;$$

.....

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2};$$

$$r_{n-2} = r_{n-1}q_n.$$

则  $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-2}, r_{n-1}) = (r_{n-1}, 0) = r_{n-1}$ 。这就是说, 最后一个余数就是要求的最大公因数。

求有限个数的最大公因数可以用连续求两个数的最大公因数的方法完成。具体办法是, 在求  $n$  个数的最大公因数时, 首先从它们当中随意挑出两个数, 求它们的最大公因数, 然后再求这个最大公因数与其它  $n-2$  个数的最大公因数, 这样就把求  $n$  个数的最大公因数的问题化成求  $n-1$  个数的最大公因数的问题, 如此反复作下去, 最后可求得  $n$  个数的最大公因数。

## 1.2 同余式和欧拉-费尔马定理

### 1.2.1 整数按模运算

设 $n$ 是任意给定的正整数,  $a$ 是一个整数, 用 $n$ 去除 $a$ 得到的商为 $q$ , 余数为 $r$ , 于是

$$a = nq + r, \quad 0 \leq r < n. \quad (1.2.1)$$

我们知道,  $q$ 和 $r$ 是由 $a$ 和 $n$ 唯一确定的。为此引进符号 $r = (a)_n$ , 表示 $a$ 除以 $n$ 的余数, 于是上式可以写成

$$a = nq + (a)_n. \quad (1.2.2)$$

设 $Z$ 是所有整数的集合。若 $a, b \in Z$ , 按下面规则定义 $a$ 与 $b$ 的和(记为 $a \oplus b$ )及 $a$ 与 $b$ 的积(记为 $a \odot b$ )为

$$a \oplus b = (a + b)_n, \quad a \odot b = (ab)_n. \quad (1.2.3)$$

我们把 $Z$ 中的加法 $\oplus$ 叫做模 $n$ 加法, 把乘法 $\odot$ 叫做模 $n$ 乘法。按此定义的运算, 显然有

$$0 \leq a \oplus b < n, \quad 0 \leq a \odot b < n.$$

下面给出整数按模运算的一些简单性质。

1° 设 $a_1, a_2$ 是给定的两个整数,  $n$ 是给定的正整数, 则 $(a_1)_n = (a_2)_n$ 的充分必要条件是  $n \mid (a_1 - a_2)$ 。

$$2^\circ (a_1 \pm a_2)_n = ((a_1)_n \pm (a_2)_n)_n, \quad (a_1 a_2)_n = ((a_1)_n (a_2)_n)_n.$$

$$3^\circ (a_1 + a_2 + \cdots + a_m)_n = ((a_1)_n + (a_2)_n + \cdots + (a_m)_n)_n.$$

### 1.2.2 同余式

**定义 1.7** 如果任意两个整数 $a$ 和 $b$ 被正整数 $n$ 除所得的余数相同, 我们就说 $a$ 与 $b$ 模 $n$ 同余, 记为

$$a \equiv b \pmod{n}, \quad (1.2.4)$$

否则, 我们说 $a$ 与 $b$ 模 $n$ 不同余。

下面给出两个判定 $a$ 和 $b$ 同余的定理。

**定理 1.4**  $a \equiv b \pmod{n}$  的充分必要条件是 $a$ 可以表成 $a = b + nt$ 。

**定理 1.5**  $a \equiv b \pmod{n}$  的充分必要条件是 $n \mid a - b$ 。

同余式和普通等式有许多相似的性质, 而且可以进行运算。下面将同余式的主要性质列举出来, 以便今后应用。

$$1^\circ \text{ 如果 } a \equiv b \pmod{n}, c \equiv d \pmod{n}, \text{ 则 } a + c \equiv b + d \pmod{n}, \quad ac \equiv bd \pmod{n}.$$

$$2^\circ \text{ 如果 } a \equiv b \pmod{n}, c \text{ 为任意整数, 则 } ac \equiv bc \pmod{n}.$$

$$3^\circ \text{ 如果 } a \equiv b \pmod{n}, b \equiv c \pmod{n}, \text{ 则 } a \equiv c \pmod{n}.$$

$$4^\circ \text{ 如果 } ac \equiv bc \pmod{n}, \text{ 且 } (c, n) = 1, \text{ 则 } a \equiv b \pmod{n}.$$

$$5^\circ \text{ 如果 } a \equiv b \pmod{n}, \text{ 则 } (a, n) = (b, n). \text{ 特别地, 当 } (a, n) = 1 \text{ 时有 } (b, n) = 1.$$

$$6^\circ \text{ 如果 } a \equiv b \pmod{n}, d \text{ 是 } a, b, n \text{ 的一个公因数, 则 } \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

$$7^\circ \text{ 如果 } a \equiv b \pmod{n}, \text{ 且 } n_1 \mid n, \text{ 则 } a \equiv b \pmod{n_1}.$$

$$8^\circ \text{ 如果 } a \equiv b \pmod{n}, \text{ 且 } n_1 \mid n, n_1 \mid a, \text{ 则 } n_1 \mid b.$$

### 1.2.3 模 $n$ 剩余系和剩余缩系

**定义 1.8** 如果有  $n$  个整数  $r_0, r_1, \dots, r_{n-1}$ , 任何两个都  $\text{mod } n$  不同余, 那么这  $n$  个数叫做  $\text{mod } n$  的一个剩余系, 每一个  $r_i$  叫做一个代表。

实际上, 所有整数集合  $Z$  中元素被  $n$  除所得的余数只可能是  $0, 1, 2, \dots, n-1$ , 因此一个  $\text{mod } n$  剩余系中只有  $n$  个两两不同的整数, 即一个  $\text{mod } n$  剩余系中只有  $n$  个代表。下面给出  $\text{mod } n$  剩余系的一个重要性质, 即如果  $(a, n) = 1$ , 则当  $x$  取遍  $\text{mod } n$  剩余系中  $n$  个值时,  $ax + b$  也取遍  $\text{mod } n$  剩余系中  $n$  个值。

**定义 1.9** 设  $r_0, r_1, \dots, r_{n-1}$  是  $\text{mod } n$  的一个剩余系, 从中挑出那些与  $n$  互素的全部代表, 记为  $r_{\alpha_1}, r_{\alpha_2}, \dots, r_{\alpha_m}$ , 它们叫做  $\text{mod } n$  的一个剩余缩系。

**例 1.1**  $0, 1, 2, \dots, 11$  是  $\text{mod } 12$  的一个剩余系, 而  $1, 5, 7, 11$  是  $\text{mod } 12$  的一个剩余缩系。

最后, 我们给出剩余缩系的两个性质。

1° 任何一个与  $n$  互素的整数  $a$  必和剩余缩系中一个且仅与其中一个代表  $\text{mod } n$  同余。

2° 如果  $(a, n) = 1$ , 当  $x$  取遍  $\text{mod } n$  剩余缩系的  $m$  个值时,  $ax$  也取遍  $\text{mod } n$  剩余缩系的  $m$  个值。

### 1.2.4 欧拉-费尔马定理

**定义 1.10** 设  $n$  为任意正整数, 下列  $n$  个数

$$0, 1, 2, \dots, n-1$$

中与  $n$  互素的个数记为  $\varphi(n)$ , 称为欧拉函数。

显然  $\varphi(n)$  就是  $\text{mod } n$  剩余缩系中代表的个数。当  $n$  是一个较大数时,  $\varphi(n)$  究竟等于多少呢? 下面定理给出了明确的结果。

**定理 1.6** 设  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ , 当  $i \neq j$  时,  $p_i \neq p_j$ ,  $p_i$  为素数,  $e_i \geq 1$ , ( $i = 1, 2, \dots, r$ ), 则

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right). \quad (1.2.5)$$

**定理 1.7(欧拉-费尔马定理)** 设  $n$  是大于 1 的整数, 对于任意整数  $a$ ,  $(a, n) = 1$ , 则

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \quad (1.2.6)$$

特别地, 当  $n = p$  为素数时,  $\varphi(n) = p - 1$ , 于是

$$a^p \equiv a \pmod{p}. \quad (1.2.7)$$

## 1.3 群

### 1.3.1 群的概念

设  $G$  是由一些元素组成的集合,  $a, b, \dots$  表示元素,  $a \in G$  表示  $a$  属于  $G$ ,  $\bar{a} \in G$  表示  $a$  不属于  $G$ 。

**定义 1.11** 如果集合  $G$  中任意两个元素按照一定的法则结合起来等于  $G$  中一个确定的元素, 那么这个结合法则称为集合  $G$  的一个运算。

**定义 1.12** 一个非空集合  $G$ , 对于一个称为乘法的运算“ $\cdot$ ”, 如果它满足以下条件:

1° 对于  $G$  中任意三个元素  $a, b, c$ , 结合律

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

成立;

2° 在 $G$ 中存在一个单位元素 $e$ , 对于 $G$ 中一切元素都有

$$e \cdot a = a \cdot e = a \quad ;$$

3° 对于 $G$ 中任意一个元素 $a$ , 在 $G$ 中都有一个称为 $a$ 的逆元的元素 $a^{-1}$ 存在, 满足

$$a^{-1} \cdot a = a \cdot a^{-1} = e \quad ;$$

那么 $G$ 对于乘法运算“ $\cdot$ ”来说构成一个群。

由以上两个定义可以看出, 要验证一个集合 $G$ 对于某一结合法则是否成群, 首先应验证这个结合法则是否是 $G$ 的一个运算, 然后还要验证它是否满足定义中的三个条件。

在一个群里, 由于结合律成立, 故 $a_1 \cdot a_2 \cdot \cdots \cdot a_n$ 是有意义的, 它是 $G$ 中某个元素, 当然也可以把 $G$ 中 $n$ 个相同的 $a$ 作乘法, 如果用普通乘法符号表示群的乘法运算, 这样 $n$ 个 $a$ 作乘法可以用 $a^n$ 表示。

**定义 1.13** 如果一个群 $G$ 还满足交换律, 即对于 $G$ 中任意两个元素 $a, b$ , 都有 $a \cdot b = b \cdot a$ , 则称 $G$ 为交换群。

**定义 1.14** 一个群 $G$ 的非空子集 $H$ , 对于 $G$ 中所定义的乘法运算也构成一个群, 则称 $H$ 为群 $G$ 的子群。

### 1.3.2 有限群

**定义 1.15** 若群 $G$ 中只含有限个元素, 则称 $G$ 为有限群, 否则称为无限群。一个有限群所含元素的个数叫做这个群的阶。

**定义 1.16**  $a$ 是群 $G$ 中任一个元素, 若对于任意整数 $n$ 都有 $a^n \neq e$ , 则称 $a$ 为无限阶元, 否则, 若有正整数 $n$ 使 $a^n = e$ 成立, 则称 $a$ 为有限阶元, 具有性质 $a^n = e$ 的最小正整数 $n$ 称为 $a$ 的阶。

我们今后经常遇到有限群, 因此下面列举有限群的一些性质。

1° 若 $G$ 是有限群, 则 $G$ 中每一个元都是有限阶元。

2° 若 $a$ 是 $n$ 阶元, 当且仅当 $n \mid m$ 时,  $a^m = e$ 。

3°  $a, b \in G$ ,  $G$ 是一个有限交换群,  $a$ 是 $m$ 阶元,  $b$ 是 $n$ 阶元, 且 $(m, n) = 1$ , 则 $a \cdot b$ 是 $m \cdot n$ 阶元。

4°  $G$ 是有限交换群,  $a$ 是 $G$ 的一个 $n$ 阶元,  $k$ 是任意正整数, 那么 $a^k$ 是 $\frac{n}{(k, n)}$ 阶元。

5° 设 $G$ 是有限交换群,  $n$ 阶元 $a$ 是 $G$ 中阶数最大的元, 那么 $G$ 中任一元的阶数均是 $n$ 的因数。

6° 设 $G$ 是有限交换群,  $a$ 是 $G$ 的一个 $n$ 阶元, 那么下面 $n$ 个元

$$a^0 = e, a, a^2, \cdots, a^{n-1}$$

是 $G$ 中 $n$ 个两两不同的元,  $a$ 的任意次幂皆在其中, 且 $[a] = \{e, a, a^2, \cdots, a^{n-1}\}$ 对于 $G$ 中的运算是一个 $n$ 阶交换群。

### 1.3.3 循环群

**定义 1.17** 若一个群 $G$ 的每一个元都是 $G$ 的某一个固定元 $a$ 的幂, 我们就称 $G$ 为循环群, 也说 $G$ 是由生成元 $a$ 生成的群, 记为 $G = \langle a \rangle$ 。

下面列举循环群的主要性质。



1° 若生成元 $a$ 是 $n$ 阶元, 则 $\langle a \rangle$ 是 $n$ 阶循环群.

2° 若 $G = \langle a \rangle$ 是 $n$ 阶循环群, 则 $a^k$ 是 $G$ 的一个生成元的充分必要条件是 $(k, n) = 1$ .

3°  $n$ 阶循环群 $G$ 有 $\varphi(n)$ 个生成元. 特别地, 当 $n$ 为素数时,  $G$ 有 $n-1$ 个生成元, 即 $G$ 中所有非单位元的元素都是 $G$ 的生成元.

4° 设 $G = \langle a \rangle$ 是一个 $n$ 阶循环群, 则 $G$ 的任一个子群 $H$ 也是一个循环群, 且 $H$ 中存在一个 $a$ 的最小正整数次幂 $a^m$ , 它生成 $H$ , 即 $H = \langle a^m \rangle$ , 且有 $m \mid n$ .

5° 如果 $G$ 是一个 $n$ 阶循环群, 则对于 $n$ 的任一个因子 $m$ ,  $a^m$ 生成一个循环子群 $H_m$ , 且 $H_m$ 是 $\frac{n}{m}$ 阶循环群.

## 1.4 域

### 1.4.1 域的概念

域是信道编码理论中另一个较为重要的概念, 它是具有两种运算的代数系统.

**定义 1.18** 设 $F$ 是一个非空集合,  $F$ 中规定两种运算, 一个叫做加法, 另一个叫做乘法, 如果满足下列条件:

1°  $F$ 对加法构成一个交换群;

2°  $F$ 中至少有一个非零元;

3°  $F$ 中非零元的全体 $F^*$ 对乘法构成一个交换的乘法群;

4° 乘法和加法有分配律,  $a(b+c) = ab+ac$ ;

则 $F$ 叫做一个域.

在编码理论中我们经常遇到的是包含有限个元素的域.

**定义 1.19** 如果一个域只包含有限个元, 则我们称它为有限域或伽罗华(Galois)域. 如果这个域含有 $q$ 个元, 则这个域简记为 $GF(q)$ .

从域的定义可以看出, 一个域至少含有两个元素, 即零元和单位元. 我们常用的正是这个最简单的域.

**例 1.2** 由 0 和 1 组成集合 $F_2 = \{0, 1\}$ ,  $F_2$ 上的加法和乘法用下列两个表给出:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

不难验证, 对于如上规定的加法和乘法 $F_2$ 是一个域, 我们把这个域记为 $GF(2)$ . 事实上,  $GF(2)$ 上的加法和乘法就是 mod2 加法和 mod2 乘法.

类似地, 任取一个素数 $p$ , 若

$$F_p = \{0, 1, 2, \dots, p-1\},$$

在 $F_p$ 上规定加法为 mod $p$ 加法, 乘法为 mod $p$ 乘法, 即如果 $a+b \equiv c \pmod{p}$ , 则规定 $a$ 与 $b$ 的和 $a+b=c$ ; 如果 $a \cdot b \equiv d \pmod{p}$ , 则规定 $a$ 与 $b$ 的积 $a \cdot b=d$ . 不难证明 $F_p$ 对于以上规定的加法和乘法是一个域.

**例 1.3**  $F_3 = \{0, 1, 2\}$ , 在 $F_3$ 上规定加法和乘法分别为 mod3 加法和乘法,  $p=3$ 是