



Figure 1
Micrographs of the
samples

Figure 1 shows the micrographs of the samples. The samples are labeled as follows: (a) 100% PCL, (b) 90% PCL/10% PEG, (c) 80% PCL/20% PEG, and (d) 70% PCL/30% PEG. The images show the morphology of the samples, which are characterized by a porous structure. The pores are interconnected and have a size that increases with the PEG content.

信道编码

(修订版)

刘玉君 编 著

河南科学技术出版社

内 容 提 要

本书比较详细地论述了信道编码理论和主要纠错码类的编、译码原理。内容包括:数学预备知识;线性分组码、循环码、BCH码和卷积码等主要纠错码类的编、译码原理,译码算法和实现方法;最后两章着重介绍纠突发错误编、译码技术和扰乱器。本书可作为高等院校通信、计算机等专业的高年级本科生、研究生教材和参考书,也可供从事通信与计算机等工作的技术人员参考。

信 道 编 码

(修 订 版)

刘玉君 编著

责任编辑 袁元

河南科学技术出版社出版发行

解放军信息工程大学印刷厂印刷

787×1092毫米 16开本 23印张 589千字

1992年6月第1版 2001年9月第2次印刷

印数:3001—5000册

ISBN 7-5349-1090-0/G·252

定 价:(精)59.80元

前 言

信道编码是二十世纪 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 50 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作了系统介绍,特别对 BCH 码的迭代译码原理及译码算法的改进进行了深入的讨论,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,并对软判决的大数逻辑译码,即 APP 算法作了推广工作,提出了 L 步 APP 门限译码算法。

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,并用不变因子分解定理,从理论上彻底解决了非系统卷积码中由生成多项式矩阵求解监督多项式矩阵的问题和非系统卷积码的译码恢复问题。

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,并对级连码、Turbo 码等与实际通信结合密切的重要码类作了简要介绍。

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较为详细地讨论。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。在本书这次修改重印过程中,北京理工大学安建平教授,对本书修改提出了许多建设性意见,我校宋惠元教授、张水莲副教授和刘建洲、巩克现、周山等同志分别对部分章节进行了认真校对,改正了其中许多错误,巩克现,赵仁才等同志为本书修改工作提供许多可靠数据,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

2001年9月

于解放军信息工程大学

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	2
1.1.3 欧几里德算法	3
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	4
1.2.3 模 n 剩余系和模 n 剩余缩系	4
1.2.4 欧拉函数及欧拉-费尔马定理	5
1.3 群的基本概念	7
1.3.1 群的定义	7
1.3.2 有限群及其性质	8
1.3.3 循环群及其性质	9
1.3.4 陪集的概念	11
1.4 域和域的同构	12
1.4.1 域的概念	12
1.4.2 域的性质	13
1.4.3 域的同构	14
1.4.4 域的特征和素域	15
1.5 交换环与理想	17
1.5.1 交换环的概念	17
1.5.2 子环与理想	18
1.6 $F_p[x]$ 中多项式	18
1.6.1 $F_p[x]$ 中一元多项式的运算	18
1.6.2 $F_p[x]$ 中多项式的最大公因式	19
1.6.3 $F_p[x]$ 中多项式的性质	23
1.7 欧拉-费尔马定理的推广	24
1.7.1 多项式的同余式	24
1.7.2 模 n 剩余系的推广	25
1.7.3 欧拉-费尔马定理的推广	25
1.8 多项式的周期和本原多项式	27
1.8.1 多项式的周期	27
1.8.2 本原多项式	30
1.9 $F_p[x] \bmod f(x)$ 的同余类环	31
1.9.1 $F_p[x] \bmod f(x)$ 的同余类环的概念	31
1.9.2 同余类环 $F_p[x]/(f(x))$ 的性质	32

1.10 有限域 $GF(p^n)$ 及极小多项式	34
1.10.1 $F_p[x] \bmod p(x)$ 的同余类域	34
1.10.2 有限域 $GF(2^n)$ 性质的进一步讨论	35
1.10.3 极小多项式	37
习 题	40
参考文献	42
第二章 数字通信与信道编码	43
2.1 差错控制与信道编码	43
2.1.1 信道编码的基本思想	43
2.1.2 突发错误和随机错误	44
2.1.3 差错控制的基本方式	45
2.1.4 信道编码的分类	45
2.2 信道模型和译码	47
2.2.1 信道模型	47
2.2.2 纠错译码	47
2.2.3 最大似然译码	48
2.2.4 最小距离译码	48
2.2.5 分组码的检、纠错能力	50
2.3 常用检错码	51
2.3.1 奇偶监督码	51
2.3.2 水平一致监督码	52
2.3.3 水平垂直一致监督码	52
2.3.4 群计数码	53
2.3.5 水平群计数码	53
2.3.6 等比码	54
2.3.7 交错监督码	54
2.3.8 二进制总计监督码	55
习 题	55
参考文献	56
第三章 线性分组码	57
3.1 线性分组码的基本概念	57
3.1.1 线性分组码的生成	57
3.1.2 (n, k) 线性分组码的一致监督矩阵	58
3.2 线性分组码的数学描述	61
3.2.1 线性分组码的代数结构	61
3.2.2 等价码	61
3.2.3 零化空间和对偶码	62
3.2.4 线性分组码的主要性质	62
3.3 线性分组码的译码	62
3.3.1 监督矩阵与最小距离的关系	62
3.3.2 标准阵列译码表	63
3.3.3 伴随式纠错译码	64
3.4 纠错能力与码限	66

3.4.1	辛格尔顿(Singleton)限	66
3.4.2	普洛特金(Plotkin)限	66
3.4.3	汉明(Hamming)限	67
3.5	汉明码及扩展汉明码	68
3.5.1	汉明码的构造	68
3.5.2	扩展汉明码	70
3.6	由已知码构造新码	71
3.6.1	对偶码	71
3.6.2	扩展码	71
3.6.3	删余码	72
3.6.4	增信删余码	72
3.6.5	增余删信码	73
3.7	RM 码及里德译码算法的改进	73
3.7.1	RM 码的概念	73
3.7.2	RM 码的里德译码算法	75
3.7.3	里德译码算法的改进	76
3.7.4	小数逻辑译码	77
	习 题	79
	参考文献	81
第四章	循环码	82
4.1	循环码的数学描述	82
4.1.1	循环码的基本概念	82
4.1.2	循环码的多项式表示	83
4.1.3	循环码与理想	83
4.2	循环码的矩阵描述和对偶码	86
4.2.1	循环码的生成矩阵	86
4.2.2	循环码的监督矩阵	88
4.2.3	对偶码	89
4.3	由生成多项式的根定义循环码	89
4.4	平方剩余码	93
4.4.1	平方剩余的概念	93
4.4.2	平方剩余码	94
4.5	多项式的乘除运算电路	95
4.5.1	乘法电路	95
4.5.2	除法电路	96
4.5.3	乘除电路	97
4.6	循环码的编码电路	98
4.6.1	r 级编码电路	98
4.6.2	k 级编码电路	99
4.7	循环码的译码电路	100
4.7.1	伴随式计算电路	100
4.7.2	错误图样检测器	102
4.7.3	梅吉特(Meggitt)译码器的设计	102

4.8	缩短循环码	105
4.8.1	缩短循环码的构成	105
4.8.2	缩短循环码的生成矩阵和监督矩阵	106
4.8.3	缩短循环码的编码和译码电路	106
4.9	循环冗余码	107
4.9.1	循环冗余码的编、译码原理	107
4.9.2	循环冗余码的检、纠错能力	108
4.10	循环码的性质及其应用	108
4.10.1	循环码的主要性质	108
4.10.2	循环码性质的应用	109
	习 题	110
	参考文献	111
第五章	BCH 码	112
5.1	BCH 码的基本概念	112
5.1.1	BCH 码的定义	112
5.1.2	BCH 码的进一步讨论	113
5.1.3	BCH 码的扩展	114
5.2	BCH 码的纠错能力	117
5.3	RS 码	118
5.3.1	RS 码的基本概念	118
5.3.2	非系统 RS 码的编码	119
5.3.3	RS 码的扩展	120
5.3.4	系统 RS 码的编码电路	121
5.4	彼得森(Peterson)译码算法	123
5.4.1	彼得森译码原理	123
5.4.2	彼得森译码算法的计算机实现	126
5.5	BCH 码译码电路的设计	127
5.5.1	计算伴随式的电路设计	127
5.5.2	求错位多项式 $\sigma(x)$ 根的电路设计	129
5.6	BCH 码迭代译码原理	130
5.6.1	牛顿公式	130
5.6.2	关键方程的建立	133
5.6.3	迭代算法	135
5.6.4	迭代算法的计算机实现	139
5.7	快速迭代译码	141
5.7.1	二元 BCH 码迭代译码算法的简化	141
5.7.2	BCH 码的快速迭代译码	141
5.8	快速迭代译码的进一步改进	143
5.9	错误值计算和福尼(Forney)算法	147
5.9.1	福尼算法	147
5.9.2	福尼算法的简化	148
5.10	欧几里德译码算法	149

5.10.1 欧几里德译码算法原理	149
5.10.2 欧几里德算法的计算机实现和性能比较	152
5.11 RS 码的变换编码和译码	153
5.11.1 MS 多项式和有限域上的傅氏变换	153
5.11.2 RS 码的变换编码	155
5.11.3 RS 码的变换译码	156
习 题	158
参考文献	159
第六章 循环码的大数逻辑译码	160
6.1 一步大数逻辑译码	160
6.1.1 大数逻辑译码的基本原理	160
6.1.2 一步大数逻辑译码的纠错能力	161
6.2 一步大数逻辑译码电路	162
6.2.1 I 型大数逻辑译码电路	162
6.2.2 II 型大数逻辑译码电路	164
6.3 某些一步大数逻辑可译码	165
6.3.1 极长码	165
6.3.2 差集循环码	166
6.4 L 步大数逻辑译码	169
6.4.1 L 步大数逻辑译码的概念	169
6.4.2 L 步大数逻辑译码电路的设计	171
6.5 欧氏几何码	174
6.5.1 欧氏几何的基本概念	174
6.5.2 欧氏几何码	175
6.5.3 欧氏几何码译码和 SCR 译码电路	178
6.6 APP 门限译码	180
6.6.1 离散无记忆信道(DMC)和距离函数	181
6.6.2 APP 门限译码	182
6.6.3 APP 门限译码的实现	185
6.6.4 L 步 APP 门限译码	187
习 题	188
参考文献	189
第七章 卷积码	190
7.1 $(n_0, 1, m)$ 卷积码的概念	190
7.1.1 卷积码的一般概念	190
7.1.2 $(n_0, 1, m)$ 卷积码的矩阵描述	191
7.2 $(n_0, 1, m)$ 卷积码的多项式表示	194
7.2.1 子生成多项式和生成多项式矩阵	194
7.2.2 卷积码的生成多项式	194
7.3 (n_0, k_0, m) 卷积码	195
7.3.1 (n_0, k_0, m) 卷积码的矩阵描述	195
7.3.2 (n_0, k_0, m) 卷积码的多项式表示	198

7.3.3	(n_0, k_0, m) 系统卷积码	199
7.4	不变因子分解定理与监督矩阵	200
7.4.1	系统码的监督矩阵	200
7.4.2	非系统卷积码的监督矩阵	203
7.4.3	不变因子分解定理和监督多项式矩阵	204
7.5	(n_0, k_0, m) 卷积码的编码电路	207
7.6	卷积码的译码	208
7.6.1	伴随式计算与实现电路	209
7.6.2	反馈译码电路的设计	210
7.7	卷积码的距离特性和纠错能力	213
7.7.1	初始截短码	213
7.7.2	距离特性和纠错能力	214
7.8	卷积码的大数逻辑译码	216
7.8.1	自正交码	216
7.8.2	可正交码	219
7.8.3	卷积码的软判决大数逻辑译码	222
7.9	卷积码的定译码	226
7.9.1	误差传播	226
7.9.2	定译码	228
7.10	怀纳—阿什(WA)纠一个错误卷积码	229
7.11	非系统卷积码的大数逻辑译码	231
7.11.1	伴随式计算和大数逻辑译码	231
7.11.2	$(n_0, 1, m)$ 卷积码的译码恢复电路	233
7.11.3	(n_0, k_0, m) 卷积码的译码恢复电路	235
7.11.4	不变因子分解定理与译码恢复电路	237
7.12	卷积码的树图描述和栅格图	238
7.12.1	卷积码的树图描述	238
7.12.2	状态图与栅格图	239
7.13	卷积码的维特比译码	241
7.13.1	维特比译码算法的基本原理	241
7.13.2	维特比译码算法的修改	244
7.13.3	软判决的维特比译码	245
7.13.4	BSC 中维特比译码算法的性能和适用的码	247
7.14	删除卷积码	252
	习 题	254
	参考文献	256
第八章	纠突发错误码	257
8.1	循环码的纠突发错误能力	257
8.2	几类纠突发错误码	259
8.2.1	艾布拉姆森码和法尔码	259
8.2.2	巴顿码的构造	260
8.2.3	RS 码的纠突发错误性能	262

8.3	循环码的捕错译码	262
8.3.1	捕错译码的一般原理	262
8.3.2	纠单个突发错误码的捕错译码	265
8.4	循环码的矩阵交错编码	267
8.4.1	矩阵交错编码的原理	268
8.4.2	矩阵交错码的编、译码电路	270
8.5	分组码的卷积交错编码	270
8.5.1	交错次数 $m = pn + 1$ 的卷积交错编码	270
8.5.2	交错次数 $m = pn - 1$ 的卷积码交错编码	273
8.5.3	交错交数 m 与码长 n 互素的卷积交错编码	274
8.6	乘积码	276
8.6.1	乘积码及其纠错能力	276
8.6.2	循环乘积码	277
8.7	级连码	278
8.8	伪随机交错编码	280
8.8.1	线性同余交错编码	280
8.8.2	伪随机交错编码	282
8.9	纠突发错误卷积码	285
8.9.1	基本概念	285
8.9.2	岩垂(Iwaware)码	286
8.10	扩散卷积码	288
8.10.1	自正交扩散卷积码	288
8.10.2	可正交扩散卷积码	290
8.11	卷积码的交错编码	291
8.11.1	卷积码的矩阵交错	291
8.11.2	卷积码的卷积交错	292
8.12	Turbo 码	296
8.12.1	Turbo 码的编码	296
8.12.2	Turob 码的译码	297
8.12.3	Turbo 码在实际通信系统中的应用	299
	习 题	299
	参考文献	300
第九章	数字数据扰乱器	301
9.1	线性移位寄存器序列的数学描述	301
9.1.1	线性移位寄存器序列与递推关系	301
9.1.2	生成函数与生成多项式	304
9.1.3	状态转移矩阵和特征多项式	305
9.2	线性移位寄存器序列的周期性	306
9.3	$G(f)$ 中的平移等价类	309
9.4	m 序列及其伪随机性	310
9.4.1	m 序列的定义	310
9.4.2	m 序列的伪随机性	311

9.5	m 序列的移加特性和抽样特性	314
9.5.1	m 序列的移加特性	314
9.5.2	m 序列的抽样特性	316
9.6	线性移位寄存器的综合	318
9.6.1	解方程组法	318
9.6.2	迭代算法	320
9.7	伪随机扰乱器	321
9.8	自同步扰乱器	324
9.8.1	自同步扰乱器的基本原理	324
9.8.2	循环输入扰乱器的线性变换矩阵	326
9.8.3	自同步扰乱器的临界状态	328
9.8.4	带有特殊循环输入的扰乱器	330
9.9	自同步式伪随机扰乱器	331
9.10	扰乱器的主要特性	333
	习 题	334
	参考文献	334
	部分习题参考答案	335
	附录 英汉信道编码词汇	345

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细论述, 这里仅对本书常用到的一些主要数学概念, 给以简要介绍.

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:

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

显然, 任意两个自然数的和与积仍然是自然数, 但两个自然数相减就不一定是自然数, 因为减法运算产生了零和负数. 通常我们把正整数、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 中可以做加、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 对于整数集合 Z 中任意两个数 a, b , 如果存在一个 $q \in Z$, 使得 $b = aq$, 则称 a 整除 b , 记为 $a|b$. 否则称 a 不能整除 b . 若 $a|b$, 也称 a 是 b 的因数, 或 b 是 a 的倍数.

下面列举有关整除的一些性质.

1° 如果 $a|b$, 则 $a|(-b)$, $-a|b$, $-a|(-b)$.

有了性质 1°, 我们今后只需考虑正整数和零的正因子和正倍数即可.

2° 如果 $a|b$ 及 $a|c$, 则 $a|mb+nc$, $m, n \in Z$.

该性质还可以推广到有限个的情况, 即

如果 $a|b_i, i=1, 2, \dots, n$, 则

$$a \mid \sum_{i=1}^n k_i b_i, \quad k_i \in Z, i = 1, 2, \dots, n.$$

3° 如果 $a|b, b|c$, 则 $a|c$.

4° 如果 $a|b$, 且 $b|a$, 则 $a=b$.

5° 如果 $a|b, c \neq 0$, 则 $ac|bc$.

6° 如果 $ac|bc$, 则 $a|b$.

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 中任一个整数, 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 中任一个数 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 $a \neq 0$, 则一定存在唯一的两个整数 q 和 r , 使得

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

1.1.2 最大公因数和最小公倍数

若 $a|b$, 则 $-a|b$, 及 $a|(-b)$, 因此我们只讨论正整数和零的正因数及正倍数.

定义 1.2 若 d 是 a 的因数, 又是 b 的因数, 则 d 称为 a 与 b 的公因数;

若 m 是 a 的倍数, 又是 b 的倍数, 则 m 称为 a 与 b 的公倍数.

一般情况下, 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, 因为若 m 是 a 与 b 的公倍数, 则 $2m, 3m, \dots$, 等都是 a 与 b 的公倍数, 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° $d|a, d|b$;

2° 若 e 是 a 与 b 的公因数, 则有 $e|d$.

我们就称 d 是 a 与 b 的最大公因数, 记为 $d=(a, b)$, 或者 $d=\text{GCD}(a, b)$.

最大公因数是今后经常用到的, 因此下面给出最大公因数的一些简单性质.

1° $d|a$ 与 $d|b$ 同时成立的充分必要条件是 $d|(a, b)$.

2° 设 $(a, b)=d$, 则 $(ka, kb)=kd$;

若 $k|a, k|b$, 则 $\left(\frac{a}{k}, \frac{b}{k}\right) = \frac{(a, b)}{k}$.

3° $(a, b)=d$ 的充分必要条件是 $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

4° 如果 $(a, b)=d$, 则一定存在一对整数 u, v , 使得

$$ua + vb = d, \quad (1.1.2)$$

而且还可以进一步要求 u, v 适合条件

$$0 \leq u < \frac{b}{d}, \quad 0 \leq |v| < \frac{a}{d}.$$

其中 $a \cdot b \neq 0, a \neq b$, 且适合上述条件的 u, v 是唯一的.

定义 1.4 设 a, b 不全为零, 如果 a, b 的一个公倍数 m 具有如下性质: a 与 b 的任何一个公倍数都是 m 的倍数, 则 m 叫做 a 与 b 的最小公倍数, 记为 $m=[a, b]$ 或 $m=\text{LCM}(a, b)$.

定义 1.5 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 是互素的.

类似性质 4°, 我们有

5° 如果 $(a, b)=1$, 则存在一对整数 u 和 v 使得

$$ua + vb = 1,$$

其中 $0 \leq u < b, 0 \leq |v| < a$ ($a \neq 0, b \neq 0$, 且 a, b 不全为 1), 而且 u, v 是唯一确定的.

6° 如果 $a|b \cdot c$, 且 $(a, b)=1$, 则 $a|c$.

7° 如果 $a|c, b|c$, 且 $(a, b)=1$, 则 $a \cdot b|c$.

8° 如果 $(a, c)=1, (b, c)=1$, 则 $(a \cdot b, c)=1$.

定义 1.6 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, 大于 1 不是素数的数叫做合数.

素数有以下性质:

1° 对于一个素数 p 和任一个整数 $a, p|a$ 或者 $(p, a)=1$, 两者必有且仅有一成立.

2° 如果一个素数 $p|a \cdot b$, 则 $p|a$ 或者 $p|b$.

定义 1.7 如果一个素数 $p|a$, 则 p 叫做 a 的素因子.

根据互素和素数的性质, 应用数学归纳法, 可以证明整数的基本定理, 即因子分解唯一性

定理,这就是定理 1.2.

定理 1.2 任何一个大于 1 的整数 a 可以分解成有限个素因子 p_1, p_2, \dots, p_r 的乘积

$$a = p_1 p_2 \cdots p_r,$$

且上述分解是唯一的,这就是说,如果还有一种分解

$$a = q_1 q_2 \cdots q_s,$$

其中 p_i 和 q_i 都是素数,则 $r=s$ 且将 q_i 的脚标作适当调换之后可使

$$q_1 = p_1, \quad q_2 = p_2, \quad \dots, \quad q_r = p_r.$$

最后,我们还可以得到两个整数 a 与 b 的最大公因数和最小公倍数之间的关系.

定理 1.3 设两个整数 a 与 b 的最大公因数和最小公倍数分别为 (a, b) 和 $[a, b]$, 则有

$$a \cdot b = (a, b) \cdot [a, b].$$

1.1.3 欧几里德算法

如何求两个数的最大公因数是我们今后经常遇到的问题. 求两个数的最大公因数的常用方法是辗转相除法,即欧几里德(Euclid)算法. 欧几里德算法是以下面定理为基础的.

定理 1.4 若 $a > b > 0$, 且

$$a = bq + r, \quad 0 < r < b, \quad (1.1.3)$$

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. 由此得到用辗转相除法求两个数的最大公因数的方法.

定理 1.5(Euclid) 设 $a > b > 0$, 那么

$$\left. \begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b; \\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1; \\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2; \\ &\dots\dots\dots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1}, & 0 < r_{n-1} < r_{n-2}; \\ r_{n-2} &= r_{n-1}q_n. \end{aligned} \right\} \quad (1.1.4)$$

则 $(a, b) = (b, r_1) = (r_1, r_2) = \dots = (r_{n-2}, r_{n-1}) = (r_{n-1}, 0) = r_{n-1}$.

该定理告诉我们,在对 a, b 作辗转相除时,最后一个余数 r_{n-1} 就是要求的最大公因数.

求有限多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来完成,具体办法是,在求 n 个数的最大公因数时,首先从它们当中任意挑出两个数,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 , 于是有

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

我们知道, q 和 r 是由 a 和 n 唯一确定的,为此引入符号 $(a)_n$, 它表示用 n 去除 a 所得的余数,因此(1.2.1)式可以写成

$$a = nq + (a)_n.$$