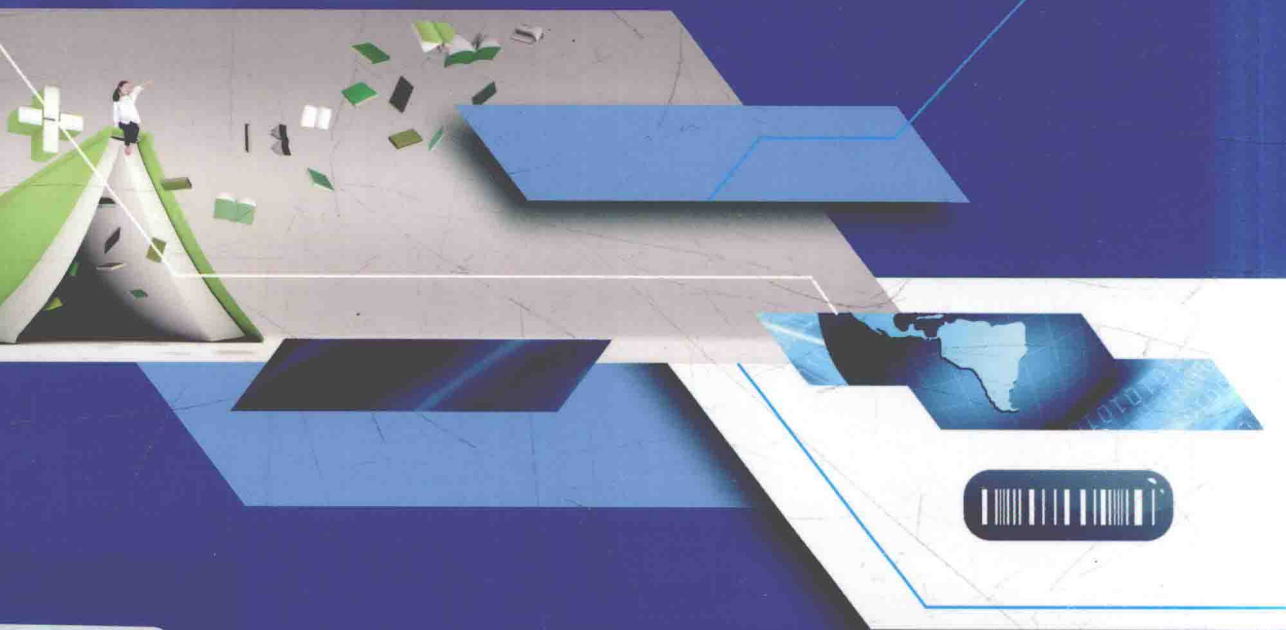


高等学校通信工程专业“十二五”规划教材

通信工程应用数学

TONGXIN GONGCHENG YINGYONG SHUXUE

王国才 董 健 雷文太 主编



中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

高等学校通信工程专业“十二五”规划教材

通信工程应用数学

王国才 董 健 雷文太 主 编
漆华妹 副主编
邹逢兴 主 审

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书以高等数学、线性代数、概率论与数理统计等数学知识为基础,也是通信工程主要专业课程的基础。全书共分9章,主要内容包括整数、关系与函数、复变函数论、数学变换、图与网络分析、随机过程、随机序列、排队论、矢量分析,每章后均附有习题。

本书力图简明而全面地介绍通信工程专业课程中应用的数学基础知识,力求数学原理与通信技术相结合。本书适合作为高等学校通信工程专业本科生的教材,也可作为通信工程技术人员的参考书。

图书在版编目(CIP)数据

通信工程应用数学 / 王国才,董健,雷文太主编. —
北京:中国铁道出版社,2017.1

高等学校通信工程专业“十二五”规划教材

ISBN 978-7-113-22591-9

I. ①通… II. ①王… ②董… ③雷… III. ①通信-
工程数学-高等学校-教材 IV. ①TN911.1

中国版本图书馆CIP数据核字(2016)第295142号

书 名:通信工程应用数学

作 者:王国才 董 健 雷文太 主编

策 划:曹莉群 周海燕

读者热线:(010) 63550836

责任编辑:周海燕 徐盼欣

封面设计:一克米工作室

封面制作:白 雪

责任校对:张玉华

责任印制:郭向伟

出版发行:中国铁道出版社(100054,北京市西城区右安门西街8号)

网 址: <http://www.51eds.com>

印 刷:北京海淀五色花印刷厂

版 次:2017年1月第1版 2017年1月第1次印刷

开 本:787mm×1092mm 1/16 印张:15 字数:370千

书 号:ISBN 978-7-113-22591-9

定 价:38.00元

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社教材图书营销部联系调换。电话:(010) 63550836

打击盗版举报电话:(010) 51873659

高等学校通信工程专业“十二五”规划教材

主 任：施荣华 李 宏

副主任：王国才 彭 军

主 审：邹逢兴

委 员：（按姓氏笔画排序）

王 玮 王 浩 石金晶 张晓勇

李 尹 李曦柯 杨政宇 赵亚湘

郭丽梅 康松林 梁建武 彭春华

董 健 蒋 富 雷文太

在社会信息化的进程中,信息已成为社会发展的重要资源,现代通信技术作为信息社会的支柱之一,在社会发展、经济建设方面,起着重要的核心作用。信息的传输与交换的技术即通信技术得到了快速的发展,通信技术是信息科学技术发展迅速并极具活力的一个领域,尤其是数字移动通信、光纤通信、射频通信、Internet 网络通信使人们在传递信息和获得信息方面达到了前所未有的便捷程度。通信技术在国民经济各部门和国防工业以及日常生活中得到了广泛的应用,通信产业正在蓬勃发展。随着通信产业的快速发展和通信技术的广泛应用,社会对通信人才的需求在不断增加。通信工程(也作电信工程,旧称远距离通信工程、弱电工程)是电子工程的一个重要分支,电子信息类子专业,同时也是其中一个基础学科。该学科关注的是通信过程中的信息传输和信号处理的原理和应用。本专业学习通信技术、通信系统和通信网等方面的知识,能在通信领域中从事研究、设计、制造、运营及在国民经济各部门和国防工业中从事开发、应用通信技术与设备。

社会经济发展不仅对通信工程专业人才有十分强大的需求,同样通信工程专业的建设与发展也对社会经济发展产生重要影响。通信技术发展的国际化,将推动通信技术人才培养的国际化。目前,世界上有3项关于工程教育学历互认的国际性协议,签署时间最早、缔约方最多的是《华盛顿协议》,也是世界范围知名度最高的工程教育国际认证协议。2013年6月19日,在韩国首尔召开的国际工程联盟大会上,《华盛顿协议》全会一致通过接纳中国为该协议签约成员,中国成为该协议组织第21个成员。标志着中国的工程教育与国际接轨。通信工程专业积极采用国际化的标准,吸收先进的理念和质量保障文化,对通信工程教育改革发展、专业建设,进一步提高通信工程教育的国际化水平,持续提升通信工程教育人才培养质量具有重要意义。

为此,中南大学信息科学与工程学院启动了通信工程专业的教学改革和课程建设,以及2016版通信工程专业培养方案。与中国铁道出版社在近期联合组织了一系列通信工程专业的教材研讨活动。他们以严谨负责的态度,认真组织教学一线的教师、专家、学者和编辑,共同研讨通信工程专业的教育方法和课程体系,并在总结长期的通信工程专业教学工作的基础上,启动了“高等院校通信工程专业系列教材”的编写工作,成立了高等院校通信工程专业系列教材编委会,由中南大学信息科学与工程学院主管教学的副院长施荣华教授、中南大学信息科学与工程学院电子与通信工程系李宏教授担任主任,邀请国家教学名师、国防科技大学邹逢兴教授担任主审。力图编写一套通信工程专业的知识结构简明完整的、符合工程认证教育的教材,相信可以对全国的高院校通信工程专业的建设起到很好的促进作用。

本系列教材拟分为三期,覆盖通信工程专业的专业基础课程和专业核心课程。教材内容覆盖和知识点的取舍本着全面系统、科学合理、注重基础、注重实用、知识宽泛、关注发展的原则,比较完整地构建通信工程专业的课程教材体系。第一期包括以下教材:《信号与系统》《信号与系统分析》《信息论与编码》《网络测量》《现代通信网络》《通信工程导论》《计算机通信网络安全技术及应用》《北斗卫星通信》《射频通信系统》

《数字图像处理》《嵌入式通信系统》《通信原理》《通信工程应用数学》《电磁场与电磁波》《电磁场与微波技术》《现代通信网络管理》《微机原理与接口技术》《微机原理与接口技术实验指导》。

本套教材如有不足之处,请各位专家、老师和广大读者不吝指正。希望通过本套教材的不断完善和出版,为我国信息与通信工程教育事业的发展和人才培养做出更大贡献。

高等学校通信工程专业“十二五”规划教材编委会

2015.7

通信的目的是由一个地方向另一个地方传递信息,以实现人与人之间、人与机器之间或机器与机器之间的信息交换。现代通信是用“电信号”或“光信号”运载信息的通信方式。信号可以表示为一个或者多个变量的函数,例如,一个语音信号可以表示为声压随时间变化的函数。为了分析信号在通信传输中的性质及其变化,需要应用数学变换、随机过程、随机序列、矢量分析;为了设计更大的通信范围,需要应用图论知识设计通信网络,应用排队论知识分析通信网络;为了实现通信保密和通信系统安全,可以应用数论知识、关系知识。可见,数学在通信工程领域中应用广泛,数学在通信系统以及信息处理等学科中具有极其重要的地位。

本书内容共分九章,第1章为整数,介绍整数的表示法、素数与因子分解、同余、离散对数、质素数有限域;第2章为关系与函数,介绍集合的概念与关系、关系的定义、相容关系、等价关系、偏序关系、函数;第3章为复变函数论,介绍复数与解析函数与柯西-黎曼条件、复积分、复级数、留数及其应用;第4章为数学变换,介绍傅里叶变换、拉普拉斯变换、 z 变换、小波变换;第5章为图与网络分析,介绍图的基本概念、图的连通性、树和图的最小部分树、最短路径问题及算法、网络最大流与最小费用流、关键路径;第6章为随机过程,介绍随机过程的基本概念、平稳随机过程、高斯随机过程、平稳随机过程通过线性系统、窄带随机过程;第7章为随机序列,介绍随机序列的基本概念、随机序列的产生方法、伪随机序列、随机序列在通信工程中的应用;第8章为排队论,介绍排队服务系统的基本概念、到达与服务时间的分布、简单的排队系统模型、 $M/G/1$ 排队系统、排队系统的优化、排队系统的随机模拟法;第9章为矢量分析,介绍矢量代数、三种常用的正交坐标系、标量场的梯度、矢量场的散度、矢量场的旋度、亥姆霍兹定理。

本书力图简明而全面地介绍通信工程专业课程中应用的数学基础知识,力求数学原理与通信应用相结合。

本书以高等数学、线性代数、概率论、数理统计为基础,由王国才、董健、雷文太任主编,由漆华妹任副主编。具体编写分工如下:第1、3、4、5、8章由王国才编写,第2章由漆华妹编写,第6、7章由董健编写,第9章由雷文太编写。本书由国防科技大学邹逢兴教授主审。中南大学施荣华教授、王伟副教授、康松林副教授、郭丽梅副教授对本书的编写提供了很多宝贵的建议;中国铁道出版社对本书的出版给予了大力支持,并提出了很多宝贵意见;在本书编写过程中参考了大量的书籍和国内外文献资料,在此,谨向这些著作者以及为本书出版付出辛勤劳动的同志深表感谢!

本书凝聚了编写人员多年的通信工程专业的教学经验和应用经验,由于编者水平有限,书中难免存在疏漏与不足之处,殷切希望广大读者批评指正。

编者

2016年8月

目 录

CONTENTS

第 1 章 整数	1
1.1 整数的表示法	1
1.1.1 进位制	1
1.1.2 原码、补码、反码	2
1.2 素数与因子分解	3
1.2.1 整除的概念及其性质	3
1.2.2 素数与合数	3
1.2.3 分解素因数	4
1.2.4 公约数与公倍数	5
1.2.5 辗转相除法	5
1.3 同余	6
1.3.1 同余的性质	6
1.3.2 欧拉定理	8
1.3.3 中国剩余定理	8
1.4 离散对数	9
1.5 素数检验方法	11
1.5.1 AKS 算法	11
1.5.2 Miller-Rabin 判定法	12
1.6 有限域	13
1.6.1 相关概念	13
1.6.2 有限域多项式	14
习题	16
第 2 章 关系与函数	18
2.1 集合的概念与表示	18
2.2 关系的定义与性质	20
2.3 相容关系	22
2.4 等价关系	23
2.5 偏序关系	25
2.6 函数	27
2.6.1 函数的概念	27
2.6.2 复合函数与逆函数	29
习题	33

第3章 复变函数论	34
3.1 复数与复变函数	34
3.1.1 复数及其代数运算	34
3.1.2 复数的几何表示	35
3.1.3 复数的乘幂与方根	37
3.1.4 区域	38
3.1.5 复变函数	39
3.1.6 复变函数的极限和连续	39
3.2 解析函数与柯西-黎曼条件	40
3.2.1 复变函数的导数与微分	41
3.2.2 解析函数及其简单性质	42
3.2.3 柯西-黎曼条件	43
3.3 复积分	45
3.3.1 复变函数积分的概念	45
3.3.2 柯西积分定理	48
3.3.3 柯西积分公式	50
3.4 复级数	52
3.4.1 复数项级数	52
3.4.2 幂级数	56
3.4.3 泰勒级数	59
3.4.4 洛朗级数	60
3.5 留数及其应用	62
3.5.1 孤立奇点	62
3.5.2 留数	66
3.5.3 留数在定积分计算中的应用	67
习题	70
第4章 数学变换	72
4.1 傅里叶变换	72
4.1.1 傅里叶级数	72
4.1.2 傅里叶变换的概念	75
4.1.3 傅里叶变换的性质	76
4.1.4 离散傅里叶变换	79
4.1.5 短时傅里叶变换与 Gabor 变换	83
4.2 拉普拉斯变换	85
4.2.1 拉普拉斯变换的提出	85
4.2.2 拉普拉斯变换的基本性质	88
4.2.3 拉普拉斯反变换	90
4.3 z 变换	96

4.3.1	z 变换的定义及其收敛域	96
4.3.2	序列 z 变换的基本特性	98
4.3.3	z 变换的性质	102
4.3.4	逆 z 变换	104
4.4	小波变换	110
4.4.1	小波	110
4.4.2	连续小波变换 (CWT)	112
4.4.3	离散小波变换 (DWT)	112
	习题	114
第 5 章	图与网络分析	115
5.1	图的基本概念	115
5.2	图的连通性	118
5.2.1	连通性的概念	118
5.2.2	有向图的连通性	119
5.2.3	k -连通	120
5.2.4	通信网的可靠性	121
5.3	树和图的最小部分树	122
5.3.1	树图的性质	122
5.3.2	图的最小部分树	123
5.3.3	求图的最小部分树的方法	123
5.3.4	霍夫曼树与霍夫曼编码	125
5.4	最短路径问题及算法	126
5.4.1	最短路径问题	126
5.4.2	最短路径算法	127
5.4.3	Bellman - Ford 算法	130
5.4.4	SPFA 算法	131
5.4.5	A* 搜索算法	132
5.4.6	Floyd 算法	133
5.5	网络最大流与最小费用流	134
5.5.1	网络最大流的概念	134
5.5.2	网络最大流的线性规划模型	134
5.5.3	弧标号法	135
5.5.4	最小费用流	136
5.6	关键路径	139
	习题	140
第 6 章	随机过程	142
6.1	随机过程的基本概念	142
6.1.1	随机过程的定义	142

6.1.2	随机过程的分布函数	142
6.1.3	随机过程的数字特性	143
6.2	平稳随机过程	144
6.2.1	平稳随机过程的定义	144
6.2.2	各态历经性	145
6.2.3	平稳随机过程自相关函数的性质	145
6.2.4	平稳过程的功率谱密度	146
6.3	高斯随机过程(正态随机过程)	148
6.3.1	定义	148
6.3.2	重要性质	149
6.3.3	高斯随机变量	149
6.4	平稳随机过程通过线性系统	151
6.5	窄带随机过程	153
6.6	随机过程在通信工程中的应用	154
	习题	154
第7章	随机序列	156
7.1	随机序列的基本概念	156
7.1.1	随机序列的定义及其概率描述	156
7.1.2	随机序列的数字特征	157
7.1.3	平稳随机序列	158
7.1.4	功率谱密度	159
7.1.5	平稳随机序列通过线性系统	159
7.2	随机序列的产生方法	161
7.2.1	随机数与伪随机数	161
7.2.2	随机序列的产生方法	162
7.3	伪随机序列	164
7.3.1	基本概念	164
7.3.2	序列的相关特性及其分类	165
7.3.3	m 序列	166
7.3.4	Gold 序列	170
7.3.5	M 序列	174
7.4	随机序列在通信工程中的应用	175
	习题	176
第8章	排队论	178
8.1	排队服务系统的基本概念	178
8.1.1	排队系统的组成和特征	178
8.1.2	排队服务系统的分类	179
8.1.3	排队系统的状态及参数	179

8.1.4	排队系统的指标	180
8.2	到达与服务时间的分布	182
8.2.1	顾客到达的分布	182
8.2.2	服务时间的分布	182
8.2.3	k 阶 Erlang 分布	183
8.3	简单的排队系统模型	183
8.3.1	$M/M/1$	183
8.3.2	$M/M/S$	187
8.3.3	$M/M/1/K/\infty/FCFS$	189
8.3.4	$M/M/S/K/\infty/FCFS$	191
8.3.5	$M/M/S/S/\infty/FCFS$	193
8.4	$M/G/1$ 排队系统	195
8.4.1	服务时间为任意分布	195
8.4.2	服务时间为 Erlang 分布	196
8.5	排队系统的优化	197
8.5.1	排队系统的优化问题	197
8.5.2	$M/M/1$ 模型中最优服务率 μ	197
8.5.3	$M/M/s/\infty/\infty/FCFS$ 模型中最优的服务台数 s	200
8.6	排队系统的随机模拟法	201
8.6.1	排队系统的模拟问题描述	201
8.6.2	随机数的产生	203
8.6.3	随机变量的模拟	204
8.6.4	到达过程和服务过程的模拟	205
8.6.5	排队系统的模拟	206
习题		211
第9章	矢量分析	213
9.1	矢量代数	213
9.1.1	标量和矢量	213
9.1.2	矢量的运算	213
9.2	三种常用的正交坐标系	214
9.2.1	直角坐标系	214
9.2.2	圆柱坐标系	215
9.2.3	球坐标系	216
9.3	标量场的梯度	218
9.3.1	方向导数	218
9.3.2	梯度	218
9.3.3	梯度的运算法则	219
9.4	矢量场的散度	219
9.4.1	矢量的通量	219

9.4.2 矢量的散度	220
9.4.3 散度定理	221
9.5 矢量场的旋度	222
9.5.1 矢量的环流	222
9.5.2 矢量场的旋度	222
9.5.3 斯托克斯定理	224
9.6 亥姆霍兹定理	224
习题	225
参考文献	226

第1章 整数

通信,一般是指信息的传输与交换.通信速率的基本单位是 bit/s. 可以将每一次传输与交换的信息看成一个整数或者若干整数.例如,因特网中的一个 IP 数据包 4500 001C 0001 0000 0411 8BB1 0A0C 0E05 0C06 0709 0102 0304 0506 0708,可以看成一个十六进制的整数,也可以看成由 45,00,00,1C,...28 个十六进制整数组成.在通信领域中,利用整数的性质,可以对信息进行编码、校验、加密等处理.

如果不加特殊说明,本章所涉及的数都是整数,所采用的字母(除了十六进制的数值)也表示整数.

1.1 整数的表示法

像 $-2, -1, 0, 1, 2$ 这样的数称为**整数**.正整数、零与负整数构成**整数系**.在整数系中,零和正整数统称为**自然数**. $-1, -2, -3, \dots, -n, \dots$ (n 为非零自然数)为**负整数**.

1.1.1 进位制

进位制是一种计数方式,亦称进位计数法或位值计数法.利用这种计数方式,可以使用有限种数字符号来表示所有的数值.一种进位制中可以使用的数字符号的数目称为这种进位制的**基数**或**底数**.若一个进位制的基数为 n ,即可称之为 n 进位制,简称 n 进制.现在最常用的进位制是十进制,这种进位制通常使用 10 个阿拉伯数字(即 $0 \sim 9$)进行计数.也常用十二进制,用于计算时辰、月份、一打物品.用于计算时间秒、分,使用六十进制.

在信息技术领域,通常用二进制、八进制、十六进制.二进制通常使用 2 个阿拉伯数字(即 0 和 1)进行计数.八进制通常使用 8 个阿拉伯数字(即 $0 \sim 7$)进行计数.十六进制通常使用 10 个阿拉伯数字(即 $0 \sim 9$)和 6 个英语字母(A~F)进行计数.

可以用不同的进位制来表示同一个数.例如,57,一般看成十进制数 57,为了区分其他进制的数,可以记成 $57_{(10)}$,可以用二进制表示为 $111001_{(2)}$,也可以用五进制表示为 $212_{(5)}$,同时也可以利用八进制表示为 $71_{(8)}$,亦可用十六进制表示为 $39_{(16)}$,它们所代表的数值都是一样的.这是因为有如下的关系式.

$$\begin{aligned} 57_{(10)} &= 5 \times 10^1 + 7 \times 10^0 \\ &= 1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 \\ &= 2 \times 5^2 + 1 \times 5^1 + 1 \times 5^0 \\ &= 7 \times 8^1 + 1 \times 8^0 \end{aligned}$$

$$= 3 \times 16^1 + 9 \times 16^0$$

一般来说, b 进制有 b 个数字, 如果 a_3, a_2, a_1, a_0 是其中四个数字, 那么就有

$$a_3 a_2 a_1 a_0 = a_3 \times b^3 + a_2 \times b^2 + a_1 \times b^1 + a_0 \times b^0$$

其中, $a_3 a_2 a_1 a_0$ 表示一个数字序列, 而不是数字的相乘。

从上面的叙述中, 不难得出以下结论:

- (1) 一个数的某种进制的表示形式是唯一的。
- (2) 不同的进制表示形式可以相互转换。
- (3) 转换的方法采用除法, 一个数除以 b , 则可以得到最低位; 商数除以 b , 则可以得到次低位, 重复用商数除以 b , 则可以得到全部位。
- (4) 在编写程序时, 大整数的表示也可以采用一个数组来存储表示这个数的数字序列。

1.1.2 原码、补码、反码

原码、补码、反码的目的是简化运算, 具体地说, 是为了让减法转换成加法。比如说时间, 按 12 个小时来算, 这个 12 就称为模数。假如现在的准确时间是 4 点, 有一个时钟显示的是 7 点, 要校准时间为 4 点, 可以将时针退 3 格 ($-3 = 4 - 7$), 也可以向前拨 9 格 ($-3 + 12 = 4 - 7 + 12$)。后退 3 格 (即 -3) 转换成前进 9 格 (即 $+9$)。这里的 9 怎么得到呢? 通过 $12 - (7 - 4)$ 。为了不用减法得到 9, 就需要引进反码和补码。

原码: 将符号位数码化了的数, 其中 “+” 用 0 表示, “-” 用 1 表示, 数值部分不变。

反码: 正数的反码表示与原码表示一样; 负数的反码表示是原码表示的符号位不变, 数值位逐位取反。

补码: 正数的补码表示与原码表示一样; 负数的补码表示是原码表示的符号位不变, 数值位逐位取反后最低位加 1 (反码加 1)。

对于 8 bit 的数据, 通常最高位表示符号, 低 7 位表示该数的绝对值, 这就是原码表示。部分 8 bit 整数的原码、反码、补码见表 1.1.1。应用补码, 容易验证 $12 - 3$ 可以转换成加法: 12 的补码 (00010100) 和 (-3) 的补码 11111101 相加。因为 $00010100 + 11111101 = 00001001$ (忽略进位)。

表 1.1.1

整数	-128	-127	-18	-3	-1	-0
原码	-	11111111	10010010	10000011	10000001	10000000
反码	-	10000000	11101101	11111100	11111110	11111111
补码	10000000	10000001	11101110	11111101	11111111	10000000
整数	+128	+127	+18	+3	+1	+0
原码	-	01111111	00010010	00000011	00000001	00000000
反码	-	01111111	00010010	00000011	00000001	00000000
补码	-	01111111	00010010	00000011	00000001	00000000

用 8 位二进制记录数据, 按照定义, 0 有两种补码形式, 即 $+0$ (00000000) 和 -0 (10000000)。为了防止 0 有两个编码, 即保证 0 的唯一性, 把 10000000 分配给 -128, 这样还可以多表示一个数字。之所以不分配给 +128, 是因为其最高位是 1, 表示一个负数, 分给正数的话将会引起出错。

用 8 位二进制记录数据, 只能存储 -128 ~ 127 之间的数据, 如果超过 127 或小于 -128 就需要增加位数, 原码、补码、反码的表示规则不变。

1.2 素数与因子分解

1.2.1 整除的概念及其性质

设 a, b 是给定的整数, $b \neq 0$, 若存在整数 c , 使得 $a = bc$, 则称 b 整除 a , 记作 $b \mid a$, 并称 b 是 a 的一个约数(因子, 因数), 称 a 是 b 的一个倍数, 如果不存在上述 c , 则称 b 不能整除 a .

显然:

- (1) 1 是任何整数的约数, 即对于任何整数 a , 总有 $1 \mid a$.
- (2) 0 是任何非零整数的倍数, $a \neq 0, a$ 为整数, 则 $a \mid 0$.
- (3) 若一个整数的末位是 0, 2, 4, 6 或 8, 则这个数能被 2 整除.

1.2.2 素数与合数

一个数, 如果只有 1 和它本身两个约数, 则称为素数(或称质数). 100 以内的素数有 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

一个数, 如果除了 1 和它本身还有别的约数, 则称为合数. 例如, 4, 6, 8, 9, 12 都是合数.

0 和 1 不是素数也不是合数. 自然数除了 0 和 1 外, 不是素数就是合数. 如果把自然数按其约数的个数的不同分类, 可分为素数、合数、0 和 1.

如何找出某个正整数 n 内的所有素数呢? 公元前 250 年由古希腊数学家埃拉托斯特提出了一种筛法, 现在称之为埃拉托斯特筛法, 简称埃氏筛或爱氏筛, 是一种简单地找出某个正整数 n 内的所有素数的方法. 其方法如下:

首先, 列出从 2 到 n 的所有整数. 先用 2 去筛, 即把 2 留下, 把 2 的倍数剔除掉; 再用留下来的比 2 大的最小数, 也就是 3 筛, 把 3 留下, 把 3 的倍数剔除掉; 接下去用留下来的比 3 大的最小数 5 筛, 不断重复下去, 直到这个数大于 $\sqrt{n}$. 留下来的就全部是素数.

例如, 求 25 以内的素数的步骤如下:

- (1) 列出 2 以后的所有整数:

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- (2) 标出序列中的第一个素数, 也就是 2(序列中第 1 个), 划掉 2 的倍数(用下画线标出), 序列变成

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- (3) $25 > 2 \times 2$, 继续标出序列中的第二个素数, 也就是 3, 划掉 3 的倍数(用下画线标出), 即 9, 15, 21, 序列变成

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- (4) $25 > 3 \times 3$, 继续标出序列中的第三个素数, 也就是 5, 划掉 5 的倍数(用下画线标出), 即 25, 序列变成

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

- (5) 现在这个序列中最大数 $23 < 5 \times 5$, 那么剩下的序列中所有的数都是素数, 即

2 3 5 7 11 13 17 19 23

1.2.3 分解素因数

每个合数都可以写成几个素数相乘的形式,并且这种表示形式是唯一的. 这个结论称为**算术基本定理**. 其中每个素数都是这个合数的因数,称为这个合数的**素因数**. 例如, $15 = 3 \times 5$, 3 和 5 称为 15 的**素因数**. 把一个合数用素因数相乘的形式表示出来,称为**分解素因数**. 例如,把 28 分解素因数: $28 = 2 \times 2 \times 7$.

显然,每个偶数都有素因数 2. 分解素因数的问题变为奇数的素因数分解问题.

分解素因数的方法有多个,目前的研究也很活跃.

1. 试除法

试除法就是尝试 $2 \sim \sqrt{n}$ 的整数是否整除 n . 如果能整除则得到一个素因数和商. 从该素因数开始继续对该商进行尝试,直到尝试的素因数等于尝试的商为止,或者尝试的素因数大于 $\sqrt{n}$ 为止.

2. 试拆法

试拆法就是尝试将奇数 n 表示成 m 个连续整数的和. 例如, $51 = 16 + 17 + 18 = 3 \times 17$. 试拆法的过程就是从 1 开始寻找若干连续整数的和的过程,全程不用除法. 用试拆法分解 51 的素因数的过程如下:

$$51 < 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = 55$$

$$51 < 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = 54$$

$$51 < 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = 52$$

$$51 > 4 + 5 + 6 + 7 + 8 + 9 + 10 = 49$$

$$51 < 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 = 60$$

$$51 < 5 + 6 + 7 + 8 + 9 + 10 + 11 = 56$$

$$51 = 6 + 7 + 8 + 9 + 10 + 11 = (6 + 11) / 2 \times 6 = 17 \times 3$$

3. 费马整数分解方法

费马整数分解方法基于以下事实:如果正整数 $N = 2n + 1$,那么存在正整数 a, b 使得 $a^2 - b^2 = N$.

假设 $N = cd$,那么 c 和 d 必为奇数,令 $a = \frac{c+d}{2}, b = \frac{c-d}{2}$,不难验证 $a^2 - b^2 = N$. 因为 $(n+1)^2 - n^2 = N$,

方程 $x^2 - y^2 = N$ 至少有一组整数解,如果 $(x, y) = (a, b)$ 是它的一组正整数解,那么 $a \geq \sqrt{cd} = \sqrt{N}$,可见 a 取值于 $\sqrt{N} \sim n+1$ 之间. 费马整数分解的算法描述如下:

输入:正奇数 N .

输出:无.

返回: N 的一个因子.

(1) 令 $x = \sqrt{N}$;

(2) 令 $a = \lceil x \rceil, b = a^2 - N$;

(3) 如果 b 是一个完全平方数,转(5);

(4) 令 $a = a + 1, b = a^2 - N$,转(3);

(5) 返回 $a - \sqrt{b}$,结束.

如果费马整数分解算法返回的值为 1,则说明 N 为素数. 费马整数分解方法只是分解出整数的一个因子,不像试除法那样分解出整数的各个素数因子. 如果希望用费马整数分解方法分解出整数的各个素因子,可以反复使用该方法.