七彩数学

姜伯驹 主编

QICAISHUXUE

数论与密码

冯克勤□著

科学出版社
www.sciencep.com

七彩数学

姜伯驹 主编

QICAISHUXUE

数论与密码

冯克勤□著

科学出版社

北京

内 容 简 介

密码学和信息安全是一个重要的科学技术领域，不仅关系到国家的安全，而且与人们的经济活动和社会生活息息相关. 通信的数字化和计算机技术的发展使得离散型数学(数论、代数、组合学等)在通信中得到广泛而深刻的应用. 本书通俗地介绍密码学和信息安全的历史发展与进步，用例子解释重要密码体制和信息安全的一些基本问题，讲述初等数论的基本知识及其在密码学和信息安全中的应用.

本书读者对象为对初等数论和密码学有兴趣的广大读者，具有高中以上数学知识的人均可阅读.

图书在版编目(CIP)数据

数论与密码/冯克勤著. —北京：科学出版社，2007

(七彩数学)

ISBN 978-7-03-017885-5

Ⅰ.数… Ⅱ.冯… Ⅲ.①数论-通俗读物②密码-理论-通俗读物

Ⅳ.①O156-49②TN918.1-49

中国版本图书馆 CIP 数据核字(2007)第 099664 号

责任编辑：吕 虹 陈玉琢 莫单玉/责任校对：张 琪

责任印制：赵德静/封面设计：王 浩

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

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2007 年 3 月第 一 版 开本：A5(890×1240)

2007 年 3 月第一次印刷 印张：4 5/8

印数：1—5 000 字数：60 000

定价：18.00 元

(如有印装质量问题，我社负责调换〈环伟〉)

冯克勤

清华大学教授。1941年出生，1968年中国科学技术大学数学系研究生毕业。1973至2000年在中国科学技术大学数学系和研究生院（北京）任教，2000年后到清华大学数学系工作。从事代数数论和代数编码理论研究。出版专著《分圆函数域》、《代数数论简史》等，出版大学生和研究生教材《整数与多项式》、《近世代数引论》、《交换代数基础》、《代数数论》和《代数与通信》等，主编丛书《走向数学》。

七彩数学

姜伯驹 主编

《数学走进现代化学与生物》

姜伯驹 钱敏平 龚光鲁 著

《数论与密码》 冯克勤 著

《迭代 浑沌 分形》 李 忠 著

《数学的力量——漫话数学的价值》

李文林 任辛喜 著

《古希腊名题与现代数学》 张贤科 编著

丛书序言

2002 年 8 月，我国数学界在北京成功地举办了第 24 届国际数学家大会. 这是第一次在一个发展中国家举办的这样的大会. 为了迎接大会的召开，北京数学会举办了多场科普性的学术报告会，希望让更多的人了解数学的价值与意义. 现在由科学出版社出版的这套小丛书就是由当时的一部分报告补充、改写而成.

数学是一门基础科学. 它是描述大自然与社会规律的语言，是科学与技术的基础，也是推动科学技术发展的重要力量. 遗憾的是，人们往往只看到技术发展的种种现象，并享受由此带来的各种成果，而忽略了其背后支撑这些发展与成果的基础科学. 美国前总统的一位科学顾问说过："很少有人认识到，当前被如此广泛称颂的高科技，本质上是数学技术".

在我国，在不少人的心目中，数学是研究古老难题的学科，数学只是为了应试才要学的一门学科. 造成这种错误印象的原因很多. 除了数学本身比较抽象，不易为公众所了解之外，还有

学校教学中不适当的方式与要求、媒体不恰当的报道等等. 但是,从我们数学家自身来检查,工作也有欠缺,没有到位. 向社会公众广泛传播与正确解释数学的价值,使社会公众对数学有更多的了解,是我们义不容辞的责任. 因为数学的文化生命的位置,不是积累在库藏的书架上,而应是闪烁在人们的心灵里.

20 世纪下半叶以来,数学科学像其他科学技术一样迅速发展. 数学本身的发展以及它在其他科学技术的应用,可谓日新月异,精彩纷呈. 然而许多鲜活的题材来不及写成教材,或者挤不进短缺的课时. 在这种情况下,以讲座和小册子的形式,面向中学生与大学生,用通俗浅显的语言,介绍当代数学中七彩的话题,无疑将会使青年受益. 这就是我们这套丛书的初衷.

这套丛书还会继续出版新书,我们诚恳地邀请数学家同行们参与,欢迎有合适题材的同志踊跃投稿. 这不单是传播数学知识,也是和年青人分享自己的体会和激动. 当然,我们的水平有限,未必能完全达到预期的目标. 丛书中的不当之处,也欢迎大家批评指正.

姜伯驹

2007 年 3 月

序　言

人类社会发展到一定阶段，产生了语言和文字. 一些国家或地区的人们采用共通的语言和文字进行思想的交流和沟通，对于社会生产和生活产生巨大的作用. 但是在另一方面，在许多社会活动中，思想交流需要对外人保守秘密，使用各种暗语、密文和密码. 大约四千年前，埃及尼罗河畔有些墓碑上所刻的铭文不是用当时的文字写成的，而是用一些奇怪的符号. 公元前 130 年左右，在另一个文明古国美索不达米亚，碑文上的人名改换成数字，增加了神秘性. 在印度，公元前 300 年左右，《经济论》一书，记载了官员用密码给密探下达任务. 在中国，明朝蒋一葵所著《尧山堂外记》一书谈到三国时期蜀国考试制度时，提到主考官和考生约定的作弊暗语……

公元 10 世纪以后，密码逐渐广泛地使用到政治、军事和外交上，在这些领域中通信加密的重要性，加速了密码的发展. 中国在公元 11 世

纪的《武经总要》一书中，详细记载了一个小型但却是名符其实的军用密码本，将从“申请弓箭”到“报告胜利”等 40 条信息，分别用一首诗的前 40 个汉字来代替. 在 16 世纪末期，欧洲许多国家设定了专职的密码秘书，重要的文件都采用密写. 有加密就有破密，加密和破密是矛和盾的两个方面，呈现出“魔高一尺，道高一丈”的竞赛场面. 到了 18 世纪，欧洲各国普遍建立了“黑屋”，它的任务就是截取别人来往信件，设法破译这些信件，获得重要的军事和外交情报. 在当时，维也纳的“黑屋”是最高明的一个，曾破译过拿破仑的信件. 在第一次大战期间，英国的“40 号房间”从 1914 年 10 月至 1919 年，共截获和破译了 15000 份德国密码电报.

除了保密在政治和军事中的重要性之外，通信技术的进步也极大地加速了保密通信的发展. 在人类早期通信中，重要的信件主要靠信使传送，密码的构作方式主要借用文字或字母的替换，或者把字母改用数字代码，而破译主要用纸笔手工操作. 后来发明了保密机，用机械式的运算或变换方式代替手工运算和操作，提高了保密通信的效率. 1844 年有线电报的发明和 1895 年无线电的诞生，引发通信技术的一场

重要革命. 有线电报和无线电通信使信息传输快速方便,与此同时,大量的电信号在无线电传输时容易被外人截取. 这些容易截取到的大量密文为破译者提供了更多的素材,促进了破译技术的发展. 由于密文易被截取从而增大了被破译的可能,因此也要求加大保密程度,这迫使人们创造更高明的加密方法和手段. 到了第二次世界大战期间,电子通信技术手段促使加密和破译方法有新的飞跃. 于是,交战双方——德国、日本、英国,尤其是美国——采取了一项重大措施,就是请一批出色的数学家从事这项工作,借助于数学思想和工具进行加密和破译. 美国数学家在密码分析(即破译)方面干得非常出色. 日本人在 20 世纪 30 年代后期发明了一种高级加密机"九七式欧文印字机"(美国人称之为"紫密"),使用了相当复杂的多表代替型密码. 美国密码分析学家利用数学工具(数论、群论和数理统计学)在 1940 年破译了"紫密",但不为日本人所知. 1942 年日本突袭中途岛海战的失败,一个重要原因是美国破译了日本攻击中途岛的情报. 1943 年 4 月,美国破译了日本联合舰队长官山本五十六视察前线阵地的详细日程表,在 4 月 18 日这一天,派 18 架战斗机在

预定时间和地点打下山本的座机，成为密码史上精彩的一页，也展现了数学在加密和破译中的巨大威力. 美国数学家香农(Claud Elwood Shannon)是这期间建立和发展通信理论的杰出代表. 他在1948年和1949年分别发表了两篇著名论文《通信的数学理论》和《保密系统的通信理论》. 前一篇文章建立了信息论，把整个通信(特别是可靠性通信)建立在坚实的数学基础之上；而后一篇文章建立了保密通信的数学理论. 在早期发展中，加密方式五花八门(包括用密写药水的隐写术、把文字藏在优美画图之中的隐形术等)，而破译更多地体现为心智的竞赛，其特性更像是一种艺术，香农建立保密通信数学理论之后，加密和解密才成为一种科学(密码学和密码分析学).

20世纪60年代末期开始，通信技术又有飞速的发展. 微电子学的进步使电子元件更加可靠和小型化，并且出现了高速的数字计算机和大规模的数字通信网络. 这些技术进步为保密通信带来许多新的课题. 首先，由于计算机的进步，密码分析有了更快速的计算手段，原来以为安全的加密方法现在变得不安全了，这就促使加密和破译的方式都提高到一个新的水平.

另一方面，通信网络在全球的普遍采用，深入到经济和社会的各个层面，甚至到千家万户的日常生活. 保密通信不仅是政治和军事上的需要，而且也成为电子商务活动、社会管理以及保护个人隐私等方面的重要问题. 通信进入多样化和复杂的社会活动各领域之后，也对通信的安全性提出了许多新的要求. 例如，如何保护计算机数据？通信网络的发展，每个用户与众多用户进行保密通信，大量的密钥如何保存、管理和更换？以电子的方式购货或付款时，如何进行电子签名以确认购货人和借款人的身份？商业电子活动的双方发生冲突时，以何种方式加以仲裁，并且在仲裁过程中各方还保证不泄漏秘密……这些需要解决的新课题使主要研究信息加密的密码学扩展成考虑各种安全性能的一个广泛领域，现在称之为“信息安全”领域. 1976年，美国人狄菲(W. Diffie)和海尔曼(M · E · Hellman)发表了“密码学中的新方向”一文，提出一种全新的密码思想，叫作公开密钥体制. 这种体制很好地解决了大量密钥管理和数字签名问题，马上就受到广泛的注意. 公钥体制是信息领域一场重大的变革，现在已经有效而广泛地应用于信息安全的各个方面.

半个多世纪以来，在通信的发展中，数学起了很大的作用，这主要体现在两个方面：数学工具的更新和通信与数学发展的互动. 在电子通信和计算机的早期发展阶段，电子信号是连续信号，分析信号的主要数学工具是微积分中的傅里叶变换. 大家知道，17 世纪欧洲工业革命当中，由于机械工业发展，力学导致牛顿发明微积分、流体力学和电磁学，使微积分得到巨大发展，成为数学的主流. 数字通信和数字计算机采用脉冲信号，信号不是连续的而只有有限个状态(通常只有两个状态，数学上表示成 0 和 1). 描述这种有限离散的逻辑线路采用离散性数学工具，主要是数论、代数和组合数学. 数论、代数和几何是最古老的 3 个数学分支. 数学被认为是科学的皇后，而数论被大数学家高斯称为是数学的皇后. 数论的研究博大精深，一直是象牙之塔，现在在通信中得到深刻的应用. 比如，在公钥体制中目前广泛采用的两种方案(其一是大数分解的离散对数方案)都是采用了数论方法. 数论和抽象代数(群、环、域、特别是有限域)现已成为通信工程师必不可少的数学工具. 组合数学在半个世纪之前不属于数学的大雅之堂，被认为是一些数学游戏(36 军官问

题、一笔画问题、四色问题、周游世界问题等). 数字通信和离散规划等方面的发展大大提高了组合数学的地位. 在具有百年历史的世界数学家大会上,历来只有传统的数学学科被列为大会分组之中. 1978 年设立了新的小组“离散数学与计算机科学中的数学”. 而从 1983 年开始,组合数学单独成为一个小组. 第二个方面,是通信(比如信息安全)为数学界提出了一系列具有实际意义的研究问题,推动了数学的发展,为传统学科(如数论)注入了新的活力,开辟了新的研究方向(如计算数论和计算代数),甚至出现了许多全新的数学研究领域(如计算复杂性理论等). 在许多先进国家,通信和计算机领域凝聚了阵营强大的数学家队伍. 保密通信和信息安全领域是最需要独立自主和创新思想的一个领域,需要数学家与通信、计算机专家有效地通力合作.

以上我们简要地介绍了保密通信发展的大致轮廓. 从介绍中可以看出数论、代数、组合数学和概率统计学等多个学科在密码学、密码分析和信息安全各方面都有重要的应用. 在这本小册子里,我们通俗地讲述密码学和信息安全发展中的一些例子,说明数论(主要是初等数

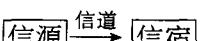
论)如何用于保密通信的这些领域. 在讲述过程中我们也浅显地介绍初等数论的一些知识以及数论发展中的一些故事.

作者

目　录

1 什么是保密通信

人们在社会活动和日常生活中离不开通信交往. 通信有许多不同的具体方式. “烽火连三月,家书抵万金”中传递战事信息的烽火台和战士寄回家中的书信为通信的两种方式. 从电发明之后的电报和电话一直到计算机时代的电子邮件、图象和数据的传送,通信的技术手段日新月异,但是通信的数学模型均可简单而统一地表成以下形式.



(发方) (收方)

通信是发方和收方之间的一种活动. 发方在信源把信息 x 通过信道传送出去,收方在信