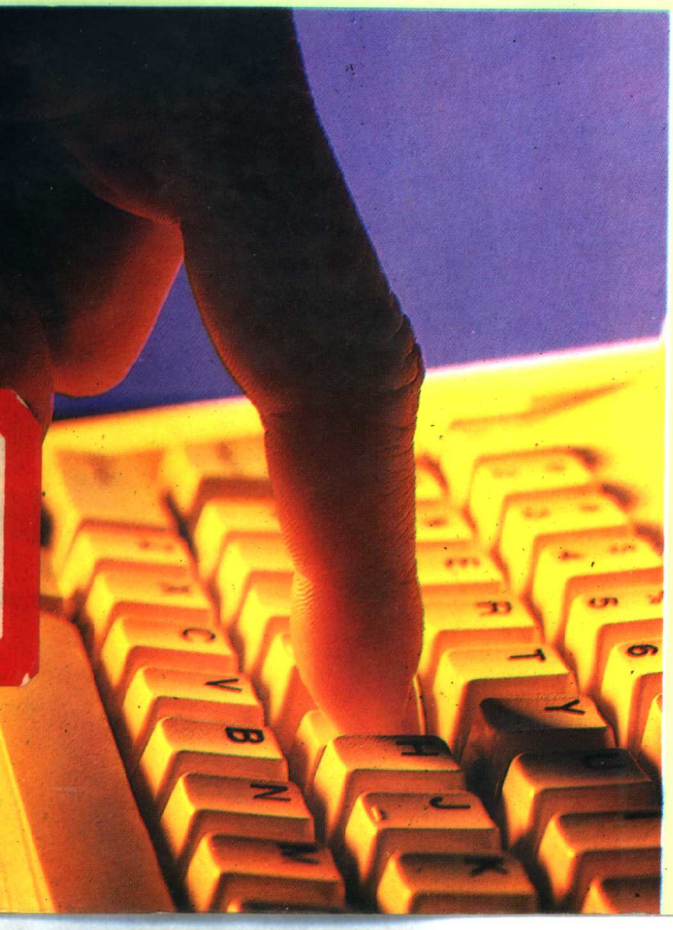
数学与电脑

MATHEMATICS AND CONPUTER

走向数学丛书

杨重骏
杨照崑 著



走向数学丛书

数学与电脑

杨重骏
杨照崑 著

湖南教育出版社

数学与电脑

Mathematics and Conputer

杨重骏　杨照崑　著

Yang Chong—Chun Mark C. K. Yang

责任编辑：孟实华

湖南教育出版社出版发行　（东风路附1号）

湖南省新华书店经销　湖南省新华印刷二厂印刷

787×1092毫米　32开　印张：5　字数：110,000

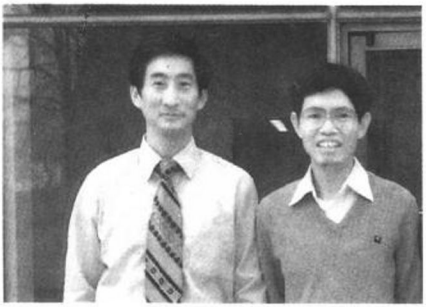
1993年4月第1版　1993年4月第1次印刷

ISBN 7—5355—1581—9/G·1576

定　价：3.50元

"走向数学"丛書

陳省身題



作 者 简 介

杨重骏，男，1942年生于江苏无锡，华裔数学家，教授。台湾大学数学系毕业后，1965年前往美国威斯康辛大学专修复分析，取得硕士及博士学位。后在美国密西根州立大学从事博士后研究，于1970年到美国海军研究实验所、数学研究中心从事数学研究工作，直至1990年应聘担任新成立的香港科技大学数学系教授。其间曾应聘担任台湾中央研究院客座专家及美国芝加哥城的伊里诺理工学院的客座教授。

主要的数学研究是亚纯函数值分布及其分解等方面。

（照片中左为作者）

杨照崑，男，1942年生，安徽桐城人，华裔数学家，教授。1964年台湾大学电机系毕业，于1967年、1970年取得美国威斯康辛大学数学硕士、统计学博士学位。毕业后主要任职于佛罗里达大学统计系，曾访问伊州理工学院电机系、贝尔实验室、美国能源部、海军研究所，以及台湾中央研究院资讯所。现为佛罗里达大学软体工程研究所研究员。

研究方向为软体可靠性测定及模拟理论，科研方面曾发表论文60余篇，中文著作有《不等式》，《现代应用数学》，《整数论及其应用》，《电脑硬体简介》，英文著作有《如何用计算机了解统计》。曾获海外华人著作奖，并被选为泛华统计协会理事。

业余方面喜欢小说与魔术，曾在报纸上发表多篇小说并在当地中小学为孩子们表演魔术。

前　言

王　元

从力学、物理学、天文学直到化学、生物学、经济学与工程技术，无不用到数学．一个人从入小学到大学毕业的十六年中，有十三、四年有数学课．可见数学之重要与其应用之广泛．

但提起数学，不少人仍觉得头痛，难以入门，甚至望而生畏．我以为要克服这个鸿沟，还是有可能的．近代数学难于接触，原因之一大概是由于其符号、语言与概念陌生，兼之近代数学的高度抽象与概括，难于了解与掌握．我想，如果知道讨论的对象的具体背景，则有可能掌握其实质．显然，一个非数学专业出身的人，要把数学专业的教科书都自修一遍，这在时间与精力上都不易做到．若停留在初等数学水平上，哪怕做了很多难题，似亦不会有助于对近代数学的了解．这就促使我们设想出一套“走向数学”小丛书，其中每本小册子尽量用深入浅出的语言来讲述数学的某一问题或方面，使工程技术人员，非数学专业的大学生，甚至具有中学数学水平的人，亦能懂得书中全部或部分含义与内容．这对提高我

国人民的数学修养与水平，可能会起些作用.显然，要将一门数学深入浅出地讲出来，决非易事.首先要对这门数学有深入的研究与透彻的了解.从整体上说，我国的数学水平还不高，能否较好地完成这一任务还难说.但我了解很多数学家的积极性很高，他们愿意为“走向数学”撰稿.这很值得高兴与欢迎.

承蒙国家自然科学基金委员会、中国数学会数学传播委员会与湖南教育出版社的支持，得以出版这套“走向数学”丛书，谨致以感谢.

序：现代电子计算机中的几个数学问题

在这本小册子里我们收集了10篇与电子计算机科学有关的数学问题，我们介绍这些问题的主要原因是我们曾做过这些方面的研究或常常读到别人报导这一类的问题，当我们发现它们可以用较浅显的文字有趣地写出来时，我们就陆续地写，其中前面五篇都在《数学传播》（台湾中央研究院数学研究所编的一个刊物，后同.）上发表过，不过收集在本书中时，我们略有增删，为的是方便读者的阅读.

计算机与数学有一个共同点，就是要条理分明，一丝不苟.讲不清楚的东西不算数学，也无法叫计算机运转计算，即使要描写一种模糊的观念，都得描述得清清楚楚（参看第六章模糊集浅介）.由于计算机的性能愈来愈强，可以应用的范围也就愈来愈大，数学也就用得更多.以往应用数学多半是指物理工程方面的微分方程式，偏重于解析数学，现代计算机所要用到的数学几乎无所不包，数论、抽象代数及几何都有重要的用途.特别是现有的数学技巧还不够应付巨大计算量的处理实际问题，仍需要向前发展、突破，获得新的数学理论及应用.

本册所收集的只包括：一、计算机信号传递的正确性与保密性（第一，二，三，五，八，九章）；二、计算机快速计算问

题(第四及第七章);三、计算机处理模糊问题的数学(第六章);四、统计学与模拟实验(第十章)。虽材料有限,但至少可以略窥数学在计算机上应用的梗概及其进展。

此书前九章原由台湾知识系统出版社发行,为其电脑丛书之一,今很高兴此书有机会被介绍给国内广大的读者而再版。为充实本书的内容及效用,我们特加添了新的一章作为此版的第十章。

最后由于北京大学李忠教授及中国科技大学冯克勤教授等对本书的赏识及推荐,天元基金的赞助及湖南教育出版社孟实华女士再版本书所作的种种努力,使得我们再一次达成回馈故国之愿,容在此致上我们的谢忱。

杨重骏　杨照崑

目　录

第一章　质数的建造、分布及检验

§1 前　言

你看过《数学传播》1984年12月号（32期）上第三十四届国际科技展数学得奖作品简介吗？这类展览都以是否“创新”为作品的评价，而在数学部门中，在《数学传播》所介绍的八个得奖作品中，就有五个属于“数论”的领域，占了得奖作品的一半以上，为什么？因为数论有它特别迷人的地方——那就是在极简单的规则中作极复杂的变化，一个类似的例子是围棋。围棋的规则极简单而其变化极为复杂，可以说是最迷人的一种棋类。相反的，海陆空军棋其规则极繁而变化又小，几乎没有人下了。又研究整数论所遭遇的问题及研究对象要比其它各门数学来得简单明了，不外乎是讨论正整数1，2，3，4…的种种特殊性质，其变化之大，一直困惑许许多多的数学家。

以往整数论曾一直被人认为是最纯的纯数学，没想到由于最近美国有人利用找一个大数目的质数因子的困难性及其它质

数的一些特有性质，而设计了一种可公开传递(即不怕被敌方截获)且保密性极高的密码，引起了军方、工商界的莫大兴趣，有关这方面研究经费大为增加，我们在此简略地说明一下该密码的原理（对数论不熟的读者可参阅[1]或先阅下章)。在收报方甲先找出两个大的质数p、q，使$m=pq$，及取任一与$\varphi(m)=(p-1)(q-1)$互质的整数a，将此两数值m、a公开传递给发报方乙（甚至登报声明!)，现假设发报方乙要将一信号（整数形式)拍给甲。设该代号为整数值x(这是保密的且比p、q小很多)，当然乙不能迳自公开拍发x给甲，而公开拍明码$c\equiv x^a \pmod m$给甲方，现甲方收到明码整数c后设法译回到x，如何做到此一译码的工作呢？因甲方有资料a及$\varphi(m)$，φ为Euler函数，$\varphi(m)$表所有小于m且与m互质的正整数的数目。由假设a，$\varphi(m)$互质，故有正整数d及负整数b使得$ad+\varphi(m)b=1$，这时甲方将收到的明码c作变换：$y=c^d \pmod m$；注意取y为小于m的整数，及由于x小于p及q，故x必与m互质，因而由尤拉(Euler)定理我们有$x^{\varphi(m)}\equiv 1 \pmod m$，因此

$$y\equiv c^d\equiv(x^a)^d\equiv x^{ad}\equiv x^{1-\varphi(m)b}$$

$$\equiv x\cdot x^{-\varphi(m)b}\pmod m\equiv x\pmod m$$

现若两正整数x、y皆小于m且模m同余，故只有$x=y$，因而甲方就可把密码收到了。

欲解此密码势必要知d，但要知d非要知$\varphi(m)(=(p-1)\cdot(q-1))$也即要知$p$及$q$，找不到$p$、$q$就无法得$\varphi(m)$及$d$，而硬要从$c$得出$x$就似乎很困难了。目前分解一个整数$n$的因子仍停留在近似硬试的阶段，由后面的“筛法”原理我们知道要从2，3，5，7，…一直试到小于$\sqrt{n}$的质数为止，由[1]中可知若n为－50位数(p、q皆为25位数)，则分解n要除10^{25}次，以每秒10^6次的电脑计算速度则将是一个10^{11}年的工作，若用特殊的快速法则来

进行也得要10^{10}次的运算，约4个小时电脑的计算时间，若n为一个100位的整数，则用目前最快速的电脑来操作运算也得要74年左右(中间还要保证机械没故障才行)，所以目前用这种方法来传递需保密的密码是相当安全的了。

质数可以说是整数的基础，由上面的应用我们欲充分利用质数必须要能建造很大的质数，要侦破上面密码的应用，我们也要知道质数的分布.本文就是针对此而需求作些浅显的介绍，希望能引起读者更大的兴趣，作更进一步的研究（而且可以保证的、是任何这方面的突破，无论在理论上与实用上都会引起强烈的反响)，光大我们祖先的光辉(因有的密码是利用“中国剩余定理”造成的)。

具体地讲，我们主要将介绍的是：1.质数及质数表的制造；2.如何构造任何一串列的大质数；3.质数在整数中的分布或密度；4.质数的检验。又本文的介绍之参考书〔1〕、〔2〕皆是新近出版的。

§2 质数表(筛法)及质数的制造

由于质数是不具有任何异于1及其本身的因子，所以早在纪元前200年左右古希腊学者Eratosthenes（以下简称爱氏）就为我们发明一个可找出所有质数的法则，称为筛法（Sieve method)。据说爱氏在找质数时，他把整数一一照序写在一片草质的纸上，凡是非质数他就用火在那位置烧一个洞，最后整片纸只留下密密麻麻的许多洞，很像一个筛子，故叫做“筛法”。它的原则如下：将正整数由1照大小依次排出一列或一矩阵（如图1是一正方形矩阵，其由1至100的整数组成)，则头一个

数为1，为非质数删掉，其下一个为2为质数留下，则2以后删掉所有2的倍数(4，6，8，10，12，14，16，18…)，然后在所剩的数中大于2的第一个数3，其为一质数，继3以后删掉3的倍数(即6，9，15，21…)，3之后5为第一个未被删掉的数其为一质数，删掉所有5的倍数(10，…)，如此泡制，所留下的就是所有的质数(若只取1至N来筛，则如此所得的是1与N间所有的质数。在没有一张质数表时，我们怎样确定一给定的正整数N是否为质数呢?在N很大时若是以2到$N-1$所有的质数一一来试除N会是件很耗时的事的。好在我们只需用2到$\sqrt{N}$间所有的质数来试即可，这样一来就省了许多的除法。这是因为若N为非质数，则$N=n_1\times n_2$，n_1及n_2为两个大于1的正整数，且必有一个数n_1或n_2不大于$\sqrt{N}$，利用此一观察及筛法我们很容易把所有不大于某个正整数N(N不是很大时)的质数找出来。例如我们要列出100以下所有的质数，我们只需用小于$\sqrt{100}=10$以下的质数2，3，5，7用筛法把所有小于100的质数找出如下：

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。

目前我们有10亿($=10^9$)以内的质数表。而利用大质数的密码为了防止敌人利用电脑来侦破，往往是用有50位的质数，所以用筛法来建造大质数仍无法合于实用。

又用筛法制造大的质数时的一个缺点是每次要列出或利用许多的正整数来求得，这在实用上很不方便。我们很想随意制造一些很大的质数，该如何做呢？最理想的是我们能找出一个公式或一个式子，只要把适当的数代入就可得出很大的质数，我们中国人很早有一个有关质数的制造及拣选，认为一个正整数n为质数的充要（充分及必要）条件是n可整除2^n-2，即