教师教育新行动论丛

数论与密码

杨思熳　主编

SHU LUN YUMIMA

华东师范大学出版社

教师教育新行动论丛

数论与密码

杨思熳　主编

华东师范大学出版社

图书在版编目（CIP）数据

数论与密码/杨思熳主编. —上海：华东师范大学出版社，2010
ISBN 978-7-5617-7838-8

Ⅰ.①数… Ⅱ.①杨… Ⅲ.①初等数论②密码—理论
Ⅳ.①O156.1②TN918.1

中国版本图书馆 CIP 数据核字(2010)第 106448 号

教师教育新行动论丛

数论与密码

主　　编　杨思熳
策　　划　王　焰
责任编辑　吴海红
审读编辑　徐慧平　钱海丰
责任校对　徐慧平
装帧设计　卢晓红

出版发行　华东师范大学出版社
社　　址　上海市中山北路 3663 号　邮编 200062
电话总机　021-62450163 转各部门　行政传真 021-62572105
客服电话　021-62865537(兼传真)
门市(邮购)电话　021-62869887
门市地址　上海市中山北路 3663 号华东师范大学校内先锋路口
网　　址　www.ecnupress.com.cn

印 刷 者　上海商务联西印刷有限公司
开　　本　787×1092　16 开
印　　张　9.25
字　　数　169 千字
版　　次　2010 年 9 月第 1 版
印　　次　2010 年 9 月第 1 次
印　　数　2 100
书　　号　ISBN 978-7-5617-7838-8/O·210
定　　价　19.00 元

出 版 人　朱杰人

华东师范大学
“985 工程”哲学社会科学
“教师教育理论与实践”创新基地建设成果

教师教育新行动论丛

丛书主编：华东师范大学教师教育改革推进委员会

主　任：俞立中
副主任：庄辉明（常务）　陈　群

成　员：（以姓氏笔画为序）
丁　钢　方俊明　毕志毅　任友群　庄辉明　李学昌　杨　凯　吴　刚　吴庆麟　沐　涛
陆嘉星　陈　群　陈玉琨　周长江　周忠良　周南照　季　浏　范国睿　胡炳元　赵小平
赵中建　俞立中　祝智庭　聂幼犁　袁　雯　顾伟列　柴　俊　倪文锦　徐伯兴　徐斌艳
唐永华　唐安国　戚业国　崔允漷　谢安邦　谭　帆　戴立益

丛书策划：任友群

序

进入21世纪，世界各国都将提升教育质量确定为教育改革的重心，教师教育改革与创新更是成为重中之重。中国教师教育改革发展同样面临的一个核心问题，即如何把国家教师教育的战略导向和基础教育新课程改革对教师教育的要求，转化为教师教育改革实践的具体目标与措施，加快传统师范教育向现代教师教育的转变，培养造就一大批优秀教师和未来教育家。

自教师教育产生发展至今，源起于为教师提供教学法训练的学科教育，在教师培养与培训过程中一直充当着重要角色。自新中国建立以来，师范院校一直是教师教育的主阵地，因此，学科教育研究与实践的核心任务，就是研究基础教育，培养、培训中小学校教师。其遵循的一个核心原则是，对不同学科的教学规律的发现与运用，要与教育学的一般理论紧密结合起来，一般而言，教育学理论对于学科教育研究与实践具有指导作用，而学科教育反过来促进教育学理论的发展。

1986年，美国公布霍姆斯报告，新一轮教师专业化运动迅速兴起，“学科教学知识”概念应运而生。这一概念强调，学科知识既包括学科内容，也包括学科知识的逻辑结构，因此对学科知识结构的掌握，直接影响着教师传授知识的方法和效果。这就要求学科知识与教育学知识要在更深层次和更广范围上实现结合，从而对传统的学科教育理论提出了挑战。

但是，迄今为止，大多数学科教育研究与实践者仍然尊奉的是传统原则。基于各学科自身的知识逻辑，基于教师自身所需知识的逻辑结构，以及基于基础教育阶段各学科学习的认知规律和教学策略，尝试重新构建一个全新的学科教育理论框架，仍停留在一个讨论的层面。

2008年，全国学科教师教育论坛举行。教育部副部长陈小娅在论坛开幕式上作了重要讲话，要求从事学科教学研究与实践的教师，要以服务基础教育为导向，以强烈的责任感、使命感直面学科基础教育与教师教育改革的理论与

实践问题，积极开展学科教师教育的探索与创新，逐步建立起学科教师教育的研究共同体。

这样的期待，似乎并不仅仅意味着对学科教育研究与实践的激励。要改变目前学科教育在各师范院校的边缘化和研究队伍青黄不接等现状，除了各师范院校要重视学科教育的学科建设与师资队伍的建设外，学科教育也必须寻找到足以使其安身立命的新的合法性基础，即确立自身学科的理论基石与体系，积极探索形成自身的研究传统与优势。

我们也一起期待，教育界、科学界有更多的专家学者来推动和投身学科教育事业，提出更多的、更具体的理论与实践课题，为促进学科教育研究、实践和教师教育的可持续发展而共同努力。

2009年6月6日

前　言

近年来随着信息安全与密码学知识的日益普及和社会对此的需求，各高校数学系、计算机系乃至高中课堂陆续开设了相关课程。目前国内已出版了不少密码学的相关书籍。本书希望能为密码学尤其是公钥密码学及其所需要的数论知识提供一个简明而完备的入门教程，使学生了解数论的一些基础知识及其在现代信息理论和信息安全技术中的一些重要应用，拓展学生的数学视野，提高学生对数学的科学价值、应用价值的认识。

本书论述了公钥密码学的基本理论及实现，主要包括：RSA 密码体制、ElGamal 公钥密码体制、椭圆曲线公钥密码体制和数字签名。本书的特点之一，内容涉及面广，在有限的篇幅内，包含了必要的预备知识和较完备的数学证明；特点之二，用系统的数学方法讲述了公钥密码学的主要数学原理；特点之三，从算法的角度进行论述，对每个主要的理论结果给出其可编程的实际算法；特点之四，对目前理论和实践前景最好的椭圆曲线密码的实现，结合最新的国际研究进展（如 2009 欧密会论文）给出了浅显的介绍。本书的内容曾多次在华东师范大学数学系给本科生讲授。

本书可作为信息安全、数论及相关专业的研究人员、高等学校的教师和高年级学生的参考书，其部分内容也可作为信息安全、数论等专业的研究生的入门教材。

在本书的编写过程中，得到了我的研究生刘巍、齐璐璐、季君丽的协助，在此一并表示感谢。本书的编写得到了国家自然科学基金（批准号：10801050）和华东师范大学 985 课程建设专项基金的资助，特此感谢。

最后，笔者特别要感谢亲爱的妻子邢秀红和家人，是他们的支持使本书的完成成为可能。

杨思熳

2010 年 5 月

符 号 说 明

符号	说　明
$\mathbb{N}$	自然数集：$\mathbb{N}=\{1,2,3,\cdots\}$
$\mathbb{Z}$	整数集：$\mathbb{Z}=\{0,\pm n: n\in\mathbb{N}\}$
$\mathbb{Z}^+$	正整数集：$\mathbb{Z}^+=\mathbb{N}$
$\mathbb{Q}$	有理数集：$\mathbb{Q}=\left\{\frac{a}{b}: a,b\in\mathbb{Z}\text{且}b\neq 0\right\}$
$\mathbb{R}$	实数集：$\mathbb{R}=\{n+0.d_1d_2d_3\cdots: n\in\mathbb{Z}, d_i\in\{0,1,\cdots,9\}$且没有9的无穷序列出现$\}$
$\mathbb{C}$	复数集：$\mathbb{C}=\{a+b\mathrm{i}: a,b\in\mathbb{R}\text{且}\mathrm{i}=\sqrt{-1}\}$
$\mathbb{Z}/n\mathbb{Z}$	或记为$\mathbb{Z}_n$，模n的剩余类环；若n为素数，则为域
$(\mathbb{Z}/n\mathbb{Z})^*$	$\mathbb{Z}_n$中乘法可逆元(即，$\mathbb{Z}/n\mathbb{Z}$中与n互素的元素)构成的乘法群
F_p	p元有限域，其中p是素数
F_q	q元有限域，其中$q=p^k$是素数幂次
$\mathcal{K}$	域
$\mathcal{R}$	环
$\mathcal{G}$	群
$\lvert\mathcal{G}\rvert$	群$\mathcal{G}$的阶
$\sqrt{x}$	x的算术平方根
$\sim$	渐近等式
$\approx$	近似等式
∞	无穷

$\Rightarrow$	推出
$\Leftrightarrow$	等价
$\square$	证明结束符
$\|S\|$	集合 S 的基数
$\in$	属于
$\subset$	真包含
$\subseteq$	包含
$\bigstar$，$*$	二元运算
$\oplus$	二元运算(加法)
$\odot$	二元运算(乘法)
$f(x) \sim g(x)$	$f(x)$ 与 $g(x)$ 渐近相等
e_k	密钥
d_k	解钥
$E_{e_k}(M)$	加密过程 $C = E_{e_k}(M)$，其中 M 是明文
$D_{d_k}(C)$	解密过程 $M = D_{d_k}(C)$，其中 C 是密文
$f(x)$	x 的函数
f^{-1}	f 的逆
$\binom{n}{i}$	二项式系数
$\sum_{i=1}^{n} x_i$	和式：$x_1 + x_2 + \cdots + x_n$
$\prod_{i=1}^{n} x_i$	乘积式：$x_1 x_2 \cdots x_n$
$n!$	阶乘：$n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1$
kP	$kP = P \oplus P \oplus \cdots \oplus P$，$P$ 是椭圆曲线上的一个点
O_E	椭圆曲线 E 的无穷远点
e	超越数 $\mathrm{e} = \sum_{n\geqslant 0} \frac{1}{n!} \approx 2.718\,281\,8$
$\log_b x$	以 $b(b \neq 1)$ 为底 x 的对数：$x = b^{\log_b x}$
$\log x$	以 2 为底的对数：$\log_2 x$
$\ln x$	自然对数：$\log_{\mathrm{e}} x$
$\exp(x)$	指数函数：$\mathrm{e}^x = \sum_{n\geqslant 0} \frac{x^n}{n!}$
$a \mid b$	a 整除 b
$a \nmid b$	a 不整除 b
$p^\alpha \parallel n$	$p^\alpha \mid n$ 但 $p^{\alpha+1} \nmid n$

$\gcd(a, b)$	(a, b) 的最大公因子
$\mathrm{lcm}(a, b)$	(a, b) 的最小公倍数
$\lfloor x \rfloor$	小于等于 x 的最大整数
$\lceil x \rceil$	大于等于 x 的最小整数
$x \bmod n$	剩余：$x - n\left\lfloor \frac{x}{n} \right\rfloor$
$x \equiv y \pmod n$	x 与 y 模 n 同余
$x \not\equiv y \pmod n$	x 与 y 模 n 不同余
$[a]_n$	a 模 n 的剩余类
$\mathrm{ord}_n(a)$	整数 a 模 n 的阶
$\mathrm{ind}_{g,n}a$	以 g 为底 a 模 n 的指标；当 n 固定时，也记为 $\mathrm{ind}_g a$
$\pi(x)$	小于等于 x 的素数的个数：$\pi(x) = \sum_{\substack{p \leqslant x \\ p\text{为素数}}} 1$
$\phi(n)$	欧拉函数：$\phi(n) = \sum_{\substack{0 \leqslant k < n \\ \gcd(k, n) = 1}} 1$
$\lambda(n)$	Carmichael 函数：若 $n = \prod_{i=1}^{k} p_i^{\alpha_i}$，则 $\lambda(n) = \mathrm{lcm}(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \cdots, \lambda(p_k^{\alpha_k}))$
$\left(\frac{a}{p}\right)$	勒让德符号，其中 p 是素数
$\left(\frac{a}{n}\right)$	雅可比符号，其中 n 可以是合数
$O(\cdot)$	上界：$f(n) = O(g(n))$，若存在某一常数 c，使得 $f(n) \leqslant c \cdot g(n)$，$\forall n \in \mathbf{N}$
$O((\log N)^k)$	用位运算度量的多项式时间复杂性，其中 $k > 0$ 是常数
$O(\exp(c\sqrt{\log N \log\log N}))$	亚指数复杂性，$O(\exp(c\sqrt{\log N \log\log N})) = O(N^{c\sqrt{\log\log N/\log N}})$
$O(\exp(x))$	指数复杂性，有时记为 $O(e^x)$
ECC	椭圆曲线密码
ECDSA	椭圆曲线数字签名算法
ECDLP	椭圆曲线离散对数问题
DSS	数字签名标准
DLP	离散对数问题
RSA	Rivest - Shamir - Adleman

目　录

第一部分　密码学中的数论

第二部分　公钥密码学

第一部分

密码学中的数论

第一章　数论基础

本章介绍数论的基本概念和结果，取材自[4]. 目的在于为密码学中所需要的数论知识提供一个独立和自包含的讲述内容. 数论与抽象代数有着紧密的联系，特别是群、环、域理论. 群、环、域，尤其是有限域的理论在密码学和信息安全上起着重要的作用.

1.1　导　　言

整数有许多让人着迷的性质. 我们先通过著名的“哈代—拉马努金出租车牌照号”故事来了解什么是数论.

拉马努金(1887—1920)，印度最伟大的数学天才. 他从事椭圆函数、连分数以及无穷级数的研究，在解析数论方面作出了突破性的贡献. 尽管缺少正规的教育，但是在印度 Madras，他是有名的数学天才，他的朋友建议他把他自学得到的数论结果寄给英国的教授看. 1913 年 1 月，拉马努金给剑桥大学的数学家哈代写信，信中列出了他给出的一长串未证明的定理，并写道：“我没有受过大学教育，但是我完成了中等学校的课程. 在离开学校之后，我将可供我支配的业余时间用来做数学研究.”哈代和李特伍德看到信后都认为拉马努金是一个有数学天分的人，并决定把他带到剑桥. 拉马努金在 1914 年 4 月抵达剑桥. 不久，哈代就确信，拉马努金的天分与欧拉、高斯是同一级别的. 有一天，哈代到英国一家医院拜访拉马努金. 闲聊中提到来时乘坐的出租车牌照号是 1729，在他看来是一个相当无趣的数字. 拉马努金回答说它是一个很有趣的数，因为它是可以表示成两个正整数立方和并且表示方法恰有两种的最小正整数：$1\,729 = 1^3 + 12^3 = 9^3 + 10^3$. 接着哈代问拉马努金是否还可以告诉他四次方和问题的解. 拉马努金想了一会儿说，虽然他不知道具体的例子，但是他猜测这样的最小正整数一定非常大. 欧拉曾给出这样一个解：$635\,318\,657 = 59^4 + 158^4 = 133^4 + 134^4$. 拉马努金和哈代合作，在数论研究上取得了一系列重大的突破. 31 岁时拉马努金当选为英国皇家科学院院士. 李特伍德曾

说：每个整数都是拉马努金的朋友. 令人遗憾的是，1917 年 5 月，拉马努金染病；1919 年返回印度，1920 年去世，年仅 33 岁.

1.1.1 数论简介

数论主要是研究整数性质的理论，例如奇偶性、整除性、素性、堆叠性以及可积性等等. 以下我们简略讨论整数的这些性质.

(Ⅰ) 奇偶性

如果一个整数被 2 除余 1，则是奇数；反之，则为偶数. 如果把一个十进制的整数表示成二进制的形式，则它的奇偶性的判断就很简单了，我们只需观察它二进制最低的位上是 1(为奇)，还是 0(为偶). 若两个整数 m 和 n 同为奇，或同为偶，则称它们有相同的奇偶性，否则称它们有相反的奇偶性. 下面是关于整数奇偶性的一些为人所熟知的结论：

(1) 若两个数都是偶数，或都是奇数，则它们的和是偶数. 一般地，n 个偶数的和为偶数；若 n 为偶数，则 n 个奇数的和也为偶数；若 n 为奇数，则 n 个奇数的和为奇数.

(2) 若两个数有相同的奇偶性，则它们的差为偶数. 一般地，n 个偶数的差为偶数；若 n 为偶数，n 个奇数的差是偶数；若 n 为奇数，n 个奇数的差为奇数.

(3) 若两个数中至少有一个数是偶数，则它们的积为偶数. 一般地，若 n 个数中至少有一个数是偶数，则这 n 个数的积为偶数.

例 1.1.1 整数的奇偶性在纠错编码上的应用.

在计算机设计和通信上有一种简单的差错检测纠正方法——奇偶校验法. 设 $x_1x_2\cdots x_n$ 为一个二元的数字串(码字)，发送这一数字串(例如通过网络从一台电脑传到另一台电脑). 若码字中 1 的个数为奇数(偶数)，则添加一个比特 1(0)到码字的末尾. 这个附加的比特称为校验位. 设要传送的码字为

$$C = 1001011011,$$

则新的码字为

$$C' = 10010110110.$$

若通过传输 C' 变为 $C'' = 11010110110$ (码字中有一位错误)，则我们就知道所接收的码字在传输过程中出现了错误，因为

$$1+1+0+1+0+1+1+0+1+1+0 = 7 \bmod 2 \neq 0.$$

(定义记号 $a \bmod n$ 为 a 除 n 的余数). 不过，这个新码还不是纠错码(无法找到发生差错的位置). 如果把码字按行排列成一个矩形，对每一行、每一列用奇偶位校验，则在一个位上出现错误是可以被纠正的.