

<<数论>>

图书基本信息

书名：<<数论>>

13位ISBN编号：9787040348347

10位ISBN编号：7040348349

出版时间：2012-9-13

出版时间：高等教育出版社

作者：蔡天新

页数：200

字数：250000

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<数论>>

内容概要

《数论:从同余的观点出发》依据作者多年数论教学心得和研究成果写成。从同余的定义和观点出发,前五章依次讲述整除的算法、同余的性质、同余式理论、平方剩余、原根和 n 次剩余,后两章是有关素数幂模和整数幂模的同余式,不在通常的初等数论范畴却伸手可触。本书的另一特点是,每节内容都有引人入胜的补充读物,借此拓宽读者的知识面和想象力。这些读物或讲述了某一数论问题的初步知识,如佩尔方程和丢番图数组、阿廷猜想和特殊指数和、椭圆曲线和同余数问题、自守形式和模形式;或介绍了整数理论的新问题和新猜想,如完美数问题、格雷厄姆猜想、哥德巴赫猜想、abc猜想、 $3x+1$ 问题、华林问题、欧拉数问题、素数链问题、卡塔兰猜想、费尔马大定理等及其延拓。此外,本书重视语言描写,对背景知识和图表予以关注。

《数论:从同余的观点出发》可供数学及相关专业的大学生、研究生用作教材或参考书,也适合广大的业余数论爱好者和研究者阅读浏览。

<<数论>>

书籍目录

前言

第一章整除的算法

- 1.1 自然数的来历【完美数与亲和数】
- 1.2 自然数的奥妙【镶嵌几何与欧拉示性数】
- 1.3 整除的算法【梅森素数与费尔马素数】
- 1.4 最大公因数【格雷厄姆猜想】
- 1.5 算术基本定理【哥德巴赫猜想】

习题

第二章同余的概念

- 2.1 同余的概念【高斯的《算术研究》】
- 2.2 剩余类和剩余系【函数 $[x]$ 和 fxg 】
- 2.3 费尔马{欧拉定理【欧拉数和欧拉素数】
- 2.4 表分数为循环小数【可乘函数】
- 2.5 密码学中的应用【广义欧拉函数】

习题

第三章同余式理论

- 3.1 中国剩余定理【斐波那契兔子问题】
- 3.2 威尔逊定理【高斯未证的定理】
- 3.3 丢番图方程【毕达哥拉斯数组】
- 3.4 卢卡斯同余式【覆盖同余式组】
- 3.5 素数的真伪【素数之链】

习题

第四章平方剩余

- 4.1 二次同余式【高斯环上的整数】
- 4.2 勒让德符号【表整数为平方和】
- 4.3 二次互反律【 n 角形数与费尔马】
- 4.4 雅可比符号【阿达马矩阵和猜想】
- 4.5 合数模同余【正十七边形作图法】

习题

第五章原根与 n 次剩余

- 5.1 指数的定义【埃及分数】
- 5.2 原根的存在性【阿廷猜想】
- 5.3 n 次剩余【佩尔方程】
- 5.4 合数模的情形【丢番图数组】
- 5.5 狄利克雷特征【三类特殊指数和】

习题

第六章素数幂模同余

- 6.1 伯努利数与多项式【库默尔同余式】
- 6.2 荷斯泰荷姆定理【椭圆曲线】
- 6.3 拉赫曼同余式【同余数问题】
- 6.4 一类调和和同余式【自守形式和模形式】

第七章整数幂模同余式

- 7.1 拉赫曼同余式推广【abc猜想】
- 7.2 莫利定理及推广【新华林问题】
- 7.3 雅可布斯坦定理推广【新费尔马问题】

<<数论>>

7.4 多项式系数同余【多项式系数非幂】

10000 以下素数表

参考文献

章节摘录

版权页：插图：需要指出的是，密钥 e ， N 是可以公开的，只要他保存好解钥 d 。

任何人都可以按上述加密程序向他发送密码，只有他本人可以读出送来的信息，而其他人要想解出几乎不可能。

因为要想求出 d ，就必须知道 $\phi(N)$ ，那就需要知道 N 的素因数 P, q 。

当 P, q 的位数足够大，比如超过100位，按照现有的数学方法，即使是利用最高级的计算机，也不可能有限的时间内求出 $\phi(N)$ 的值，因而不可能知道 d 。

随着双钥密码体系的建立，使用了多年的单钥密码体系就被弃用了。

RSA不仅保密性能超强，且可以让很多客户使用，这是因为 e 和 $\phi(N)$ 都足够大，可以有很多对 e_i, d_i ，满足 $e_i d_i \equiv 1 \pmod{\phi(N)}$ ， $i=1, 2, \dots$ 。

可是，随着时间的推移，密码学专家不断想出新的招数来解破RSA密钥，办法是将问题分交给不同的计算机去做。

他们想出的新方法有二次筛法、数域筛法、椭圆曲线算法，等等。

其中二次筛法是利用二次剩余和连分数的技巧来分解整数。

不过目前，还没有真正威胁到RSA体制，即大数分解方案的安全性。

这里面有个原因，虽然计算机的性能越来越好，解密的方法似乎变得容易起来。

不过与此同时，可求得的大素数位数也越来越高，又可以用来设置保密性更强的密钥。

20世纪90年代以来，美国数学家利用离散数学中Hash（散列）函数来设计密码体制，取得了非常好的效果，在政府和金融机构应用极广。

比如1991年，RSA中的R——里维斯设计了所谓MD5算法，被认为坚不可摧。

可是到了2004年，这个算法却被中国数学家王小云（1966-）破解。

次年，她又与美籍华裔计算机理论家姚期智（1946-）夫妇合作，破解了美国国家安全局设计的国际通用的SHA—1算法，轰动了世界。

这些结果表明，电子签名从理论上讲是可以伪造的。

以上MD和SHA分别是信息摘要(Message-Digest)算法和安全散列算法(Secure Hash Algorithm)的简称。

除了应用于密码学以外，数论还可以用在纠错码(error correcting code)上，这是一种在纠错过程中能自动进行检错和纠正差错的代码。

例如，在每一套录音设备里，之所以能精确地复制声音，原因就在于它有纠错码。

无论是CD产品还是手机，都需要给声音编码，这方面得益于数论在纠错码中的应用。

<<数论>>

编辑推荐

《数论:从同余的观点出发》可供数学及相关专业的大学生、研究生用作教材或参考书,也适合广大的业余数论爱好者和读者阅读浏览。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>