文章编号：1672-5913(2022)03-0000-00　　中图分类号：G642

初等数论教学及其在密码学中的应用探讨

程庆丰[1]，汪　定[2, 3]，张卫明[4]

（1. 战略支援部队信息工程大学 四院，河南 郑州 450001
2. 南开大学 网络空间安全学院，天津 300350
3. 天津市网络与数据安全技术重点实验室，天津 300350
4. 中国科学技术大学 网络空间安全学院，安徽 合肥 230027）

摘要：初等数论作为网络安全和密码学专业的基础课程，在密码人才培养中发挥着重要的作用。本文在已有相关研究成果基础上，通过整理国内外相关的数字电子资源，较为全面地介绍初等数论知识在密码学领域的各种应用情况，并针对网络安全和密码学等专业人才培养过程中对数论知识的不同需求，给出了初等数论教学和应用的几点建议。

1　背景

当前万物互联的时代，网络应用发展处于快速爆发阶段，云计算、边缘计算等新型网络应用不断涌现。网络的发展形势，对计算机专业、数学专业、网络安全专业、密码专业等学科的人才培养提出了新的要求。2019 年，文献 [1] 探讨了信息安全专业人才课程建设、思维方式培养，提出了针对性的解决方案。同年，文献 [2] 分析了网络空间安全人才需求特点，提出了很多的建设性建议和对应的改革措施。2020 年，文献 [3] 深入探讨了新形势下理工学科的人才培养和学科建设，提出了人次培养、科学研究等多方面的改革建议。与此同时，2020 年 1 月 1 日正式开始实施《中华人民共和国密码法》，极大促进了国家各个领域对网络安全和密码人才的需求。

高质量密码人才的培养需要高水平密码学科的建设。众所周知，密码学是涉及计算机、通信、数学等多学科交叉的学科专业，数学特别是数论在其中发挥着基石的作用。数论经过几千年的历史发展，大致可分为初等数论、计算数论、解析数论、代数数论等分支，其中初等数论是数论中的基础部分，在密码学等领域有着广泛而重要的应用，其内容对于网络安全人才和密码人才是应该必备的基础知识。以 11 所一流网络空间安全学院为代表，国内很多高校的网络安全专业、数学专业、密码专业都开设了相应的初等数论或与初等数论内容相关的课程。初等数论中很多的基本概念和知识点较为容易理解，可以激发学生的学习兴趣，但是解决相关的初等数论问题或用于实践是具有一定难度的，特别是初等数论中的一些困难问题还是构建很多密码体制的安全基础。

国内学者对数论知识在密码学中的应用进行了很多的研究，积累了丰富的研究成果。文献 [4] 以经典的古典密码、RSA 密码、概率加密为例介绍了数论知识在密码学中的应用；文献 [5] 指出应该对高师数论教学进行改革，引入素性判定、整数分解等密码学知识，开拓学生视野；文献 [6] 以背包密码和 RSA 密码为例探讨了数论在密码学中的应用情况；文献 [7] 首先介绍了数论中的一些问题，比如整数分解、离散对数计算等，然后以 Diffie-Hellman 密钥交换协议和 ElGamal 密码体制等为例给出了数论在密码设计中的应用情况；文献 [8] 探讨了欧几里得算法在密码学中的应用。；文献 [9] 介绍了数论变换在公钥密码体制 NTRU 中的应用情况；文献 [10] 探讨了数论知识在密码学中的编程应用与算法优化问；文

作者简介：程庆丰，性别，职称，研究方向为，qingfengc2008@sina.com；汪定（通信作者），性别，职称，研究方向为，wangding@nankai.edu.cn。

献 [11] 简要总结介绍了初等数论知识在密码学中的应用情况；文献 [12] 则专门介绍了中国剩余定理在密码学中数字指纹和叛逆者追踪领域的应用；文献 [13] 也简要介绍了初等数论知识在数学竞赛和密码学中的应用情况；文献 [14] 利用二次剩余知识构造了一种基于多项式的加密体制。

随着当前密码技术的发展，对密码学相关课程的教学改革很有必要。当前已有数论在密码学中应用的研究成果，有待进一步全面梳理和加强。

2　初等数论在密码学中的应用

初等数论课程讲授的都是数论中较为基础的一些知识，当前国内较为经典的初等数论著作很多 [15-21]，所覆盖的内容主要包括了整数的理论、不定方程、同余式、数论函数、二次剩余和高次剩余、连分数、原根和指数等知识，并且不同的高校根据各自特点在讲授过程中有针对性的进行了内容筛选，同时根据学生实际情况增加了实践性编程环节的锻炼。国内学者对于这些初等数论知识内容在密码学中的应用研究情况在前面已经做了简要介绍。另外，国内学者还以著作方式对初等数论在密码学中的应用进行了研究（见表 1）。

表 1　国内数论与密码相关著作

序号	书名	作者	出版社
1	公钥密码学的数学基础	王小云、王明强、孟宪萌	科学出版社
2	密码学与数论基础	于秀源、薛昭雄	山东科学技术出版社
3	数论与密码	杨思熳	华东师范大学出版社
4	初等数论及其在密码学中的应用与 Maple 实现	游林	科学出版社
5	初等数论及其在信息科学中的应用	朱萍	清华大学出版社
6	数论与有限域	董丽华、胡予濮、曾勇	机械工业出版社
7	数论与应用	纪建	清华大学出版社
8	数论基础及其应用	沈忠华	科学出版社
9	密码学及信息安全基础	陈小松	清华大学出版社
10	信息安全数学基础：算法、应用与实践	任伟	清华大学出版社

与国内初等数论在密码学中应用研究情况类似，W. Stein、N.Koblitz、B. Hutz 等国外学者也对初等数论在密码学中的应用进行了广泛的研究，并给出了很多的著作成果，表 2 列出一些英文著作。

表 2　国外数论与密码相关著作

序号	书名	作者	出版社
1	Elementary Number Theory:Primes, Congruences,and Secrets	W. Stein	Springer
2	A Course in NumberTheory and Cryptography	N.Koblitz	Springer
3	An Experimental Introduction to Number Theory	B. Hutz	AMS
4	An Introduction to Number Theory with Cryptography	J.S.Kraft, L.C. Washington	wCRC
5	Elementary Number Theory and Its Applications	B. Goddard,K. H.Rosen	Pearson Addison–Wesley
6	Stream Ciphers and Number Theory	T.W. Cusick, C. Ding, A. Renvall	Elsevier
7	The Mathematics of Ciphers	S.C. Coutinho	A K Peters
8	Elementary Number Theory with Applications	T. Koshy	Elsevier
9	Introduction to Modern Number Theory	Y.I. Manin, A.A. Panchishkin	Springer
10	Primality Testing andInteger Factorizationin Public–KeyCryptography	S.Y. Yan	Springer
11	Factorization and Primality Testing	D.M. Bressoud	Springer
12	Elementary Number Theory, Cryptography and Codes	M.W. Baldoni, C. Ciliberto, G.M.P. Cattaneo	Springer

从表 1 和表 2 所列的著作中可以发现，初等数论中各部分知识内容在密码学中都有着广泛的应用。下面以素数、欧几里得算法、梅森素数、丢番图方程、同余、中国剩余定理、二次剩余和高次剩余、原根和指数、连分数等一些知识点为例，对初等数论在密码学中的应用进行介绍。

素数：素数在公钥密码体制中有着重要的地位，在经典的 RSA、ElGamal 等公钥密码体制中都发挥着重要的作用。素数的素性测试和生成也

一直是密码学中研究的重要内容。此外，素数在伪随机序列中也有着重要作用 [22]。

欧几里得算法：欧几里得算法是用来求解 2 个整数最大公因数的算法，可用来解决线性同余方程和线性丢番图方程。该算法在首届全国密码高效数学挑战赛的赛题三中有着巧妙的应用，利用该算法可以很容易的破解赛题 RSA 加密体制的参数，进而求出对应的明文。

梅森素数：梅森素数是一种形如 2p-1（其中 p 是素数）形式的素数。通过互联网梅森素数搜索项目 (Great Internet Mersenne Prime Search, GIMPS) 可以用来寻找最大素数，并且梅森素数在构造公钥密码系统 [23] 以及认证方案等领域有着应用。

丢番图方程：丢番图方程是数论的一个重要分支，可以用来构建公钥密码体制 [24]。

同余：同余是初等数论中一种基本的运算，当前大部分密码体制都是在同余意义下构建的。特别是古典密码中的凯撒密码、维吉尼亚密码等都是基于同余知识直接构造的。此外，同余运算在序列密码和哈希函数领域也有着广泛的应用。

中国剩余定理：中国剩余定理是我国古代数学中的宝贵成果，在现代密码学中秘密共享、素数搜索、密钥流生成器、数字签名等领域都有着广泛的应用。文献 [25] 中对中国剩余定理在计算、编码和密码学中的应用进行了总结和全面的介绍。

数论函数：初等数论中一些数论函数在密码学中也有着广泛应用，比如欧拉函数在 RSA 密码中的应用、麦比乌斯函数在序列密码中的应用等。

二次剩余和高次剩余：二次剩余是初等数论中的基本概念，在密码学中可以用于大整数分解、构造公钥密码系统等，较为经典的应用包括了 Rabin 加密、GM 加密等。高次剩余也可以用来构造数字签名方和公钥密码体制。

原根和指数：原根和指数在密码学中应用很多，较为经典的包括了 Diffie-Hellman 密钥交换协议、ElGamal 加密、DSA 数字签名等。

连分数：连分数是数的一种重要表示方法，可以用来进行整数分解，在公钥密码体制 RSA 的低解密指数攻击中具有一定的作用。

3 初等数论教学中的几点建议

初等数论在国内不同学校、不同专业中开设的学时并不相同，一般是在 30 学时至 60 学时之间。初等数论知识与初高中数学联系较为紧密，较为容易看懂和理解，但当实际解题时常常是比较困难并耗费时间，这也是初等数论课程一个非常显著的特点。针对初等数论课程特点，在初等数论教学中应注重启发式教学，引导和鼓励学生加强自主学习，不仅要用好课上时间，更需要课下投入时间自主进行数论知识的学习以及开展编程实践，逐步锻炼将初等数论理论知识转化为实践的能力。实际上，初等数论知识的学习和应用几乎贯穿网络空间安全专业和密码学专业整个人才培养周期，结合本科生导师制会发挥更好的学习效果。因此，从课上理论学习、课下自主学习、课程编程实践与应用、多种方式指导答疑等角度，提出以下几点建议（如图 1 所示）。

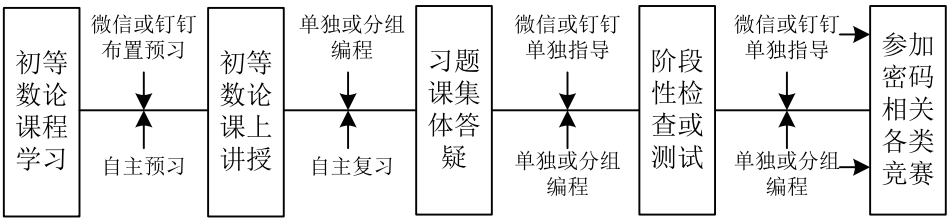

图 1 数论的学习与应用实践

1）初等数论网络资源方面。

初等数论或其部分主要内容虽然在国内很多高校都有开设相关的课程，但是网络课程资源方面还不是很丰富。腾讯课堂、壹课堂网站上的一些初等数论课程授课视频，已经是国内为数不多的较为全面和不错的学习资源了。不过互联网上有着丰富的电子图书资源，通过初步整理发现，互联网上可以搜索到将近 200 多本初等数论著作以及包括较多初等数论知识的密码学著作。这方面对学生应该加以引导，鼓励自主搜索网络资源，筛选适合辅助初等数论学习的相关电子资料。

2）初等数论知识编程方面。

与数学专业的数论学习侧重点不同，网络安

全专业和密码学专业的学生在学习初等数论理论知识的同时，还需要在编程实践方面进行更多的锻炼。初等数论内容中很多知识点也特别适合编程实现，比如欧几里得算法、厄拉多塞筛法、素性测试、中国剩余定理、指数等。学生的编程实践可分为课上和课下，常见组织方式包括了单人任务、分组任务以及分组对抗等方式，通常课下编程投入的精力多少是实践能力提升的关键。在编程实践过程中，要加强阶段引导和检查，鼓励学员自主通过搜索网络资源提升编程效率，更好的利用较好的开源程序网站，比如开源程序网站 Github 上就包含了使用 Java、C、Python 等不同编程语言实现的各种数论算法以及其在密码学相关应用中的算法。

3）初等数论知识应用方面。

通过实践方面的编程，学生具备了初步的数论实践能力。在此基础上，组织和鼓励学生参加国内密码和安全相关的竞赛，可以更好的帮助学生理解初等数论知识的理论与应用。当前，国内开展的全国密码技术竞赛、全国密码数学挑战赛、全国大学生信息安全竞赛等可以很好的帮助学生将初等数论知识用来解决实际问题、设计安全产品。另外，各类网络攻防夺旗赛 (Capture The Flag，CTF) 的很多赛题中都涉及初等数论的一些知识，学生通过参加这类 CTF 竞赛不仅可以更好的理解初等数论知识，而且可以提升综合的网络技能水平。

4　结　语

当前网络安全和密码应用的快速发展，对网络安全和密码人才有了更多的需求，对网络安全和密码学专业相关的课程以及知识内容学习提出了更高标准。通过总结国内外相关方面的文献和著作，给出了国内外学者关于初等数论和密码学方面较好的著作成果。然后，从初等数论知识内容的课堂理论学习、课程内容的编程实践到逐步深化的知识应用和技能提升等方面，简略的探讨了如何帮助学生更好的学习初等数论知识及具备较好的编程能力。

参考文献：

[1] 杜瑞颖, 张焕国, 傅建明, 等. 网络空间安全大类下的信息安全专业人才培养[J]. 网络与信息安全学报, 2019, 5(3): 25-30.
[2] 翁健, 魏林锋, 张悦.网络空间安全人才培养探讨[J]. 网络与信息安全学报, 2019, 5(3): 44-53.
[3] 李凤华, 李晖.新形势下理工门类学科建设内涵与学科评估导向[J]. 网络与信息安全, 2020, 6(1): 1-10.
[4] 曹珍富, 潘家宇. 数论在密码学中的应用[J]. 佳木斯教育学院学报, 1988, 4(1): 16-26.
[5] 于秀源. 对高师数论课程教学改革的几点看法[J]. 数学教育学报, 1996, 5(1): 82-85.
[6] 王国俊. 数论在密码学中的应用[J]. 工程数学学报, 2002, 19(1): 14-20.
[7] 颜松远. 数论及其应用[J]. 数学的实践与认识, 2002, 32(3): 486-508.
[8] 陈良臣, 芦东昕, 李春葆. Euclid算法及扩展在密码学中的研究和应用[J].计算机技术与发展, 2006, 16(11): 156-159.
[9] 孙琦, 彭国华, 朱文余, 等. 数论变换在NTRU公钥密码体制中的应用[J]. 通信技术, 2008, 41(7): 177-182.
[10] 吴晓刚.数论在密码学中的应用与算法的优化实现[J].兴义民族师范学院学报, 2010(3): 95-98.
[11] 祁兰. 初等数论在密码学中的应用[J]. 宝鸡文理学院学报(自然科学版), 2014, 34(2): 20-21.
[12] 杨坤伟, 李吉亮, 张瑞丽. 中国剩余定理在密码学中的应用研究[J]. 计算机技术与发展, 2014, 24(1): 238-241.
[13] 张本慧, 崇金凤, 卓泽朋. 初等数论在数学竞赛及密码学中的应用[J]. 赤峰学院学报(自然科学版), 2018, 34(12): 13-15.
[14] 罗婧, 范自强. 基于二次剩余的密钥体制的构造[J]. 佳木斯大学学报(自然科学版), 2020, 38(1): 168-170.
[15] 华罗庚. 数论导引[M]. 科学出版社, 1957.
[16] 陈景润. 初等数论(I II III)[M]. 哈尔滨工业大学出版社, 2012.
[17] 熊全淹. 初等整数论[M]. 湖北人民出版社, 1982.
[18] 柯召, 孙琦. 数论讲义(上册)[M]. 高等教育出版社, 2001.
[19] 闵嗣鹤, 严士健. 初等数论(第三版)[M]. 高等教育出版社, 2003.
[20] 于秀源, 瞿维建. 初等数论[M]. 山东教育出版社, 2004.
[21] 潘承洞, 潘承彪. 初等数论(第三版)[M]. 北京大学出版社, 2013.
[22] 王小云. 素数在密码中的几点应用[J]. 通信保密, 1993, 1: 31-35.
[23] Aggarwal D, Joux A, Prakash A, et al. A new public-key cryptosystem via mersenne numbers[C]//In Proc. of CRYPTO2018, LNCS 10993, 2018: 459-482.
[24] 孙琦. 用丢番图方程构作公开钥密码[J]. 四川大学学报(自然科学版), 1991, 28(1): 15-18.
[25] Ding C, Pei D, Salomaa A. Chinese remainder theorem: Applications in computing, coding, cryptography [M].World Scientific, 1996.

（编辑：史志伟）