教书札记 (一) —— 初等数论

冯克勤

冯克勤, 1941 年 10 月生于天津市宁河县, 1964 年中国科技大学数学系毕业, 1968 年中国科技大学代数与数论方向研究生毕业, 1973—2000 年在中国科技大学任教, 1985 年任教授和博士导师。2000 年至今任清华大学数学科学系教授。研究方向为代数数论和在编码及信息安全中的应用, 获 1991 年陈省身数学奖等奖项。现为 *International Journal of Number Theory*、中国科学 (数学卷) 等刊物编委。

我从 1973 年开始在中国科学技术大学 (下称 “科大”) 为工农兵学员教微积分, 在科大教了 27 年书。2000 年来到清华大学又教了 9 年。其中教的最多的课是本科生的初等数论、抽象代数和研究生的 (本科生高年级也可选修) 代数数论、代数几何、群表示理论和代数编码理论。教书时间多了总有些体会和想法, 谈不上经验。我把这些想法写出来, 目的是与诸位同仁切磋和共勉, 也许对刚走上教学岗位的年轻教师有些启发和帮助。先从初等数论谈起。

我主张大学数学系一年级的学生学一点初等数论

1977 年, 我在科大为文革后恢复高考的第一届学生在第一学期教初等数论。直到今天, 科大数学系本科生仍把初等数论作为第一学期必修课。2000 年我来到清华大学, 清华的同仁认可这种做法, 便又在清华坚持了 9 年 (是全校本科新生的选修课, 人数 150 名)。我主张大学新生学一点初等数论是基于以下三点考虑。

第一, 希望中学生来到大学之后, 继续保持对于数学的认知和亲切感。目前大学生一年级的数学课是两个重要的基础课: 微积分和线性代数。前者是研究变化的数学, 包括极限、连续、微分和积分等一系列新的概念, 对于以形式逻辑为主的中学数学而言, 是相当大的跳跃。后者有向量空间 (子空间和商空间)、线性相关和无关、线性变换、基和秩等一系列比中学抽象的概念和推导。不少新生感到大学数学和中学数学差别太大, 以至于有些中学数学成绩很好的学生, 到了大学感到不适应甚至对学数学失去兴趣。初等数论是中学生比较熟悉的, 不少学生在中学受到过课外训练, 对初等数论抱有兴趣。在刚入大学时上这样一个短课, 对他们在心理上有好处。

第二, 为今后学习抽象代数打下基础。

抽象代数一向是学生感到困难的课。在培养抽象思维和推理训练中, 一定要在心目中有大量的例子, 对抽象事物有直观的感受。这些例子主要来源两个方面, 一个是线性代数中的向量空间加法群, 线性映射的像空间和核, 子空间和商空间, 线性群和它的各种乘法子群是非交换群的典型例子。另一个来源为初等数论。整数模 m 的同余类给出群的陪集概念, 整数加法群 $\mathbb{Z}$ 模 m 的商群 $Z_m = \mathbb{Z}/m\mathbb{Z}$ 是所有有限循环群的样板, 整数环 $\mathbb{Z}$ 是主理想整环的最基本例子, 有限环 Z_m 的乘法可逆元全体是有限交换群的重要例子, 原根和指数就是循环群的生成元和元素的阶。当 m 为素数 p 时, Z_p 给出有限域的一批例子。同学通过这些具体例子熟悉概念、规律和思考方式, 是将来真正学好抽象代数的必要条件。否则, 抽象代数对于学生是空洞和玄妙的。

第三, 数论是有用的。

高斯说, 数论是数学的皇后, 有一种纯粹和高雅的气质。但是从 1960 年代数字通信技术发展以来, 数论成为通信的重要工具, 也同时扮演得力仆人的角色。有限域 Z_p (甚至是最简单的二元域 Z_2) 成为数字通信的信息载体。1976 年密码学产生公开密钥体制重大变革。目前使用的两种公钥都来源于初等数论 (基于欧拉定理和大数分解的 RSA 体制和基于原根指数的离散对数体制)。费马的许多猜想在通信中都出人意料地得到应用。这些真实的故事容易激发学生的学习兴趣。

初等数论的教法

第一节课总是要介绍初等数论的内容、历史和它的地位。初等数论是研究整数的性质和方程 (组) 整数解 (和有理数解) 的学问。它历史悠久, 古代中国的贡献有勾股定理和中国剩余定理。古希腊的数论得到很大发展并有重要的地位, 17 世纪和 18 世纪的数论中心是法国。费马 (1601—1665) 的一系列猜想引起欧拉 (1707—1783) 的兴趣, 觉得值得他花时间好好研究一下整数的性质, 随后高斯 (1777—1855) 也参加进来。经过他们二十余年的努力, 费马关于整数的诸多猜想均被 (肯定或否定地) 解决, 只有一个 1637 年费马提出的猜想直到 1994 年才由怀尔斯证明。欧拉和高斯在研究费马各种猜想的过程中系统发展了整数的性质, 从而在 18 世纪末形成了初等数论这一数学分支。这个课就是介绍两百年前的这段故事, 讲述欧拉和高斯是如何作数学的, 在研究整数时引进了哪些思想和方法, 得到哪些重要结果, 他们是如何解决费马诸多猜想的, 还有哪些重要问题没有解决, 遇到什么困难。

初等数论是近代和现代数论的源头。欧拉和高斯等人在数论上的贡献不仅解决了费马一系列猜想, 更重要的是他们的创新思想和方法把数论研究推进到一个新的阶段, 开创了用代数方法研究数论的新学科 —— 代数数论。与此同时, 另一个德国大数学家黎曼 (1826—1866) 在研究素数分布时采用了解析方法, 开创了解析数论, 这使得在 19 世纪之后数论中心由法国转到德国。经过希尔伯特等人的努

力, 一直到二战前夕, 迎来了数论发展的一个辉煌时期。另一方面, 1960 年代之后, 初等数论和近现代数论成果在信息科学中得到广泛而深刻的应用, 这些应用也为数论研究本身注入新的活力。

每年的新生中都有不少人在竞赛培训班中受到过数论的训练, 他们大都喜爱数论。所以我对他们说, 我相信你们当中有些人做数论题的技巧比我强, 有许多数论问题我也不会做, 当然我们可以相互讨论。比如我在叙述历史时讲到费马的一个猜想: $F_n = 2^{2^n} + 1 \ \ (n > 0)$ 均为素数, 而欧拉发现 $F_5 = 641 \times 6700417$, 从而否定了这个猜想。然后说, 你们当中哪些人, 如果在我介绍欧拉的工作时, 知道他是如何得到 F_5 的因子 641, 我可以把平时成绩加 10 分 (平时成绩主要是习题分数以及课下和我主动讨论的情况, 占总成绩的 60%)。我在清华大学讲完第一节课时, 连续三年每年都有两位同学下课告诉我, 他们知道用欧拉定理可推出 F_5 的素因子一定是 64 的倍数加 1, 有一位同学居然知道高斯的二次互反律, 并由此可知 F_5 的素因子为 128 的倍数加 1。这使我非常兴奋, 当场加以表扬。但我也同时说, 这个课的重点不是解数论难题的各种技巧, 而是讲解数论思想和一般方法, 描述欧拉和高斯的工作如何引导数论研究到一个新的高度, 介绍数论在通信中一些应用, 以整数为例子特别强调代数的研究方法, 对于今后学习抽象代数是有益的。所以, 有不少数论修养很好的学生也还是坚持听课, 能够进一步开阔眼界。当然, 他们在这个课上容易得到学分, 我猜想也是一个原因。

举一个代数化教学的例子: 研究二元一次不定方程 $ax + by = n$ 的整数解, 其中 a 和 b 是给定的非零整数解。问题是: 对于哪些整数 n, 此方程有整数解 (x, y)? 如果有解, 能否把所有的解都表示出来? 欧拉和高斯在研究这个问题时, 不是对每个 n 来讨论此方程, 而是考虑使此方程有整数解的所有整数 n 组成的集合 S。研究集合 S 的性质, 发现: (1) 如果 n 和 m 属于 S, 则 $n \pm m$ 也属于 S。(2) 如果 n 属于 S, 则对每个整数 a, an 也属于 S。再用带余除法便可得到 S 是一个正整数 d 的全部倍数组成的集合。进而再证明 d 就是 a 和 b 的最大公因子 (a, b)。于是: 上面方程有整数解当且仅当 n 是 (a, b) 的倍数。研究集合 S 的代数结构的思考方式对中学生是一种提高, 它的本质是说: 整数环是主理想整环。这种训练为他们今后学习抽象代数打下实在而直观的基础。至于把全部 (无穷多个) 解都表示出来, 则用到整除的一些性质即可。

上面谈到的带余除法, 是小学生都知道的。但是要真正懂得带余除法并且成为一种思考方式和自觉运用的工具, 则是数论的修养问题。比如说, 两个非零整数的公因子当然小于它们的最大公因子, 只有意识到公因子是最大公因子的因子的时候, 才算是学到了数论思考方式。同样地, 非零整数的正公倍数都不仅大于它们的最小公倍数, 而且是最小公倍数的倍数。又比如说, 当整数 a 和 m 互素时 $(m \geq 2)$, 满足 $a^d \equiv 1 \pmod{m}$ 的正整数 d 是存在的, 并且由欧拉定理, 最小的正整数 d (叫做 a 模的 m 阶) 是欧拉函数 $\varphi(m)$ 的因子。而且, 满足 $a^n \equiv 1 \pmod{m}$ 的每个整数 n 都是阶 d 的倍数。这些结论都是基于带余除法, 将来在抽象代数中讲到有限群中元素阶的类似结果时, 不仅感到很自然, 而且知道如何证明。

唯一因子分解定理是初等数论的基石, 是研究数论问题的基本工具, 也是一个漂亮的理论结果。但是对于一个工程师来说, 给出一个很大的整数, 如费马数 $F_{20}=2^{2^{20}}+1$, 是否有办法把它的具体分解式列出? 大数分解好算法的研究也有很长的历史。特别是 20 世纪 70 年代人们用大数分解设计公开密钥以来, 这个问题引起更多数学家的兴趣。人们在改进大数分解算法过程中采用了非常高深的数论知识。尽管算法不断改进, 但是仍然没有得到可以实用的算法 (用计算复杂性的语言, 仍没有得到大数分解的多项式算法)。比如说, 目前已经完全分解的费马数是 $F_n(n\leq 11)$, 人们找到 F_{12} 的一些素因子, 但至今没有把 F_{12} 分解完毕。正是因为大数分解的困难性, RSA 公钥体制目前在保密事业中已被实际应用。这是一个典型的例子, 说明数学家和工程师分别在理论和实际应用领域具有不同的价值观念和审美标准。在理论方面, 费马的一个猜想是说: 每个素数 $p\equiv 1 \pmod 4$ 都可表成两个整数的平方和, 即当素数 p 被 4 除余 1 时, 方程 $x^2+y^2=p$ 必有整数解 (x,y) (当 $p\equiv 3 \pmod 4$ 时, 利用同余式理论易知 $x^2+y^2=p$ 无整数解)。这个猜想由欧拉证明, 而高斯则考虑更一般的 “平方和” 问题: 对于哪些正整数 n, 方程 $x^2+y^2=n$ 有整数解? 在课上我主要讲这个问题的初等解法, 但是要展示高斯解决时采用的创新思想: 如果把方程放在比整数更大一些的范围去考虑, 则这个方程可表示成 $n=(x+yi)(x-yi)$, 其中 $i=\sqrt{-1}$。高斯考虑由 $a+bi$ (a 和 b 为整数) 组成的集合 $\mathbb{Z}[i]$ (后人叫作高斯整数环), 这个集合可进行加减乘运算, 叫作是环 (ring)。而方程表明: 若 $x^2+y^2=n$ 有整数解, 则 n 可写成高斯整数环中的两个高斯整数 $x+yi$ 和 $x-yi$ 的乘积。于是, 高斯便考虑: 在 $\mathbb{Z}[i]$ 中是否有和通常整数环 $\mathbb{Z}$ 类似的唯一因子分解定理? 这首先需要定义 $\mathbb{Z}[i]$ 中哪些数是素数, 然后高斯证明了环 $\mathbb{Z}[i]$ 也有唯一因子分解性。基于此, 高斯不仅完全解决了对哪些 n, 方程 $x^2+y^2=n$ 有整数解, 而且还给出方程整数解个数的漂亮公式。高斯还考虑诸如 $x^2-30y^2=n$ 等其他方程的整数解问题, 需要研究由 $x+\sqrt{30}y$ (x 和 y 为整数) 组成的环。高斯发现这个环 $\mathbb{Z}[\sqrt{30}]$ 不仅没有唯一因子分解性质, 还有其他的困难。这促使高斯发明了一系列新的代数概念和方法, 这就是代数数论的起点, 值得向学生介绍一下。

初等数论中还有一些内容是标志性的。比如说把模 m 的同余类看成是一个元素, 在 m 个同余类组成的集合中自然地引入加减乘运算, 从而形成有限交换环 $Z_m=\mathbb{Z}/m\mathbb{Z}$, 这是一个思想的飞跃。要让学生学会把初等数论许多结果采用 Z_m 中的语言加以叙述和证明, 这种训练对将来学抽象代数是有益的。又比如中国剩余定理也会使学生兴奋, 它给出一次同余方程组的解法。程大位对于《孙子算经》中 “物不知其数” 问题编了解法口诀, 要让学生自己推出口诀中的数 (70, 15, 21, 105) 是如何得到的。这个定理在抽象代数中已被推广成非常一般的形式, 但是这种一般形式在所有中外书籍和文献中仍然称之为中国剩余定理 (Chinese Remainder Theorem, CRT)。初等数论的高峰是高斯的二次互反律。高斯非常喜欢他的这个结果, 给出了 6 种证明。希尔伯特在 1900 年提出的 23 个著名数学问题中, 第 9 个问题就是: 高斯二次互反律如何推广? 在初等数论课中, 同学会看到二次互反律结果和高斯证明都是漂亮的, 也可用来解决一些问题, 但还不能理解:“近

代和现代数论的许多成就中都可以找到高斯二次互反律的影子”。我在 2001 年教过的学生中, 有 5 位毕业后到法国学习高深的数论, 他们已有人博士毕业后在美国普林斯顿大学和哥伦比亚大学就职。2008 年夏回国欢聚时, 他们还记得我在初等数论课中关于高斯二次互反律所说的话。在聚会上我告诉他们说: 你们现在数论懂得比我多, 对于高斯二次互反律的理解已经比我要深刻了。

以上主要讲的是数论课上代数思维方式的训练。另一方面, 整数是非常具体的数学研究对象, 计算能力的训练也是非常重要的。习题和考试题中大部分还是计算题 (整数分解, 解同余方程, 计算勒让德符号, 等等)。要培养学生不畏惧比较复杂的计算, 并且计算要准确。当然, 每次计算都百分之百的正确是不可能的, 所以要培养及时发现计算中间有误并加以改正的能力。现在许多学生使用计算器和电脑计算, 但这不能代替人在计算中获得的感觉和经验。华罗庚在《数论导引》一书中说, 高斯不但 “老谋”, 而且 “深算”。高斯对于不超过 x 的素数个数 $\pi(x)$ 作了大量的计算, 猜测当 $x \to \infty$ 时, $\pi(x)$ 和 $x/\log x$ 的比值的极限为 1。这个猜测于 19 世纪末被两位法国数学家用黎曼创造的解析方法和精细的计算技巧所证明。更为初等的证明是在 1950 年代由塞尔伯格给出的, 塞尔伯格这项工作得到数学家的最高奖赏 —— 菲尔兹奖。高斯还对大量的整数 d, 研究环 $\mathbb{Z}[\sqrt{d}]$ 是否有唯一因子分解性质, 在计算基础上提出两个著名的猜想, 其中的一个至今未解决。华罗庚本人不但精于计算, 而且精于珠算。文革期间有一次我去华罗庚老师家, 他说: “你来晚了一会儿, 史丰收刚走。” 善于心算的史丰收和华罗庚珠算比 4 位数的乘法, 没有比过华罗庚的算盘。我在 1964 年考研究生时, 记得华罗庚出的一道题是: 计算 2 开 5 次方根到小数点后第 5 位。要求不仅得到近似值, 而且要证明误差不超过 10^{-5}。

讲义和课外读物

国内关于初等数论的教材和课外读物已有很多, 大都受读者欢迎。影响最大的显然是华罗庚的《数论导引》(前 6 章为初等数论)。这是华罗庚在 1950 年代培养新中国第一批数论人才时, 举办讨论班由华罗庚和他的学生们集体写成。前 6 章由华罗庚本人完成, 后面每章由华写成初稿在讨论班上讲一遍, 然后指定一人加以补充和完善。整个工作由吴方、魏道政、许孔时和王元负责, 严士健和任健华也参加部分工作, 最后由越民义总负责 (详见王元的《华罗庚》一书所述), 其严肃和认真的程度堪称典范。我在中国科技大学上学时, 有幸于 1962 年听王元先生讲《数论导引》。时隔 20 年之后, 有一次儿子问我: “你是华罗庚的研究生, 怎么没有《数论导引》?” 我告诉他, 1968 年我们 6 个同学 (作为华罗庚文革前最后一届研究生) 被分配到外地当工人。临行前把包括《数论导引》在内的书籍以 8 分钱一斤的价格卖给西单一家旧书店, 然后就在旁边的东来顺用这笔钱吃了一顿涮羊肉作为临别纪念。1979 年, 我到美国做访问学者, 遇到不少台湾学生, 他们在大学读书时都念过《数论导引》, 不过要包上封面, 因为当时大陆出版的任何书籍在台湾都是禁止的。后来这本书由斯普林格出版社出版了英文本, 成为畅销书和国际

上许多数论研究的重要参考文献。

我从 1977 年起在科大教初等数论, 后来余红兵老师也教此课。在多年讲授的基础上我们合写了《初等数论》讲义, 由中国科学技术大学出版社于 1989 年出版。1995 年再版时, 余红兵希望附上习题解答, 我感到这会助长学生偷懒, 最后折衷为对部分题目给出提示。这个讲义当时主要是为我们在科大教学的需要。1999 年, 高等教育出版社和施普林格出版社共同以 “基础数学丛书” 的名义要我们把原书稍加扩充, 出版了《整数和多项式》一书, 增加了域上的多项式理论。现在欧阳毅教授在科大讲初等数论时还主张讲多项式内容, 因为域上多项式和整数环是主理想整环的两个典型例子, 许多性质是相似的。2000 年以后我到清华大学讲初等数论, 由于学时较少 (共 32 学时), 关于多项式部分忍痛割爱, 但是增加了初等数论在通信中的一些应用内容, 讲课三年积累了新的讲稿。正好严士健先生约我为中学教师编写一本数论的读物, 以适应目前中学数学改革的需要, 便以《初等数论及其应用》为名于 2003 年由北京师范大学出版社以 “走进数学新课程丛书” 出版。后来我在清华大学讲课一直采用此书。此外, 我还写过两本初等数论的普及读物。一本是《从整数谈起》, 由湖南教育出版社作为 “中学生数学视野丛书” 于 1998 年出版, 丛书主编为刘绍学先生, 其中也讲到连分数和无理数用有理数逼近等内容。另一本书是《费马猜想》, 由科学出版社作为 “数学小丛书” 于 2002 年出版。1956 年, 科学出版社曾出版过一套数学普及读物, 当时的中学生受到很大影响。我在中学时就读过这套丛书中华罗庚的《从杨辉三角谈起》。段学复的《对称》和姜伯驹的《一笔画和邮递员路线问题》等。2002 年科学出版社重印这套丛书, 我应王元先生之约为丛书写一本《费马猜想》, 介绍费马于 1637 年提出猜想到 1994 年怀尔斯证明猜想长达三百多年的故事。现在看来, 我写的内容偏多, 篇幅也偏大, 和丛书中其他书不太相称。

我对自己所写的书都不十分满意, 每次使用时, 不仅会发现印刷错误, 也有叙述不准确甚至是错误的地方, 或者还有更合适的证明方法。这使我深深感到, 一个好的教材一定要先教过多次, 不断修改后再出版, 以更合适于初学者使用。普及读物中的内容要是有机会先讲演过几次, 根据听众的反映和效果做些加工, 效果会更好些。