

代数与数论教学中的中国剩余定理——探究“三课合一”新模式

刘雨喆¹, 刘大俊^{2,*}

1. 贵州大学数学与统计学院, 贵州贵阳;
2. 安徽工程大学数理与金融学院, 安徽芜湖

摘要: 中国剩余定理是代数中的一则重要的定理, 也是初等数论中的重要基本定理之一。本文将以高等代数中的一个课后习题作为背景, 在代数教学与数论教学的背景下来讨论如何进行中国剩余定理的教学, 由此进行“三课合一”的新教学模式探究。

关键词: 抽象代数, 基础数论, 中国剩余定理, 分层教学

The Chinese Remainder Theorem in Algebra and Number Theory Teaching — Exploring the New Model of “Three Courses in One”

Yu-Zhe Liu¹, Dajun Liu^{2,*}

1. Mathematics and Statistics, Guizhou University, Guiyang, Guizhou;
2. School of Mathematics-physics and Finance, Anhui Polytechnic University, Wuhu, Anhui

Abstract: The Chinese Remainder Theorem is an important theorem in algebra and one of the fundamental theorems in elementary number theory. This paper takes an exercise from advanced algebra as a starting point and discusses how to teach the Chinese Remainder Theorem within the contexts of both algebra and number theory instruction, thereby exploring a new “Three Courses in one” teaching model.

Keywords: Abstract Algebra; Elementary Number Theory; Chinese Remainder Theorem; Layered Teaching

* 作者简介: 刘雨喆 (1992.03-), 土家族, 男, 南京大学博士, 贵州大学数学与统计学院, 校聘副教授, 硕士生导师, 主要研究方向: 同调代数与代数表示论;

通讯作者: 刘大俊 (1992.04-), 汉族, 男, 南京师范大学博士, 安徽工程大学数理与金融学院, 副教授, 硕士生导师, 主要研究方向: 同调代数与代数表示论。

1 初等数论与近世代数教学中的中国剩余定理

中国剩余定理 (Chinese Remainder Theorem, 简称CRT) 的历史可以追溯到古代的中国数学, 其中最为人们所熟知的就是“韩信点兵”问题和《孙子算经》中的“物不知数”问题[1]。通常, 在初等数论的教学过程中, 关于中国剩余定理部分的教学, 一般是先给学生讲解同余和同余式, 然后引入一次同余式方程组

$$\{x \equiv a_i \pmod{m_i}\}_{1 \leq i \leq n},$$

其中, $m_1, \dots, m_n$ 是两两互素的正整数。再之后, 任课教师会给出具体的求解方法。中国剩余定理的证明是对具体地一次同余式方程组(1)求解方法的抽象, 具体地说, 对每个 $1 \leq t \leq n$, 先将(1)转化为关于 x_t 的一次同余式方程组

$$\begin{cases} x_t \equiv 1 \pmod{m_1}; \\ \{x_t \equiv 0 \pmod{m_i}\}_{i \neq t, 1 \leq i \leq n}, \end{cases}$$

并利用Bezout定理求解此方程组, 得到 x_t ; 然后直接验证 $a_1x_1 + a_2x_2 + \dots + a_nx_n$ 就是(1)的其中一个解; 最后, 利用同余的性质证明此解在关于模 $M = m_1m_2 \dots m_n$ 的意义下解具有唯一性, 例如[2]。

在《近世代数》中, 中国剩余定理被推广到了一般形式, 它是同构基本定理的若干推论之一, 其具体叙述如下: 设 R 是交换幺环, $I_1, \dots, I_n$ 是 R 的理想且两两互素, 即对任意 $i \neq j$, 有 $I_i + I_j = R$, 则存在环的同构

$$R / \bigcap_{i=1}^n I_i \cong \prod_{i=1}^n R / I_i.$$

这一结果在许多国内外的代数学教材中都被作为主要教学内容之一, 例如[3,4]。然而, 一个众所周知的事实是, 在《近世代数》教学中大部分高校的本科生第一接触抽象的代数概念时, 产生了畏难情绪, 这使得同构基本定理的教学变得困难。再加上大部分学生很少接触初等数论, 对原始的中国剩余定理的接触不多等一系列原因, 使得交换幺环上的中国剩余定理作为同构基本定理的推论之一, 难免会让许多学生望而生畏。

综上, 可以看到在中国剩余定理 (或是一般的代数与数论的知识点) 的教学过程中, 教师往往会

遇到以下教学难点:

难点1.大部分本科学生在中学阶段对初等数论是零接触的。

难点2.大部分本科生在大学数学系课程学习过程中, 尚未形成抽象思维。

难点3.许多高校虽然有开设初等数论课程, 然而高校的理工科发展与定位并不支持基础数学的发展, 亦没有相应的数论教学科研团队, 或其数论教学科研团队获得省级、市级、校级、以及所在学院的基本支持远低于其余数学教学科研团队, 因此并不具备真正意义上开办初等数论课程的环境以及能力。

2 高等代数教学中对中国剩余定理的渗入

为了解决上述难点, 笔者试图从多个角度来完成代数与数论的重要知识点教学。鉴于高等代数是高校数学系本科生的必修课程, 本文以[5]的第五章的一道习题 (该教材第五章的C组题第1题, 以下简称习题) 为例, 来阐述如何从数学系大一本科生的高等代数课程开始, 让对数论零接触的学生初步感受中国剩余定理的魅力。该习题内容如下。

习题. 设 A 是定义在数域 F 上 n 维线性空间 V 的线性变换。在 $F[x]$ 中, 多项式 $f(x)$ 有分解 $f(x) = f_1(x)f_2(x) \dots f_n(x)$, 其中 $f_1(x), \dots, f_n(x)$ 两两互素。证明:

$$\ker f(A) = \bigoplus_{i=1}^n \ker f_i(A)$$

讲解设计 (融入中国剩余定理)。 首先, 作为一名代数与数论的教师而言, 我们对交换幺环上的中国剩余定理是熟悉的。因此, 本问题讲解的第一步是在避开抽象代数中的群与环的概念的基础上, 向学生传达环的同构

$$F[x] / \bigcap_{i=1}^n \langle f_i(x) \rangle \cong \prod_{i=1}^n F[x] / \langle f_i(x) \rangle.$$

更通俗地说, 即是向学生传达关于 $g(x)$ 的一次同余式方程组

$$\{g(x) \equiv 1 \pmod{f_i(x)}\}_{1 \leq i \leq n}$$

有解。此时, 可以将中国剩余定理的证明按如下方

式向学生展示。考虑关于 $g_i(x)$ 的一次同余式方程组

$$\begin{cases} g_i(x) \equiv 1 \pmod{f_i(x)}; \\ \{g_i(x) \equiv 0 \pmod{f_i(x)}\}_{i \neq t} \end{cases}$$

有解。该解可以通过 $f_t(x)$ 和 $f_1(x) \cdots f_{t-1}(x)f_{t+1}(x) \cdots$

$f_n(x) = \frac{f(x)}{f_t(x)}$ 互素得到。具体地说，由多项式版本的

Bezout定理（见[5]的13页，定理1.6.3）可知存在 $h_t(x)$ 和 $\varphi_t(x)$ 使得 $h_t(x)\frac{f(x)}{f_t(x)} + \varphi_t(x)f_t(x) = 1$ ，于是

$g_t(x) = -\varphi_t(x)f_t(x) + 1 = h_t(x)\frac{f(x)}{f_t(x)}$ 便是上述次同余式方程

组的一个解。进而得 $g(x) = \sum_{i=1}^n g_i(x)$ 是满足同余式方程

组(3)的多项式，这说明(3)有解。

其次，将同构(2)展示为域 F 上的线性空间的同构，利用 $\bigcap_{i=1}^n \langle f_i(x) \rangle = \langle f(x) \rangle$ 将该同构左侧中的元素解释为等价类，其对应的等价关系 $\varphi(x) \sim \phi(x)$ 定义为 $\varphi(x) \equiv \phi(x) \pmod{f(x)}$ ，并将该同构的右侧解释为直和 $\bigoplus_{i=1}^n F[x]/\langle f_i(x) \rangle$ ，它的每一个直和项中的元素也被解释为等价类，其对应的等价关系 $\varphi(x) \sim \phi(x)$ 定义为 $\varphi(x) \equiv \phi(x) \pmod{f_i(x)}$ 。那么，同构(2)就可以被解释为如下对应法则

$$[h(x)]_{f(x)} \mapsto ([h(x)]_{f_1(x)}, \dots, [h(x)]_{f_n(x)}),$$

记号 $[h(x)]_{f(x)}$ 表示 $F[x]/\langle f(x) \rangle$ 中包含 $h(x)$ 的等价类， $[h(x)]_{f_i(x)}$ 表示 $F[x]/\langle f_i(x) \rangle$ 中包含 $h(x)$ 的等价类。于是，满足同余式方程组(3)的多项式 $g(x)$ 给出了对应

$$[g(x)]_{f(x)} \mapsto I = ([1]_{f_1(x)}, \dots, [1]_{f_n(x)}),$$

这里 I 就是 $\prod_{i=1}^n F[x]/\langle f_i(x) \rangle$ 的单位元。上述对应表明：存在 $q(x)$ 使得 $g(x) = q(x)f(x) + 1$ 。带入线性变换 A ，就有 $g(A) = q(A)f(A) + E$ ，记号 E 就是 V 上的恒等变换。

最后，需要证明 $\ker f(A) = \sum_{i=1}^n \ker f_i(A)$ 以及 $\ker f_i(A) \cap \ker f_j(A) = \{0\} (\forall i \neq j)$ 。这里，受限于文章的篇幅以及本文的侧重点在中国剩余定理的教学研究，因此， $\ker f_i(A) \cap \ker f_j(A) = \{0\} (\forall i \neq j)$ 的证明留给读者，此外，第一个等式的“ $\supseteq$ ”方向是显然的，本文这里只对第一个等式的“ $\subseteq$ ”证明方法展

开简述。在 $\ker f(A)$ 上，线性变换 $g(A) = q(A)f(A) + E$ 表现为 $g(A)|_{\ker f(A)} = E|_{\ker f(A)}$ ，因此对任意 $m \in \ker f(A)$ ，

有 $g(A)|_{\ker f(A)}(m) = m$ ，也即 $\sum_{i=1}^n g_i(A)|_{\ker f(A)} m = m$ 。再由前文的 $g_i(x) = h_i(x)\frac{f(x)}{f_i(x)}$ 立刻知

$$f_i(A)g_i(A)|_{\ker f(A)} m = h_i(A)f(A)|_{\ker f(A)} m = 0,$$

这说明和式 $\sum_{i=1}^n g_i(A)|_{\ker f(A)} m$ 的每个直和项

$g_i(A)|_{\ker f(A)} m$ 必属于 $\ker f_i(A)$ 。这样就将 $\ker f(A)$ 中的元素 m 分解为 $m_1 + \cdots + m_n$ 的形式，其中 $m_i \in \ker f_i(A)$ ，故“ $\subseteq$ ”成立。

在上述讲解设计中，教师可以将侧重点放在一次同余式(3)的求解过程上，逐步引出一元多项式环 $F[x]$ 上的中国剩余定理。该教学设计本质上虽然是对多项式算法的灵活应用，然而在证明过程中，已经通过等价类侧面介绍了商环的概念，这让学生初步接触了一些抽象代数的思想。可见，上述讲解设计在一方面已经一定程度上弥补教学难点1中学生对初等数论零接触的不利事实，另一方面也直面了难点2，即教师已开始初步培养学生的抽象代数中的抽象思维能力。

3 教学数据与初步成果

笔者将高等代数、近世代数、以及基础数论进行“三课合一”综合教学的教学方法尝试虽然刚起步，但是该教学方法已具备教学内容交叉融合的鲜明特色，并产生了一定的成效。笔者依托超星学习通作为教学平台，检测了大一、大二本科生在各知识点上的掌握情况。其中，在中国剩余定理方面，学生的知识点完成数据如图1所示，知识点掌握数据如图2所示。

根据该课程超星学习通平台统计数据显示，每位同学对于知识点的掌握情况可实时更新，根据该结果可定向给该同学发布相关知识点的习题作为训练，即可达到精准练习。具体包括在系统内设计梯度性任务（如基础题、挑战题、开放性问题），满足不同能力学生的需求；根据学生的学习反馈和阶

段性表现, 灵活调整分层策略, 避免静态贴标签; 缩小学生之间的差距, 同时为学有余力者提供发展空间, 实现“保底不封顶”; 采用多元评价标准, 关注学生的进步而非横向比较; 在系统内, 采用分组活动、个性化作业、自主选择任务等方式实现, 保护学生隐私及自尊心等问题。

在该教学研究初期, 学生以极大的主观能动性自学并探究中国剩余定理, 针对其提出的问题, 文献[6]给出了一般非交换环 R 的一元多项式环 $R[x]$ 上的可进行带余除法的条件以及与之对应的中国剩余定理, 这是笔者与本科生共同探讨的结果, 是“三课合一”教学改革的效果直观体现。

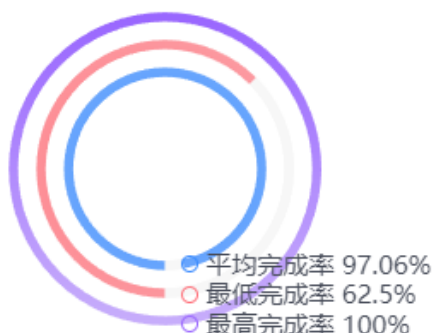


图1. 基础数论中国剩余定理完成情况

(数据来源: 贵州大学数学与统计学院初等数论课程/超星学习通平台统计数据)

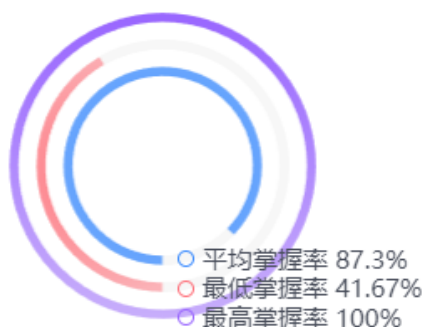


图2. 基础数论中国剩余定理掌握情况

(数据来源: 贵州大学数学与统计学院初等数论课程/超星学习通平台统计数据)

4 小结

“三课合一”教学模式通过整合初等数论、近世代数及现代信息技术课程, 有效破解了传统教学中抽象理论与实际应用脱节、学生基础差异大等难题。借助AI辅助教学工具, 如超星学习通平台的实时数据追踪与精准习题推送, 教学实现了从“统一灌输”到“个性化赋能”的转型。这种改革不仅缩小了学生差距, 更为学有余力者提供了开放探索空间。师生共研成果的诞生, 是“三课合一”促进跨学科融合、AI技术推动教学精准化与人性化的生动例证, 为数学教学改革提供了可复制的创新路径, 也为将来进一步优化和提升教学提供了新的思路。

致谢

本文由以下项目资助: 国家自然科学基金项目青年项目: 弦代数的G-同调性质及其几何实现(No. 12401042); 贵州省科技厅科学计划项目一般项目: 关于弦代数的Auslander代数及其张量表述的研究(No. ZK [2024] YiBan 066); 贵州大学高等教育研究项目: 《近世代数》课程的线上线下混合式教学模式改革(No.703217243301); 贵州大学引进人才科研启动基金项目: 弦代数的表示型及其Auslander代数的张量表述(No. 2022[65]); 安徽工程大学本科教学质量提升计划: “三全六专”综合改革在安徽工程大学《高等数学》教学管理中的应用(No. 2023jyxm23)。

本文为2024年北京世纪超星信息技术发展有限责任公司教育部产学研合作协同育人项目(数学类专业代数课程群建设与实践)阶段性成果。

参考文献

- [1] 李文林. 数学史概论(第四版)[M]. 北京: 高等教育出版社, 2021.
- [2] Kenneth H R. Elementary Number Theory and its Application (6th Ed)[M]. London: Pearson Education, 2011.
- [3] Stein W. Elementary Number Theory: primes, congruences,

- and secrets: a computational approach[M]. Berlin: Springer Science & Business Media, 2008.
- [5] 徐云阁, 章超, 廖军. 高等代数[M]. 北京: 科学出版社, 2021.
- [4] 聂灵沼, 丁石孙. 代数学引论 (第二版) [M]. 北京: 高等教育出版社, 2000.
- [6] 王传夷, 刘雨喆. 一元多项式环与中国剩余定理[J]. 理论数学, 2025, 15(4): 430-444.

