初等数论与抽象代数对接的教学探索

杨四强，杜保营，刘艺

宜宾学院，四川 宜宾 644005

DOI: 10.61369/ETR.2026010005

摘　　要： 针对高校初等数论课程教学中存在的一些共性问题，通过四个典型的教学案例探讨如何实现与抽象代数课程的有效教学对接，将抽象代数的理念与方法有机融入初等数论教学实践。具体而言，四个案例分别聚焦：抽象代数视角下同余概念及其基本性质的理解；通过一个重要习题的教学案例来体现抽象代数理论的应用；运用抽象代数理论和方法诠释和证明欧拉定理、费马定理和威尔逊定理。此教学探索旨在巩固学生的抽象代数学习成果，帮助学生深刻理解两门课程的内在联系与实际应用，激发其对初等数论的学习兴趣，最终促进数学素养的提升。

关 键 词： 初等数论；抽象代数；教学

Exploration of Teaching Methods Integrating Elementary Number Theory and Abstract Algebra

Yang Siqiang, Du Baoying, Liu Yi

Yibin College, Yibin, Sichuan 644005

Abstract： Addressing some common issues in the teaching of elementary number theory in universities, this paper explores how to effectively integrate it with abstract algebra courses through four typical teaching cases. Specifically, these cases focus on: understanding the concept of congruence and its basic properties from the perspective of abstract algebra; demonstrating the application of abstract algebra theory through a teaching case of an important exercise; and interpreting and proving Euler's theorem, Fermat's theorem, and Wilson's theorem using abstract algebra theory and methods. This teaching exploration aims to consolidate students' learning achievements in abstract algebra, help them deeply understand the intrinsic connection and practical application of the two courses, stimulate their interest in learning elementary number theory, and ultimately promote the improvement of mathematical literacy.

Keywords： elementary number theory; abstract algebra; teaching

引言

数论是现代数学的核心内容，其基础理论体系集中体现在初等数论课程中，该课程的核心内容（如同余、素数性质）不仅是现代数论很多重要研究的起点，更与中学数学教育存在紧密且多元的知识衔接。因此，《初等数论》已成为了高校数学与应用数学师范专业的重要专业课程。作者多年担任所在院校的初等数论课程教学任务，所采用的教材是闵嗣鹤的《初等数论（第四版）》[1]，该教材也是众多院校的选择。经过教学实践发现，当前的初等数论教学上存在一些待改进的地方：一是教材内容侧重理论推演，对知识的应用性挖掘不足，解题策略训练相对薄弱；二是教学过程中跨学科融合深度不够，导致学生难以充分认知课程的学科价值；三是部分知识点因呈现方式单一而显得枯燥，进而影响学习主动性。实际上，关于初等数论课程教学的研究与改革，不少学者已做了一些很有意义的探讨[2-11]，本文不再赘述。这些有价值的改革探索，为本研究提供了重要参考。

结合笔者在数学专业《抽象代数》课程的多次授课经验及多方面反馈，发现该课程在国内众多院校中普遍存在学生认知痛点：课程知识抽象程度较高，学生难以建立直观理解；知识的实际应用场景展示不足，导致学习动力与获得感受限。另外，抽象代数基本上没有后续课程，使得学生没有足够机会“学而时习之”。学生们通常也不会再花时间和精力来巩固所学，从而不能反复认识和思考课程知识，加大了理解和记忆抽象代数知识的难度，理解流于表面，学生通过期末考试之后，知识会快速遗忘。一段时间后对抽象代数课程的印象往往只剩一些基本名词的概念。

众所周知，现代数论与抽象代数有着非常紧密的联系。抽象代数是初等数论的抽象化，而初等数论中的很多问题为抽象代数提供了

项目信息：宜宾学院2023年度课程思政项目，《初等数论》课程思政示范课程 (XKCSZKC202303)。

作者简介：
杨四强（1985.03—），男，汉族，四川泸州，博士，讲师。研究方向：代数学、泛函分析。
杜保营（1981.12—），男，汉族，山东曲阜，博士，讲师。研究方向：非线性偏微分方程。
刘艺（1998.01—），女，汉族，四川自贡，硕士，讲师。研究方向：数学教育。

具体模型与直觉来源。例如模 n 同余类加上两种自然的运算可以直接抽象为环；整数的加减乘运算可以抽象为环中相应的运算；整数的算术基本定理可以抽象为唯一分解整环理论。

基于目前的初等数论教学现状与学科特点，作者在教学中有意识地结合抽象代数的方法和理论（需说明的是，在作者所在院校，抽象代数开设于大三上学期，而初等数论安排在大三下学期，这为跨课程知识衔接提供了可行性）。具体实践中，虽然初等数论传统上以初等方法为主要工具，但诸多内容可借助抽象代数视角实现简化，通过公理化方法将初等数论中的分散结论系统化，利用公理化方法构建普适性框架。从而显著降低初等数论理解的门槛，帮助学生以更高观点统摄知识脉络，又能促使其主动回顾并深化对抽象代数核心概念的认知，巩固以前的学习成果。特别地，针对部分初等证明给出对应代数证明，可直观展现数学工具从具体到抽象的演进逻辑，凸显了数学的发展性和层次性。我们还希望通过这种教学尝试向学生渗透“数学各个分支并非孤立存在，而是互相联系，通过概念迁移与方法互补实现协同发展”的整体性观念，引导其建立跨学科的知识联系。

一、教学案例及其分析

在本节中，将结合教学实践，呈现若干初等数论教学案例，具体阐释如何通过抽象代数的理论与方法实现初等数论知识点的延伸与深化。文中案例均以闵嗣鹤先生所著《初等数论（第四版）》为参考教材展开。

（一）案例一

教材第三章第1节题为“同余的概念及其基本性质”。如果将模 m（正整数）的剩余类看成一个元素，剩余类的相等就可以用同余来刻画，反之亦然。第1节中的同余的运算性质就可以转化为剩余类的运算性质。模 m 的剩余类的集合对剩余类的加法和乘法运算作成一个环，称为剩余类环。如果只考虑加法，则作成一个加群。由此我们可从抽象代数的角度来理解同余的运算性质。对 m，考虑剩余类环 $\mathbb{Z}_m=\{\bar{0},\bar{1},\bar{2},\cdots,\overline{m-1}\}$。整数间的同余关系 $a\equiv b\ (\mathrm{mod}\, m)$ 等价于在环 $\mathbb{Z}_m$ 中 $\bar{a}=\bar{b}$，这是一个简单而又关键的知识点。书上列出的11条同余性质，即性质甲到性质癸，由该知识点都可以转化为环 $\mathbb{Z}_m$ 中元素的基本性质。由于后四条性质在环中的表达意义不是太大，我们只考虑前五条性质。

甲：$a\equiv a\ (\mathrm{mod}\, m)$，

乙：若 $a\equiv b\ (\mathrm{mod}\, m)$，则 $b\equiv a\ (\mathrm{mod}\, m)$，

丙：若 $a\equiv b\ (\mathrm{mod}\, m)$，$b\equiv c\ (\mathrm{mod}\, m)$，则 $a\equiv c\ (\mathrm{mod}\, m)$，

丁：(i) 若 $a_1\equiv b_1\ (\mathrm{mod}\, m)$，$a_2\equiv b_2\ (\mathrm{mod}\, m)$，则 $a_1+a_2\equiv b_1+b_2\ (\mathrm{mod}\, m)$，

(ii) 若 $a+b\equiv c\ (\mathrm{mod}\, m)$，则 b=a(mod$m$)，

戊：若$a_1\equiv b_1\ (\mathrm{mod}\, m)$，$a_2\equiv b_2\ (\mathrm{mod}\, m)$，则 $a_1a_2\equiv b_1b_2\ (\mathrm{mod}\, m)$。特别地，若 $a\equiv b\ (\mathrm{mod}\, m)$，则 $ka\equiv kb\ (\mathrm{mod}\, m)$。

在加群 $\mathbb{Z}_m$ 中，以上性质意味着：

甲'：$\bar{a}=\bar{a}$，

乙'：若 $\bar{a}=\bar{b}$，则 $\bar{b}=\bar{a}$，

丙'：若 $\bar{a}=\bar{b}$ 且 $\bar{b}=\bar{c}$，则 $\bar{a}=\bar{c}$，

丁'：(i) 若 $\overline{a_1}=\overline{b_1}$，$\overline{a_2}=\overline{b_2}$，则 $\overline{a_1+a_2}=\overline{b_1+b_2}$，

(ii) 若 $\overline{a+b}=\bar{c}$，则 $\bar{a}=\overline{c-b}$。

这些都是剩余类加群的很显然的事实。把 $\mathbb{Z}_m$ 看作是环，则性质戊转化为下述性质。

戊'：若 $\overline{a_1}=\overline{b_1}$，$\overline{a_2}=\overline{b_2}$，则 $\overline{a_1a_1}=\overline{b_1b_2}$。特别地，若 $\bar{a}=\bar{b}$，则 $\overline{ka}=\overline{kb}$。

这样的处理使学生能直观看到“同余”是整数的分类方式，理解同余的基本性质本质上是群和环的元素阶的简单性质，由此学生能更专注于同余的核心性质，而非复杂的代数推导。这样，我们就把理论放在了更一般的框架内，使学生们站在了一个更高的层次来俯视同余的性质。

（二）案例二

教材第三章第3节题为“既约剩余系与欧拉函数”。对加群 $\mathbb{Z}_m$，只考虑与 m 互素的元素，对模 m 剩余类的乘法构成了一个群，记为 $\mathrm{U}(\mathbb{Z}_m)$。模 m 的既约剩余系可以理解为群 $\mathrm{U}(\mathbb{Z}_m)$ 的全体元素的代表元构成的集合。定理1是本节的基础结论，内容为：与模 m 互素的剩余类的个数是 $\varphi(m)$。换句话说即群 $\mathrm{U}(\mathbb{Z}_m)$ 的阶（也就是群的元素个数）为 $\varphi(m)$。这里，$\varphi(m)$ 是欧拉函数。

现在我们考虑本节的习题 3(ii)：证明 $\sum_{d|a}\varphi(d)=a$，其中 $\sum_{d|a}$ 表示展布在 a 的一切正因数上的和式。

在讲授证明前，可先举例说明该结论，帮助学生理解。

例1 令 $a=10$，有

$$\sum_{d|10}\varphi(d)=\varphi(1)+\varphi(2)+\varphi(5)+\varphi(10)$$
$$=1+1+4+4=10\text{。}$$

例2 令 $a=45$，有

$$\sum_{d|45}\varphi(d)=\varphi(1)+\varphi(3)+\varphi(5)+\varphi(9)+\varphi(15)+\varphi(45)$$
$$=1+2+4+6+8+24=45\text{。}$$

教师可向学生强调，虽然这个结论是以习题的形式呈现，但它是初等数论中关于欧拉函数的重要性质，是理解欧拉函数性质的关键，也是后续学习更复杂数论定理的基础。它揭示了欧拉函数与整数因数结构的深层联系，是数论中“整除”与“互质”两大核心概念的桥梁。不少数论定理的证明均依赖于此结论，同时它也是数学竞赛中一个常用的工具。在密码学中，该公式有助于理解 RSA 算法中模反元素的计算原理。

在讲解此结论时，可先给出传统证明方法，再给出抽象代数证明方法，形成鲜明对比。

传统证明方法 考虑 $a=p^t$，p^t 的因子为 $1,p,p^2,\cdots p^t$，而 $\varphi\left(p^k\right)=p^k-p^{k-1}$，故

$$\sum_{d|a}\varphi(d)=\varphi(1)+\varphi(p)+\cdots+\varphi\left(p^{\alpha}\right)$$
$$=1+(p-1)+\left(p^2-p\right)+\cdots+\left(p^t-p^{t-1}\right)$$
$$=p^t。$$

下一步，考虑一般情形。$a=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$，$a$ 的因子为 $d=p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$，$0\le r_i\le t_i$，则

$$\varphi(d)=\varphi(p_1^{r_1})\varphi(p_2^{r_2})\cdots\varphi\left(p_k^{r_k}\right)。$$

从而

$$\sum_{d|a}\varphi(d)=\sum\nolimits_{r_1=0}^{t_1}\cdots\sum\nolimits_{r_k=0}^{t_k}\varphi(p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k})$$
$$=\sum\nolimits_{r_1=0}^{t_1}\cdots\sum\nolimits_{r_k=0}^{t_k}\varphi(p_1^{r_1})\varphi(p_2^{r_2})\cdots\varphi\left(p_k^{r_k}\right)$$
$$=\prod\nolimits_{i=1}^{k}\sum\nolimits_{r_i=0}^{t_i}\varphi(p_i^{r_i})=\prod\nolimits_{i=1}^{k}p_i^{t_i}=a。$$

完成证明。

注意：在讲授中为帮助学生理解推理的最后几步，可举例做演示。

例3 令 $a=p_1^2p_2^3$，则

$$\sum_{d|a}\varphi(d)=\varphi(p_1^0p_2^0)+\cdots+\varphi(p_1^0p_2^3)+\cdots+\varphi(p_1^2p_2^0)+\cdots+\varphi(p_1^2p_2^3)$$
$$=\left(\varphi(p_1^0)+\varphi(p_1^1)+\varphi(p_1^2)\right)\left(\varphi(p_2^0)+\cdots+\varphi(p_2^3)\right)$$
$$=p_1^2p_2^3。$$

显然，该证明是比较繁琐的，思路也具有一定的隐蔽性，对学生而言独立完成难度很大。事实上学生们事先往往都是通过查询资料来完成该习题。现在我们讨论如何使用抽象代数的方法来证明此结论。先引导学生复习以下知识点：G 是阶为 a 的循环群，设 g 是 G 的生成元。则对任意 $k\in\mathbb{N}^+$，令 $d=\gcd(a,k)$，则 $\left\langle g^k\right\rangle$ 是阶为 a/d 的循环子群，且 $\left\langle g^k\right\rangle=\left\langle g^d\right\rangle$。特别地，$G$ 恰有 $\varphi(a)$ 个生成元。

抽象代数证明方法 令 G 是阶为 a 的循环群。对任意的 d 使得 $d|a$，G 有唯一一个阶为 d 的循环子群。且该子群有 $\varphi(d)$ 个生成元。又 G 的每个生成元都生成一个循环子群，从而 $|G|=a=\sum_{d|a}\varphi(d)$。

可见，相比传统证明，使用抽象代数知识来证明十分简洁。从而学生们可以切实体会到抽象代数理论的应用，以及抽象代数课程中处处蕴含的抽象化思维带来的好处。

注意，抽象代数证明方法虽然很简短，但比较抽象，教师应通过举例辅助学生理解。

例4 令 $a=6$，有

$$\sum_{d|6}\varphi(d)=\varphi(1)+\varphi(2)+\varphi(3)+\varphi(6)。$$

另一方面，考虑阶为6的循环群 G，我们说明上式右端这4项之和恰好是 G 的全体元素的数量。

当 d 取1，对应的循环子群是 $\{e\}$，该子群的生成元是1个，即 e；

当 d 取2，对应的循环子群是 $\{e,a^3\}$，该子群的生成元是1个，即 a^3；

当 d 取3，对应的循环子群是 $\{e,a^2,a^4\}$，该子群的生成元是2个，即 a^2、a^4；

当 d 取6，对应的循环子群是 G 本身，该子群的生成元是2个，即 a、a^5。

上述4种情形下的全体生成元正好是 G 的全体元素 $e,a,a^2,\cdots,a^5$，数量为 $1+1+2+2=6$。与结论吻合。

教学实践表明，部分抽象代数基础薄弱的学生难以理解该抽象代数证明，而例4的具象化表达易被接受。我们不要求理解抽象代数证明方法，但学生可通过例4体会证明的原理，我们相信这依然是有意义的。

（三）案例三

第三章第4节题为“欧拉定理·费马定理及其对循环小数的应用”。本节的欧拉定理和费马定理可以说是初等数论的两个典型定理，在中学奥数中也经常涉及到。它们的证明比较简单，不过给出相应的抽象代数证明仍能起到深化理解的作用。这打破了思维定势，学生可以对比不同证明方法的特点和优劣，再次加深对群的性质的理解。

欧拉定理 设 m 是大于1是整数，$\gcd(a,m)=1$，则 $a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\, m)$。

先引导学生回忆知识点：

（1）G 是阶为 n 的群，对任意 $a\in G$，有 $|a|$ 整除 $|G|$，即有 $a^n=1$。

（2）令 $\mathrm{U}(\mathbb{Z}_m)=\{\bar r\in\mathbb{Z}_m,\ \gcd(r,m)=1\}$，则 $\mathrm{U}(\mathbb{Z}_m)$ 是阶为 $\varphi(m)$ 的群（运算为剩余类的乘法，这即是在案例2中复习过的群。

证 考虑群 $\mathrm{U}(\mathbb{Z}_m)$。若 $\bar a\in\mathrm{U}(\mathbb{Z}_m)$，则 $\left(\bar a\right)^{\varphi(m)}=\bar 1$。用同余的语言表示，即 $a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\, m)$。

费马定理 若 p 是素数，则 $a^p\equiv a\ (\mathrm{mod}\, p)$。

证 只需证明在群 $\mathbb{Z}_p$ 中，有 $\overline{a^p}=\bar a$。再转化为同余的语言，即得结论。若 $\bar a=\bar 0$，则 $\overline{a^p}=\left(\bar a\right)^p=\left(\bar 0\right)^p=\bar 0$，结论成立。若 $\bar a\ne\bar 0$，则 $\bar a\in\mathrm{U}(\mathbb{Z}_p)$。而 $|\mathrm{U}(Z_p)|=p-1$。从而 $\left(\bar a\right)^{p-1}=\bar 1$。两边乘以 $\bar a$，得 $\left(\bar a\right)^p=\bar a$。即 $\overline{a^p}=\bar a$。

在上述欧拉定理的证明中，通过 $\mathrm{U}(\mathbb{Z}_m)$ 的构造，让学生理解 $a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\, m)$ 是群元素的阶的性质的直接结果。在上述费马定理的证明中，学生能直观看到定理的本质是群元素的阶与素数 p 的关系。这两个证明将定理拆解为群的构造、群元素的运算这样的步骤，降低了学生的认知负荷。其逻辑可迁移至其他数论问题，形成“问题 -- 工具 -- 应用”的闭环。

（四）案例四

第四章第4节题为“素数模的同余式”。本节中的威尔逊定理不仅是一个饶有趣味的数论结论，其本质上也是素数模同余式基本性质的直接推论。

威尔逊定理 p 是素数，则 $(p-1)!+1\equiv 0\ (\mathrm{mod}\, p)$。

威尔逊定理的内容是很直观的，现在我们从抽象代数的角度来看待该定理。考虑群 $\mathrm{U}(\mathbb{Z}_p)$，公式 $(p-1)!+1\equiv 0\ (\mathrm{mod}\, p)$ 用群论的语言表达，即是 $\bar 1\cdot\bar 2\cdots\overline{p-1}=\overline{-1}=\overline{p-1}$。详细地说，即对群 $\mathrm{U}(\mathbb{Z}_p)$ 而言，全体元素的乘积恰好等于元素 $\overline{p-1}$。

群 $\mathrm{U}(\mathbb{Z}_p)$ 具有两个值得注意的性质：$\left(\overline{p-1}\right)^2=\left(\overline{-1}\right)^2=\bar 1$；

$\overline{p-1}$ 是 $U(\mathbb{Z}_p)$ 的唯一一个二阶元。从而 $\overline{p-1}$ 的逆元为它自身，且除了 $\overline{p-1}$，其它元素的逆元都不是自身。由此群的其它非单位元可以两两配对，乘积均为单位元 $\bar{1}$。下面举例说明。

例5 当 $p=5$ 时，即考虑群 $U(\mathbb{Z}_5)=\{\bar{1},\bar{2},\bar{3},\bar{4}\}$，可作如下的简单计算

$$\bar{1}\cdot\bar{2}\cdot\bar{3}\cdot\bar{4}=\bar{1}\cdot(\bar{2}\cdot\bar{3})\cdot\bar{4}=\bar{1}\cdot\bar{1}\cdot\bar{4}=\bar{4}=\overline{-1}。$$

例6 当 $p=7$，即考虑群 $U(Z_7)=\{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$，有

$$\begin{aligned}\bar{1}\cdot\bar{2}\cdot\bar{3}\cdot\bar{4}\cdot\bar{5}\cdot\bar{6}&=\bar{1}\cdot(\bar{2}\cdot\bar{4})\cdot(\bar{3}\cdot\bar{5})\cdot\bar{6}\\&=\bar{1}\cdot\bar{1}\cdot\bar{6}=\bar{6}=\overline{-1}。\end{aligned}$$

可见都是符合威尔逊定理的。

通过这样的讲解方式，学生不仅能更好地掌握威尔逊定理的内涵，也能更轻松地记忆该定理。

二、结语

从实际教学情况来看，在教学中融入与抽象代数对接的内容，对知识点做适当的延申，虽然在一定程度上提高了知识的抽象程度和难度，但还是处在学生们的接受范围内，起到了前文中提到的效果。另外在教学中应该注意避免认知超载，不应过多抽象化而导致喧宾夺主，需平衡好直观性与严格性。例如在案例四中，对群 $U(\mathbb{Z}_p)$ 而言，除了元 $\overline{p-1}$，其它元素的逆元都不是自身，从而可以两两配对，乘积分别为单位元 $\bar{1}$。该结论可以考虑直接使用，由例5和例6作直观的说明。

受教学时间以及知识难度的限制，我们将部分知识点的扩展作为课后学习任务，鼓励部分学有余力的学生自学和自主探究。这包括整数的算术基本定理的抽象代数版本——唯一分解整环理论、孙子定理在环上的推广、一元五次方程没有求根公式的抽象代数证明。此类安排有助于培养学生的自学能力和构建跨学科知识整合的能力，为部分学生考研和进一步学习现代数学奠定基础。

冯克勤教授曾经指出：初等数论是抽象代数的“天然预科”，二者结合可缓解学生从中学到大学数学的认知跃迁焦虑。而丘维声教授的课程实践表明，通过剩余类环讲解初等数论，能使抽象代数成为“看得见的工具”而非“空中楼阁”。相信我们的教学探索实践对相关师范院校的初等数论课程的教学具有一定的借鉴作用。

在当前时代背景和高校教育形势下，我们需要深入思考如何适应当代大学生的需求，开展针对性的教学，培养具有良好核心数学素养的新一代专业人才。作为这个宏大课题的关键一环，我们将继续理论联系教学实践，探讨在学校人才培养方案的指引下，如何进一步推动初等数论与抽象代数等其他课程的合理深度融合。

参考文献

[1] 闵嗣鹤，严士健 . 初等数论（第四版）[M]. 北京：高等教育出版社，2020.
[2] 王婧哲 .《初等数论》课程教学改革研究 [J]. 内蒙古财经大学学报，2019，17(02):115-117.
[3] 张四保 . 基于 HPM 视角的初等数论课程教学探究 [J]. 长春大学学报，2019，29(06)：99-101+113.
[4] 路秀华，张全雷.《初等数论》课题化教学方法研究——以中国剩余定理为例 [J]. 高等数学研究. 2021，24(01)：116-119.
[5] 张四保，常宁. 初等数论课程教学中融入思政教育的实践探索 [J]. 内蒙古师范大学学报 (教育科学版)，2022，35(02)：147-151.
[6] 杨帆. 初等数论课程与高中数学对接的教学探索 [J]. 嘉应学院学报，2022，40(03)：105-107.
[7] 胡吉振，余志成，王允，等. 数学史视角下的课程思政教学案例研究——以《初等数论》的 " 中国剩余定理 " 为例 [J]. 高等数学研究，2023，26(01)：120-125.
[8] 梁填，张文超. 数学史融入初等数论课程的教学研究——以中国剩余定理为例 [J]. 惠州学院学报，2023，43(03)：112-115.
[9] 王立波. OBE 理念下的初等数论课程思政教学探索——以费马小定理和欧拉定理为例 [J]. 学园，2025，18(09)：4-6.
[10] 张本慧，孙忠洋. 关于高师院校初等数论课程教学改革的思考 [J]. 淮北师范大学学报 (自然科学版)，2018，39(01)：74-78.
[11] 拉珍. 基于数学素养的课堂教学尝试——初等数论课程为例 [J]. 当代教育实践与教学研究，2016，(03)：173.

