WEP Warwick Evans Publishing

International Journal of Social Sciences and Public Administration

ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 10, Number 1, Year 2026
DOI: https://doi.org/10.62051/ijsspa.v10n1.03
Journal homepage: https://ijsspa.org

Integrating the History of Mathematics into Foundations of Information Security Mathematics: A Teaching Reform Practice from the Perspective of Curriculum Ideology

Wei Gao, Mei Li

Department of Computer Science, North China Electric Power University(Baoding), Baoding, China

ABSTRACT

Foundations of Information Security Mathematics is a core foundational course for information security–related majors, covering topics such as number theory, abstract algebra, and elliptic curves, and other essential mathematical topics. Due to its high level of abstraction, intensive use of formal proofs, and substantial mathematical rigor, students often experience significant learning difficulties and lack sustained motivation. In the context of curriculum ideology and politics in higher education, this paper explores an instructional approach that integrates the history of mathematics and mathematicians' narratives into classroom teaching. Taking Fermat's Little Theorem and Euler's Theorem as representative examples, we analyze how historical narratives can enhance student engagement, deepen conceptual understanding, and foster scientific spirit and academic values. Teaching practice indicates that employing the history of mathematics as an entry point for curriculum ideology facilitates the organic integration of professional knowledge transmission and value education, offering a viable reference for instructional reform in mathematics courses for information security programs.

KEYWORDS

Foundations of Information Security Mathematics; Curriculum Ideology; History of Mathematics; Teaching Reform.

1. INTRODUCTION

With the rapid development of information security technologies, solid mathematical foundations and rigorous logical reasoning abilities have become essential requirements for cultivating qualified professionals in this field[1]. As a core foundational course, Foundations of Information Security Mathematics plays an indispensable role in the overall talent training system. However, owing to its highly abstract content, complex symbolic systems, and proof-intensive structure, many students develop learning anxiety and even perceive the course as a purely technical and impractical requirement, which negatively affects learning outcomes.

In recent years, curriculum ideology and politics has emerged as a key educational strategy in higher education aimed at integrating value education into disciplinary teaching[2]. A central challenge lies in embedding value guidance into professional courses without compromising academic rigor. Although mathematics courses primarily emphasize formal reasoning and logical deduction, the historical development of mathematical knowledge itself embodies rich intellectual and educational resources. This study therefore adopts a historical perspective to explore how mathematicians' stories and the evolution of mathematical ideas can be incorporated into Foundations of Information Security

Mathematics, with the goal of achieving a coordinated development of knowledge acquisition, ability cultivation, and value guidance.

2. COURSE CHARACTERISTICS AND TEACHING CHALLENGES

2.1. Course Nature and Educational Objectives

Foundations of Information Security Mathematics is a fundamental course that supports subsequent professional courses, particularly cryptography. Its primary objectives include enabling students to master essential mathematical theories relevant to information security, such as number theory, abstract algebra, and elliptic curves, and other essential mathematical topics; cultivating rigorous logical thinking and formal reasoning skills; and laying a solid foundation for understanding cryptographic algorithms and secure protocol design.

From an educational perspective, the course is not limited to knowledge transmission. It should also guide students toward developing a scientific attitude characterized by precision, rational inquiry, and respect for mathematical rigor, as well as an appreciation of the foundational role of mathematics in both human civilization and modern information security technologies[3].

2.2. Content Features and Instructional Difficulties

This course exhibits several distinctive features[4, 5]. First, its abstract nature and dense symbolic representations make it difficult for students to form intuitive understandings in a short period. Second, the high proportion of theorems and proofs often leads students to focus on final results while neglecting underlying motivations. Third, mathematical results are frequently presented in a polished and formalized manner, obscuring their historical background and practical significance.

Under such circumstances, reliance solely on formula derivation and problem-solving exercises may fail to sufficiently stimulate student engagement or support deeper conceptual understanding and scientific thinking.

3. INTEGRATING CURRICULUM IDEOLOGY FROM THE PERSPECTIVE OF THE HISTORY OF MATHEMATICS

3.1. Educational Value of Mathematical History and Mathematicians' Narratives

Mathematics is not an isolated symbolic system but the product of continuous human exploration under specific historical conditions. The establishment of major theorems typically involves prolonged reflection, repeated trial and error, and collective intellectual effort. Introducing the history of mathematics and stories of mathematicians into classroom teaching helps students understand the generative logic of mathematical knowledge and recognize the perseverance and integrity inherent in scientific inquiry.

For Foundations of Information Security Mathematics, historical perspectives do not dilute technical rigor. On the contrary, they contribute to a more accurate comprehension of abstract concepts and enhance students' emotional engagement and academic identification with the subject.

3.2. A Teaching Case: Fermat's Little Theorem and Euler's Theorem

When teaching modular arithmetic and congruence relations in number theory, Euler's Theorem and Fermat's Little Theorem constitute key content. Euler's theorem states that if an integer a is coprime with a positive integer n, then $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$, where $\varphi(n)$ is Euler's totient function, which denotes the number of positive integers not exceeding n that are coprime to n. Fermat's Little

Theorem states that if p is a prime number and integer a is not divisible by p, then $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$. Fermat's Little theorem is a direct corollary of Euler's theorem: when the modulus n is a prime p, the totient function satisfies $\varphi(p) = p\text{-}1$, so Euler's theorem degenerates into Fermat's little theorem[6].

In traditional instruction, students often question why Fermat's Little Theorem is emphasized separately when it appears to be a special case of Euler's Theorem. This question provides an appropriate opportunity to introduce historical context.

Historically, Fermat's Little Theorem was first proposed in 1640 by Pierre de Fermat, nearly a century before Euler's work. Fermat stated the result without proof. Even more influential was Fermat's Last Theorem, proposed in 1637, which Fermat famously recorded as a marginal note while reading mathematical texts. He remarked that he had discovered "a truly marvelous proof" of the theorem, but that the margin was too narrow to contain it[7]. The quest to prove this theorem triggered more than three centuries of intensive mathematical research.

Throughout this process, numerous outstanding mathematicians made significant contributions. Leonhard Euler provided rigorous proofs for one special case in the 18th century. In the early 19th century, Sophie Germain, working under severe social constraints, introduced critical ideas that eliminated large classes of potential counterexamples. Ernst Kummer later showed that addressing the problem required fundamentally new mathematical tools. Ultimately, in the late 20th century, Andrew Wiles completed a rigorous proof after years of independent research.

After this brief historical detour, we return to Fermat's earlier contribution.Fermat's Little Theorem was proposed by Fermat in 1640 without proof. In 1736, Euler gave the first rigorous proof and subsequently generalized the result from prime moduli to arbitrary integers by introducing the totient function $\varphi(n)$, leading to Euler's theorem.

Through this historical narrative, students come to realize that Fermat's Little Theorem is not a trivial corollary but an important starting point in the evolution of number-theoretic ideas. Euler's Theorem represents a systematic generalization built upon earlier insights. This perspective deepens understanding of the theorems themselves and highlights essential values such as persistence, critical revision, and innovation in scientific research.

4. TEACHING OUTCOMES AND EDUCATIONAL SIGNIFICANCE

Teaching practice indicates that incorporating mathematical history and mathematicians' narratives into Foundations of Information Security Mathematics produces noticeable positive effects. Students demonstrate improved acceptance of abstract theorems, increased classroom participation, and greater willingness to engage in discussion. More importantly, they begin to focus on proof strategies and mathematical reasoning rather than merely memorizing formulas.

Historical guidance also helps students form a more accurate understanding of scientific research as a cumulative and iterative process, thereby fostering a rigorous, truth-seeking, and exploratory scientific mindset.

5. EXTENSION TO OTHER COURSE TOPICS

Beyond Fermat-related theorems, the course also involves contributions from many other mathematicians, such as Sun Zi and the Chinese Remainder Theorem, Eratosthenes and systematic prime sieving, and Euclid and the Euclidean algorithm. These historical materials can similarly serve as effective carriers of curriculum ideology across different instructional topics.

6. CONCLUSION

Integrating the history of mathematics and mathematicians' stories into Foundations of Information Security Mathematics offers an effective pathway for achieving deep integration between curriculum ideology and professional instruction. By reconstructing the developmental process of mathematical knowledge, this approach enhances learning interest and conceptual understanding while subtly guiding students toward scientific values and ethics. The proposed model demonstrates strong potential for broader application in mathematics education for information security programs.

ACKNOWLEDGMENT

Supported by 'the Fundamental Research Funds for the Central Universities (2023MS136)'.

REFERENCES

[1] Jia, C., Ha, G., Gao, M., & Wang, R. Exploration on teaching methods of information security mathematics fundamentals course oriented by application and practice. Computer Education, (9), 74–78, 2025.

[2] Ministry of Education of the People's Republic of China. Guidelines for Curriculum Ideology and Politics in Higher Education. Beijing, 2020.

[3] Chang, X.-M. Research on teaching reform of mathematics foundations for information security major. Modern Computer, (11), 2020.

[4] Qin, Y.-L., Hu, W., & Chen, Y. A practical exploration of curriculum ideology and politics construction of "Information Security Mathematics Foundation". Education and Teaching Forum, (11), 2025.

[5] Jia, C., Ha, G., Li, R., & Gao, M. Teaching practice of curriculum ideology and politics in the course "Information Security Mathematics Foundation". Computer Education, (6), 2023.

[6] Chen, G. L. Mathematical foundations of information security (2nd ed.). Tsinghua University Press, 2014.

[7] Zhang, W. The Warmth of History II. CITIC Press, 2018.