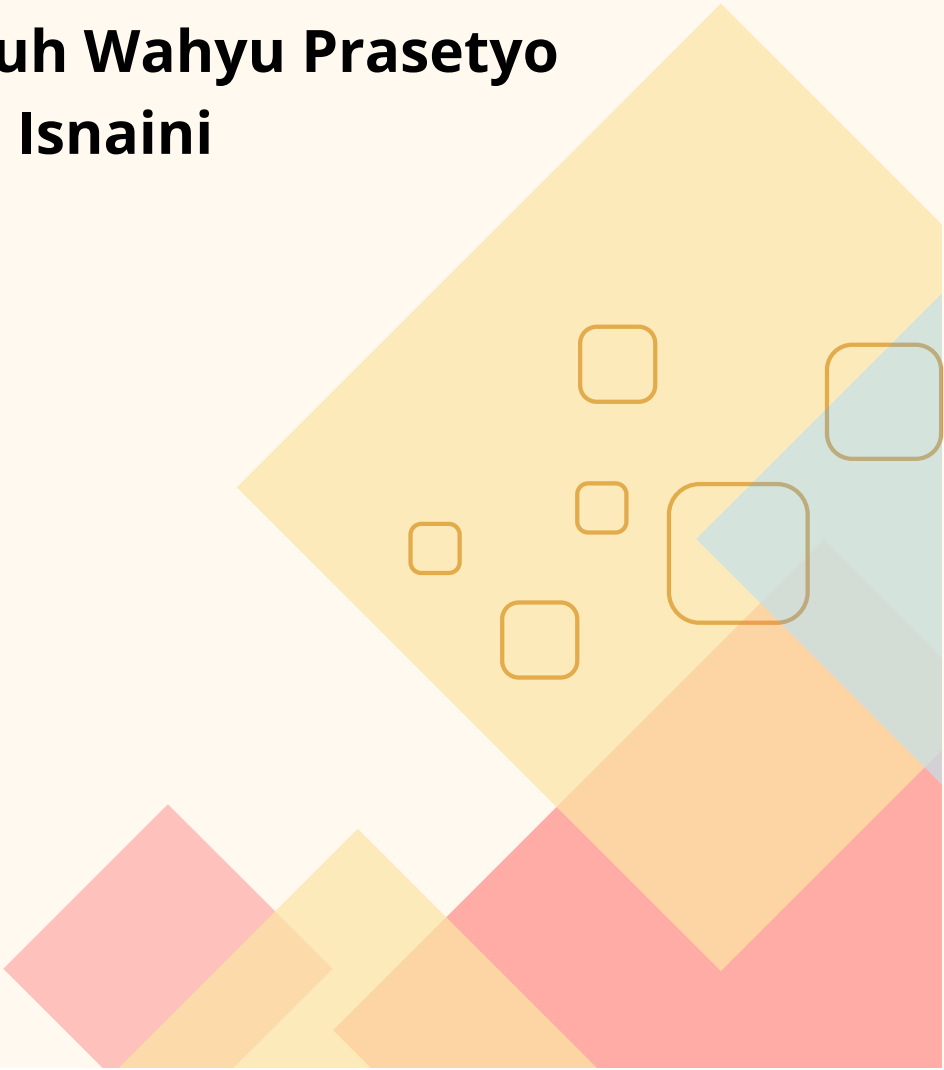


ISBN: 978-623-8449-06-4

Introduction to Number Theory

with Mathematical Problem Solving
Approach

Puguh Wahyu Prasetyo
Uha Isnaini



Introduction to Number Theory

(with Mathematical Problem Solving Approach)

Puguh Wahyu Prasetyo
Uha Isnaini



**Sanctions for Violation of Article 113
Law Number 28 of 2014
Regarding Copyright**

1. Any person who, without the right, commits a violation of economic rights as referred to in Article 9 paragraph (1) letter i for commercial use shall be punished with imprisonment for a maximum of 1 (one) year and/or a fine of up to Rp. 100,000,000 (one hundred million Indonesian Rupiah).
2. Any person who, without the right and/or without the permission of the Creator or Copyright Holder, commits a violation of the Creator's economic rights as referred to in Article 9 paragraph (1) letters c, d, f, and/or h for commercial use shall be punished with imprisonment for a maximum of 3 (three) years and/or a fine of up to Rp. 500,000,000.00 (five hundred million Indonesian Rupiah).
3. Any person who, without the right and/or without the permission of the Creator or Copyright Holder, commits a violation of the Creator's economic rights as referred to in Article 9 paragraph (1) letters a, b, e, and/or g for commercial use shall be punished with imprisonment for a maximum of 4 (four) years and/or a fine of up to Rp. 1,000,000,000.00 (one billion Indonesian Rupiah).
4. Any person who meets the elements as referred to in paragraph (3) committed in the form of piracy shall be punished with imprisonment for a maximum of 10 (ten) years and/or a fine of up to Rp. 4,000,000,000.00 (four billion Indonesian Rupiah)."

Introduction to Number Theory

(with Mathematical Problem Solving Approach)

Puguh Wahyu Prasetyo
Uha Isnaini



Introduction to Number Theory (with Mathematical Problem Solving Approach)

Copyright © 2023 Puguh Wahyu Prasetyo, Uha Isnaini

ISBN: 978-623-8449-06-4

16 x 24 cm, xiii + 206 pages

First Print, Desember 2023

Author : Puguh Wahyu Prasetyo, Uha Isnaini

Editor : UAD Press Editorial Team

Layouter : Puguh Wahyu Prasetyo

Cover Designer : Puguh Wahyu Prasetyo

Published by:

UAD PRESS

(Member of IKAPI and APPTI)

Address:

Kampus II Universitas Ahmad Dahlan

Jl. Pramuka No. 46, Sidikan, Umbulharjo, Yogyakarta.

Telp. (0274) 563515, Phone (+62) 882 3949 9820

All right reserved. All copyrights © Reproduction or alteration in any form through electronic, mechanical, photocopying, or recording of any part or the entirety of this book is not permitted without the written permission of the copyright owner.

Forewords

This book on number theory stands as a testament to the power of collaboration and the essence of problem-solving in mathematical exploration. Its inception and completion occurred within the brief yet intensive period of Dr. Prasetyo's visit to the Mathematics Department at the University of Toronto in Fall 2023. During this short visit but immensely productive stay, the vibrant academic environment and collaborative spirit fostered an atmosphere conducive to deep mathematical inquiry. Engaging discussions, shared insights, and collective problem-solving sessions formed the bedrock upon which this book was built. Number theory, a field revered for its elegance and depth, demands an approach rooted in problem-solving. The ethos of this book mirrors the ethos of the department—where mathematical problems serve as gateways to new vistas of understanding. Number theory also plays an important role since it is a background for further course including group theory and combinatorics. May this book serve as an invitation to enthusiasts, students, and scholars to embark on a journey of discovery, where the joy of solving problems illuminates the path to deeper mathematical truths.

Prof. Joe Repka, Ph.D
Mathematics Department of University of Toronto
Toronto, November 23, 2023

Preface

We begin by expressing our deepest gratitude to almighty Allah SWT for countless blessings, boundless mercy, and unwavering grace. It is through His divine guidance and providence that we are able to present to you the book "Introduction to Number Theory."

The primary distinction between this version and the previous one "Elementary Number Theory" lies in the approach we have taken. In this revised edition, we have placed a strong emphasis on problem-solving techniques right from the beginning. Our intention is to equip the reader with the skills and mindset necessary to delve into the intricacies of Number Theory with greater depth and intensity. This book has been meticulously crafted to serve as a valuable teaching resource for the Number Theory Course, catering to both undergraduate students pursuing pure mathematics and those specializing in mathematics education. Our aim in this book is to present the core concepts of Number Theory in a clear, effective, and easily comprehensible manner. We have strived to simplify complex topics, making them accessible to learners of all levels. Additionally, we have included a selection of challenging and competitive questions to stimulate critical thinking and further enhance your understanding of the subject. We extend our heartfelt appreciation to all those who have contributed to the completion of this book. Their unwavering support and dedication have been instrumental in bringing this project to fruition. However, we acknowledge that no work is without its imperfections, and we humbly welcome any suggestions, criticisms, and feedback from our readers. It is through your insights that we hope to refine and perfect this book in future editions.

In closing, it's important to note that the completion of this book took place in Toronto in the year 2023, coinciding with the active involvement of the first author, PWP, in the SAME (Scheme for Academic Mobility and Exchange) 2023 regular program at Mathematics Department, University of Toronto, Ontario, Canada as a visiting faculty. The convergence of these events underscores the collaborative and dynamic nature of the academic world, where ideas and knowledge are cultivated and shared.

As we present this book to our readers, our hope and aspiration are that it serve as a wellspring of knowledge and a source of inspiration. We envision it as a guiding light or all those who embark on the captivating journey of exploring the multifaceted and intriguing world of Number Theory. May the insights and wisdom contained within these pages ignite curiosity, spark intellectual inquiry, and foster a deeper appreciation for the beauty and intricacies of this mathematical discipline. Your engagement is crucial to us, and we wholeheartedly invite your valuable comments and suggestions to further enhance and refine this book. Your input

contributes to the ongoing journey of perfecting and enriching the content within these pages. It is through this collaborative effort that we can ensure the continuous improvement of the book, making it an even more valuable resource for all who seek knowledge in this subject matter.

Thank you for being an essential part of this endeavor. Any comments or suggestions can be shared via email at:

puguh.prasetyo@pmat.uad.ac.id.

May Allah's abundant blessings continue to envelop each and every one of us, providing the guidance and inspiration needed for a journey of ever-deepening understanding and wisdom.

With heartfelt gratitude and the warmest of regards

Toronto, November 2023

Author(s)

Acknowledgement

The first author extends heartfelt gratitude to the Directorate General of Higher Education, Research, and Technology, in collaboration with the Indonesia Endowment Fund for Education, for the Scheme for Academic Mobility and Exchange Regular 2023 Program under Grant Number: 3148/E4/DT.04.03/2023. This book was prepared during the first author's visiting program at the Mathematics Department of the University of Toronto, Toronto, Ontario, Canada, in Fall 2023 (September - November 2023).

Special thanks are extended to Professor Joe Repka, Professor Robert Jerrard, Professor Andrew Douglas, and the algebra guidance group of Professor Joe Repka, namely Jake Zimmermann, Esmeralda Tremblay, Noha ElGarem, and Xiao Ji. Their guidance and unwavering support have been of immense value. The first author would also like to express gratitude to Valeria Guio-Taylor, Zain Patel, and Sonja for their kindness and support.

Finally, the first author expresses gratitude to all parties from Universitas Ahmad Dahlan that have supported the first author's projects in Toronto. Without this invaluable support, the first author would not have been able to accomplish this achievement.

Dedication

To my wife, Isti Nur Chasanah,
To my son, Azka Praba Prasetyo,
To my parents and my whole family,
who have always supported me.

To my wife, Syarifah Inayati
To my daughter, Arsyila Faiha,
To my parents and my whole family,
who have always supported me.

Contents

Forewords	v
Preface	vi
Acknowledgement	viii
Decication	ix
Contents	x
List of Tables	xii
List of Figures	xiii
CHAPTER 1 MATHEMATICAL PROBLEM SOLVING	 1
1. 1. Mathematical Problem-Solving Steps	1
1.1. 1. Understand the Problem:	1
1.1. 2. Visualize or Draw a Diagram:	4
1.1. 3. Plan Your Approach:	6
1.1. 4. Use Mathematical Concepts:	8
1.1. 5. Solve Step by Step:	8
1.1. 6. Check Your Answer:	9
1.1. 7. Reflect and Reassess:	10
1.1. 8. Communicate Your Solution:	11
1.1. 9. Practice and Learn from Mistakes:	11
1.1. 10. Seek Help When Needed:	12
1. 2. How to Read This Book	13
CHAPTER 2 BASIC CONCEPT	 14
2. 1. Number System	14
2. 2. Mathematical Induction	15
2.2. 1. Principle of Mathematical Induction	19
2. 3. Binomial Theorem	38
2.3. 1. Binomial Expansion	39
2.3. 2. Approximations Using the Binomial Theorem	44
2.3. 3. Problems where the Power is Unknown	45
CHAPTER 3 DIVISIBILITY	 63
3. 1. Divisibility Relation	64
3. 2. Greatest Common Divisor (GCD)	69
3. 3. Least Common Multiple (LCM)	78
CHAPTER 4 INTEGERS BASES	 89
4. 1. Integers Bases	91

CHAPTER 5 INTEGER FACTORIZATION	 103
5. 1. Prime Number	104
5. 2. Unique Factorization	111
CHAPTER 6 CONGRUENCE	 123
6. 1. Concept and Basic Properties	124
6. 2. Application of Congruences	130
CHAPTER 7 DIOPHANTINE EQUATION	 144
7. 1. Linear Congruence	146
7. 2. Linear Diophantine Equation	149
7. 3. System of Linear Congruences	153
CHAPTER 8 FERMAT AND WILSON THEOREM	 182
8. 1. Fermat Theorem	182
8. 2. Wilson Theorem	188
REFERENCES	 198
GLOSSARIES	 202
INDEXES	 203
Biography First Author	 205
Biography Second Author	 206

List of Tables

1. 1. Differences in Purpose Aspects between Questions and Problems in Mathematics Learning.	2
1. 2. Assessment Differences between Questions and Problems in Mathematics Learning.	5
2. 1. Ancient Javanese-Arabic Number System	17
2. 2. Binomial Expansion	40
4. 1. Conversion Table	95
8. 1. The Integers Satisfying $ax \equiv 1 \pmod{13}$	190

List of Figures

1.1 Sieve of Eratosthenes:	7
4.1 Maya Numeral 20-Base:	90
6.1 Modular Arithmetic on 12-Hour Clock:	125

REFERENCES

- [1] Bağdat, A., EV Çimen, E. (2022). An Investigation of Sixth Grade Students' Skills of Solving and Posing Problems Which Require Using the Knowledge of Order of Operations. *International Journal of Educational Studies in Mathematics*, 9(3), 204–218. <https://doi.org/10.17278/ijesim.1146898>
- [2] Rosidah, S., Ilmi, N. (2021). Description of Students' Critical Thinking Skills in Solving Open Ended Problems Based on Their Learning Style. *ARRUS Journal of Mathematics and Applied Science*, 1(2), 89–100. <https://doi.org/10.35877/mathscience641>
- [3] Fyfe, Emily R., Rittle-Johnson, Bethany. (2017). Mathematics practice without feedback: A desirable difficulty in a classroom setting. *Instructional Science*. 45, 177–194.
- [4] Santos-Trigo, Manuel. (2007). Mathematical problem solving: an evolving research and practice domain. *ZDM* 39, 523–536.
- [5] Keng, Hua Loo., Yuan, Wang. (1981). *Applications of Number Theory to Numerical Analysis, 1st Edition*. Springer-Verlag Berlin Heidelberg, New York, USA.
- [6] Hunter, Jennifer., Turner, Irene., Russell, Charlotte., Trew, Karen., and Curry, Carol. (1993). Mathematics and the Real World. *British Educational Research Journal* 19, No. 1, 17-26.
- [7] Suherman., Vidákovich, Tibor. (2022). Assessment of mathematical creative thinking: A systematic review. *Thinking Skills and Creativity* 44 101019.
- [8] Dahal, Niroj., Manandhar, Netra Kumar., Luitel, Laxman., Luitel, Bal Chandra., Pant, Binod Prasad., Shrestha, Indra Mani. (2022). IICT tools for remote teaching and learning mathematics: A proposal for autonomy and engagements. *Adv Mobile Learn Educ Res* 2(1): 289-296.
- [9] Skovsmose, Ole. (2023). *Critical Mathematics Education*. Springer, New York, USA.

- [10] Khatin-Zadeh, Omid., Eskandari, Zahra., Marmolejo-Ramos, Fernando. (2022) Gestures Enhance Executive Functions for the Understating of Mathematical Concepts. *Integrative Psychological and Behavioral Science*. Published: 20 April 2022.
- [11] Verschaffel, Lieven., Schukajlow, Stanislaw., Star, Jon., and Van Dooren, Wim. (2020). Word problems in mathematics education: a survey *ZDM* 52:1–16 <https://doi.org/10.1007/s11858-020-01130-4>.
- [12] Hilbert, David. (1984). Mathematical Problems, A Book Chapter, *Mathematics People, Problems, Results by Douglas M. Campbell*. Chapman and Hall/CRC, New York, USA.
- [13] Patterson, Cody L., Parrott, Amy., Belnap, Jason. (2020). Strategies for assessing mathematical knowledge for teaching in mathematics content courses. *The Mathematics Enthusiast The Mathematics Enthusiast* Volume 17 Numbers 2 and 3.
- [14] Kazemi, Elham., Hintz, Allison. (2023). *Intentional talk: How to structure and lead productive mathematical discussions ebook version*. (Taylor and Francis Group, New York).
- [15] Zeitz, Paul. (2017). The art and craft of problem solving 3rd edition. John Wiley and Sons, Inc, USA.
- [16] Polya, G. (1990). *Mathematics and Plausible Reasoning, Volume 1: Induction and Analogy in Mathematics* (Princeton University Press, USA).
- [17] Polya, G. (1990). *Mathematics and Plausible Reasoning, Volume 1: Logic, Symbolic and mathematical* (Princeton University Press, USA).
- [18] Polya, G. (1973). *How to Solve It. A New Aspect of Mathematical Method Princeton*. Princeton University Press, USA.
- [19] Newman, R. S. (2017). Adaptive Help Seeking in *Handbook of Self-Regulation of Learning and Performance 2nd Edition*. Routledge, New York, USA.
- [20] Tavernor, Robert. (2007). Smoot’s Ear: The Measure of Humanity.
- [21] Nasmyth, K. (2022). *Nature Rev. Genet.* 23, 447–452.
- [22] van Dijk, P. J., Jessop, A. P., and Ellis, T. H. N. (2022). *Nature Genet.* 54, 926–933.

- [23] Zakon, Elias. (2023). *Mathematical Analysis*. University of Windsor. Open Education Resource (OER) LibreTexts Project (<https://LibreTexts.org>)
- [24] Eels, W. C. (1913). Number Systems of the North American Indians. *The American Mathematical Monthly* Volume 20, Issue 10.
- [25] Prasetyo, Puguh Wahyu., Isnaini, Uha., Prahmana, Rully., Nurnugroho, Burhanudin. (2020). *Elementary Number Theory*. Universitas Ahmad Dahlan Press, Yogyakarta, Indonesia.
- [26] Kleiner, Israel. (2000) From Fermat to Wiles: Fermat's Last Theorem Becomes a Theorem. *Elem. Math.* 55, 19-37.
- [27] Lecture note on Mathematical Induction. <https://web.stanford.edu/class/archive/cs/cs103/cs103.1242/lectures/13/>
- [28] Burton, D. M. (1986). *Elementary Number Theory Revised Printing*, Allyn and Bacon, Inc., Boston.
- [29] Hackman, P. (2007). *Elementary Number Theory*, HHH Production., Linköping.
- [30] Ore, O. (1948). *Number Theory and Its History*, McGraw-Hill Book Company, Inc., New York.
- [31] Rosen, K. H. (1993). *Elementary Number Theory and Its Applications, Third Edition*, Addison-Wesley Publishing Company., New York.
- [32] Sukirman. (2006). *Pengantar Teori Bilangan*, Hanggar Kreator., Yogyakarta.
- [33] Bressoud, David., and Wagon, Stan. (2000). *A Course in Computational Number Theory*. Key College Publishing. Springer. pp. 168–69
- [34] Gioia, Anthony. (2001). *Number Theory, an Introduction Reprint*, Dover
- [35] Everest, G., Ward, Thomas. (2006). *An Introduction to Number Theory*, Graduate Texts in Mathematics, vol. 232, Springer, p. 117.
- [36] Thomas Heath, Sir. (1981). *A history of Greek mathematics*. Vol. 2. Cambridge University Press: Cambridge.
- [37] Michael Mahoney, Sean. (1994). *The Mathematical Career of Pierre de Fermat, 1601–1665 (2nd ed.)*, Princeton University Press.

- [38] Gauss, Carl Friedrich., Clarke, Arthur A. (1986). *Disquisitiones Arithmeticae* (2nd corrected ed.), New York: Springer, ISBN 0-387-96254-9(translated into English).
- [39] Zerhusen A., Rakes, C., Meece, S. (1999). *Diophantine Equations*, University of Kentucky.,Kentucky.

GLOSSARIES

adjugate matrix:

is a matrix associated with a square matrix, especially in the context of linear algebra. 162

greatest common divisor:

The greatest common divisor (GCD) of two or more integers is the largest positive integer that divides each of the numbers without leaving a remainder. 71

integer bases:

in numeral systems is closely tied to the development of mathematics and the need to represent numbers. 89

least common multiple:

The least common multiple (LCM) of two or more integers is the smallest positive integer that is divisible by each of the given numbers. 78

Mathematical induction:

Mathematical induction is a method or principle used in mathematics to prove statements about an infinite sequence of objects or an infinite set of natural numbers. It establishes the validity of a proposition or formula for all elements within a certain set (usually the set of natural numbers). 16

Mathematical problem solving:

is a process that involves using mathematical principles, techniques, and strategies to analyze and find solutions to mathematical problems. 1

Sieve of Eratosthenes:

The Sieve of Eratosthenes is an ancient and efficient algorithm used to find all prime numbers up to a specified limit. Named after the Greek mathematician Eratosthenes, this method eliminates non-prime numbers from a list of integers. xiv, 7

INDEXES

- Brahmagupta, [144](#)
- Adjoint matrix, [162](#)
- Adjugate matrix, [162](#)
- Ancient Javanese numerals, [16](#)
- Application of Congruences, [130](#)
- Assessment, [4](#)
- Babylonian Base-60 System, [89](#)
- Beauty of mathematics, [8](#)
- Bhaskara's cyclic method, [15](#)
- Binary System, [89](#)
- Binomial coefficients, [41](#)
- Binomial Expansion, [39](#)
- Binomial Theorem, [38](#)
- Bézout's Identity, [74](#)
- Canonical form, [112](#)
- Check Your Answer, [9](#)
- Chinese Remainder Theorem, [155](#)
- Cofactor, [162](#)
- Communicate Your Solution, [11](#)
- Congruence, [123](#)
- Conversion Table , [95](#)
- Coprimality, [76](#)
- Coprime, [76](#)
- Cryptic Quadratic Cipher, [119](#)
- Cryptographic Code Breaker, [137](#)
- Cryptographic Congruence, [175](#)
- Diophantine equation, [144](#)
- Diophantus, [144](#)
- Disquisitiones Arithmeticae, [124](#)
- Divisibility, [63](#)
- Division Algorithm, [72](#)
- Egyptian Hieroglyphics, [89](#)
- Employee Shift Scheduling, [178](#)
- Enigmatic Encryption, [119](#)
- Euclid's Theorem, [113](#)
- Euler's Totient Function, [129](#)
- Exercise, [1](#)
- Fermat Theorem, [182](#), [183](#)
- Flight Connection Schedule, [180](#)
- Greatest Common Divisor, [69](#)
- Hanacaraka, [16](#)
- Highest common factor, [69](#)
- Hindu-Arabic Numeral System, [89](#)
- Integer bases, [89](#)
- Integer factorization, [103](#)
- John Wilson, [188](#)
- Least Common Multiple, [78](#)
- Level of Difficulty, [3](#)
- Mathematical Induction, [15](#)
- Mayan Base-20 System, [89](#)
- Modular arithmetic, [124](#)
- Modulo Scheduling, [178](#)
- Monic polynomial, [83](#)
- Multivariable linear congruences, [161](#)
- Octal and Hexadecimal Systems, [90](#)
- Pascal's triangle, [40](#)
- Pierre de Fermat, [182](#)
- Plan Your Approach, [6](#)
- Practice and Learn from Mistakes, [11](#)
- Primal Puzzle Palace, [121](#)

Prime factorization theorem, [107](#)
Prime Number, [104](#)
Prime Square Cipher, [120](#)
Prime testing, [108](#)
Problem, [11](#)

Quadratic Residue Encryption, [120](#)

Real-World Relevance, [4](#)
Reflect and Reassess, [10](#)
Rivest–Shamir–Adleman, [197](#)
Roman Numerals, [89](#)
RSA cryptosystem, [197](#)

Seek Help When Needed, [12](#)
Shadow puppetry, [16](#)
Sieve of Eratosthenes, [6](#)
Simple Secret Code Repository, [121](#)
Simple Secure Cryptographic Key,
[121](#)

Solution Approach, [3](#)
Solve Step by Step, [8](#)
Sun Zi, [154](#)
Symmetric matrix, [164](#)
System of Linear Congruences, [153](#)

The Enigmatic Equation, [119](#)
The Javanese calendar, [123](#)
The Prime Power Product, [119](#)
Train Schedule Optimization, [179](#)

Unique Factorization, [111](#)
Unusual Factorial Expression, [119](#)
Use Mathematical Concepts, [8](#)

Vigesimal System, [90](#)
Visualize or Draw a Diagram, [4](#)

Wilson Theorem, [188](#)

Zahlen, [15](#)

AUTHOR BIOGRAPHY



Puguh Wahyu Prasetyo is an associate professor in the Mathematics Education Department at Universitas Ahmad Dahlan. Born in Bora on July 22, 1988, he obtained his bachelor's degree in Mathematics from Yogyakarta State University in 2010, followed by a master's degree in Mathematics from Universitas Gadjah Mada in 2012. In 2018, he completed his doctoral degree in Mathematics at Universitas Gadjah Mada, under the supervision of Prof. Dr. rer.nat. Indah Emilia Wijayanti, M.Si; Prof. Dr. Halina France-Jackson; and Prof. Joe Repka, Ph.D.

During 2016, he served as an International Visiting Graduate Student at the University of Toronto under the supervision of Prof. Joe Repka. He successfully concluded his postdoctoral program in 2022 through collaborative research with Prof. Dr. rer.nat. Indah Emilia Wijayanti, M.Si (Universitas Gadjah Mada), and Prof. Hidetoshi Marubayashi, Ph.D (Naruto University of Education).

In Fall 2023, he participated in a visiting program at the Mathematics Department of the University of Toronto, focusing on Abstract Algebra and related concepts.

AUTHOR BIOGRAPHY



Uha Isnaini is a fulltime lecturer at the Department of Mathematics, Universitas Gadjah Mada, Indonesia. He received his bachelor and master degree from Universitas Gadjah Mada, and did his PhD at the National Institute of Education, Nanyang Technological University, Singapore. His research interests are Number Theory and Algebra.

Join an exciting journey into the captivating world of number theory with this comprehensive book tailored for problem-solving enthusiasts. It starts by exploring fundamental problem-solving strategies before diving into prime numbers and divisibility, unraveling their intricate properties and practical uses. As you progress, you'll master congruences, modular arithmetic, solve Diophantine equations, and wield number-theoretic functions. Discover the significance of quadratic residues and their role in cryptography. The pinnacle lies in an enthralling exploration of Fermat's Last Theorem and Wilson's Theorem. Throughout, engaging explanations, vivid examples, and diverse problem sets empower readers to conquer number theory, culminating in a confident grasp of these enduring theorems.

