}essentials{

Thorsten Holm

Modulare Arithmetik

Von den ganzen Zahlen zur Kryptographie

Springer Spektrum

essentials

essentials liefern aktuelles Wissen in konzentrierter Form. Die Essenz dessen, worauf es als „State-of-the-Art“ in der gegenwärtigen Fachdiskussion oder in der Praxis ankommt. *essentials* informieren schnell, unkompliziert und verständlich

- als Einführung in ein aktuelles Thema aus Ihrem Fachgebiet
- als Einstieg in ein für Sie noch unbekanntes Themenfeld
- als Einblick, um zum Thema mitreden zu können

Die Bücher in elektronischer und gedruckter Form bringen das Expertenwissen von Springer-Fachautoren kompakt zur Darstellung. Sie sind besonders für die Nutzung als eBook auf Tablet-PCs, eBook-Readern und Smartphones geeignet. *essentials:* Wissensbausteine aus den Wirtschafts-, Sozial- und Geisteswissenschaften, aus Technik und Naturwissenschaften sowie aus Medizin, Psychologie und Gesundheitsberufen. Von renommierten Autoren aller Springer-Verlagsmarken.

Weitere Bände in der Reihe http://www.springer.com/series/13088

Thorsten Holm

Modulare Arithmetik

Von den ganzen Zahlen zur Kryptographie

Springer Spektrum

Thorsten Holm
Institut für Algebra, Zahlentheorie und
Diskrete Mathematik,
Leibniz Universität Hannover
Hannover, Deutschland

ISSN 2197-6708 ISSN 2197-6716 (electronic)
essentials
ISBN 978-3-658-31945-8 ISBN 978-3-658-31946-5 (eBook)
https://doi.org/10.1007/978-3-658-31946-5

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung/Lektorat: Iris Ruhmann
Springer Spektrum ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Was Sie in diesem *essential* finden können

- Eine Einführung in die modulare Arithmetik, die mit recht wenig Vorkenntnissen zugänglich und mit vielen Beispielen illustriert ist.
- Einen Rückblick auf den Zahlbereich der ganzen Zahlen und eine ausführliche Behandlung der Teilbarkeit.
- Den Euklidischen Algorithmus zur Berechnung eines größten gemeinsamen Teilers.
- Grundlegende Eigenschaften von Primzahlen.
- Die Einteilung der ganzen Zahlen in Restklassen modulo einer natürlichen Zahl. Neue Zahlbereiche $\mathbb{Z}_n$ mit endlich vielen Elementen und eine ausführliche Behandlung ihrer Rechenregeln.
- Teilbarkeitsregeln für ganze Zahlen und ihre Begründung mit Hilfe der modularen Arithmetik.
- Lösungsverfahren für simultane Kongruenzen und den Chinesischen Restsatz.
- Die Eulersche φ-Funktion und ihre Anwendung beim effizienten Rechnen in den Zahlbereichen $\mathbb{Z}_n$.
- Eine Beschreibung des für viele moderne Anwendungen grundlegenden RSA-Verschlüsselungsverfahrens.