BARCODE

checksum

Prüfziffer

ISBN

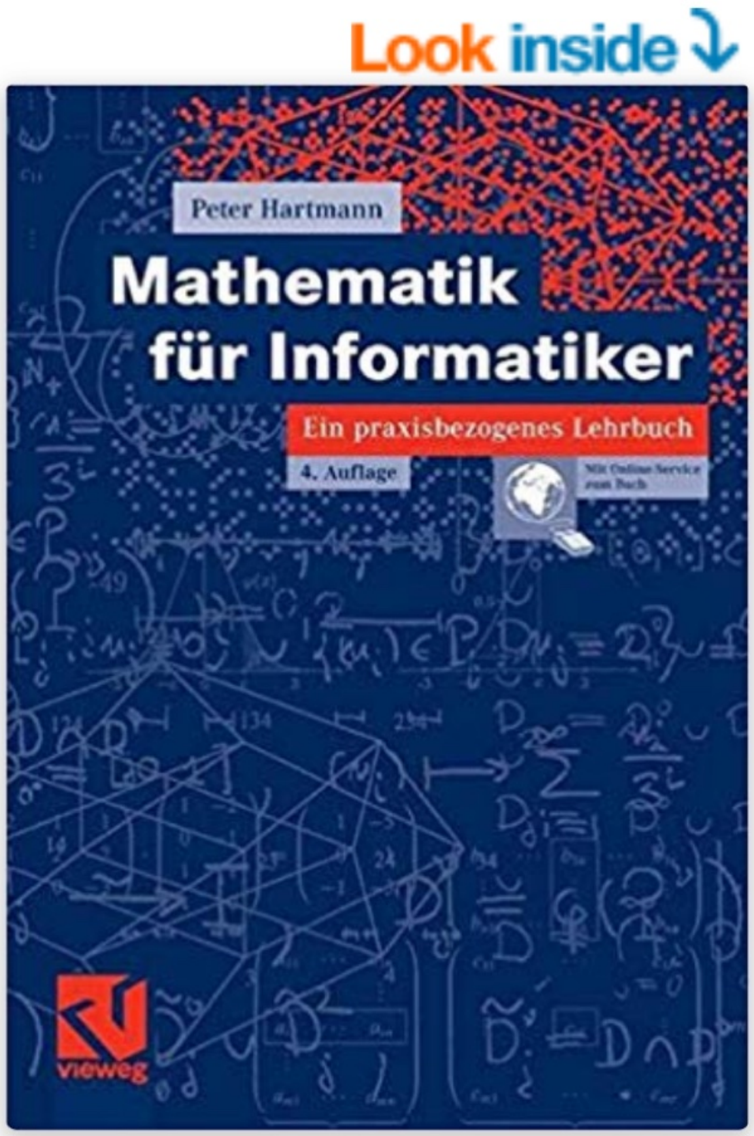
Hash

digital signature

amazon.com

Books Advanced Search New Releases Amazon Charts Best Sellers & More The New York Times®

Books › Computers & Technology › Databases & Big Data



See this image

Mathematik für Informatiker: Ein praxisbezogenes Lehrbuch (German Edition) (German) Paperback – March 27, 2006

by Peter Hartmann (Author)

Be the first to review this item

ISBN-13: 978-3834800961 | ISBN-10: 3834800961 | Edition: 4, überarb. Aufl. 2006

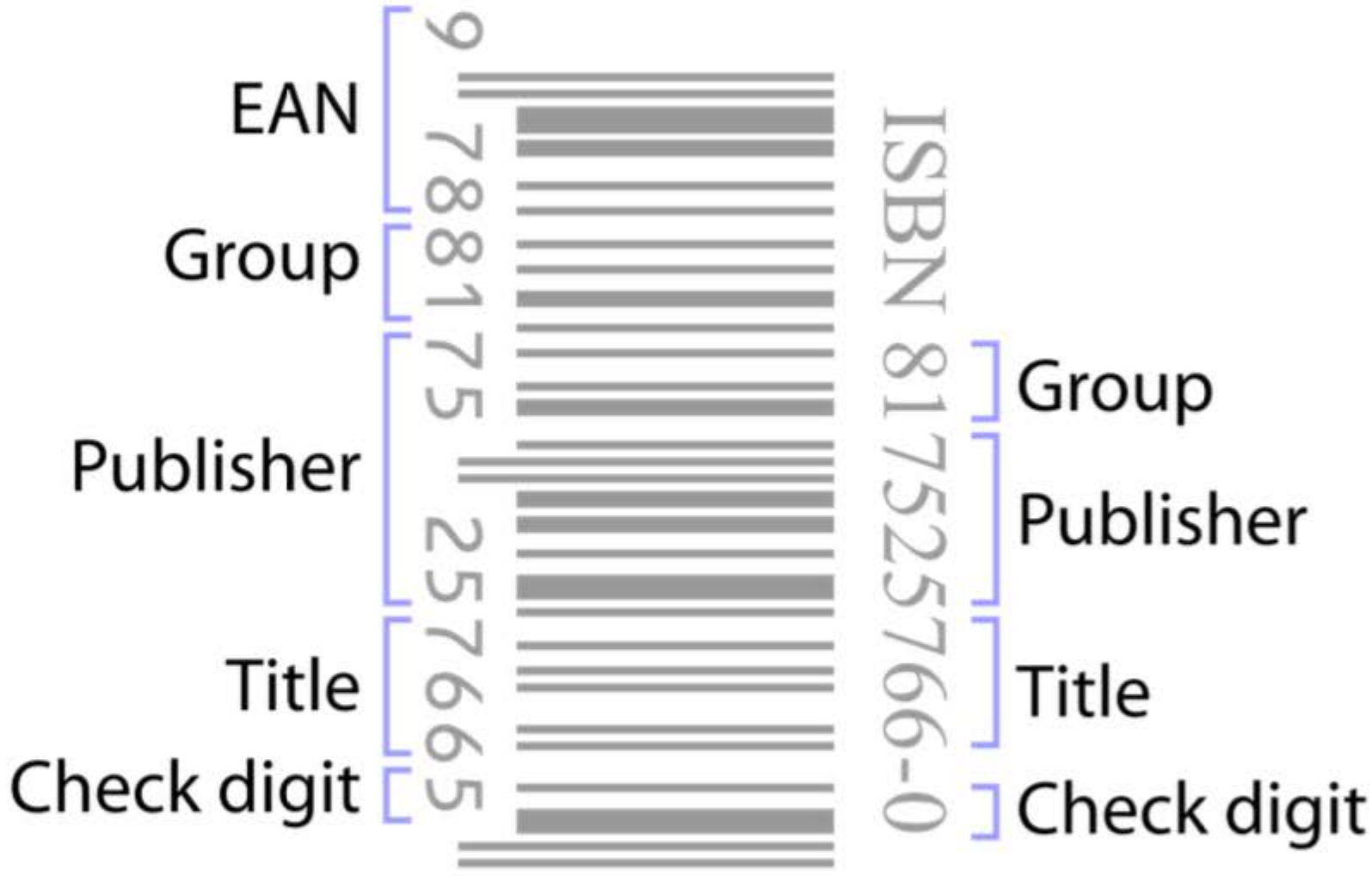
Used

Price: $37.08

5 Used from $33.15

› See all 6 formats and editions

Kindle	**Paperback**
$31.00	**from $33.15**
Read with Our **Free App**	5 Used from $33.15


EAN
Group
Publisher
Title
Check digit
9 788175 257665
ISBN 81752576 6-0
Group
Publisher
Title
Check digit

PRÜFZIFFER

3834800361

↑ Prüfziffer / checksum / hash

$Y = a_1 a_2 a_3 a_4 \dots a_{10} \qquad a_i \in \{0, \dots, 9\}$

checksum $\quad a_{10} \equiv 1 \cdot a_1 + 2 \cdot a_2 + 3 \cdot a_3 + \dots + 9 \cdot a_9 \mod 11$

Übung: check checksum ✓

Exkurs: $1 + 2 + 3 + 4 + \dots + 97 + 98 + 99 + 100 = \sum_{k=1}^{100} k$ ($\Sigma \sim$ Sigma)

Bsp: $\sum_{k=1}^{4} k^2 = 1^2 + 2^2 + 3^2 + 4^2 = 30$

→ ISBN 10er : $a_{10} \equiv \sum_{k=1}^{9} k \cdot a_k \mod 11$ checksum

Vertipper werden bemerkt

Wir vertippen uns an Stelle i $\rightsquigarrow y'$

Merkt dies die checksum? Ja, in der Tat:

Betrachte $a_{10} - a'_{10} \equiv i \cdot a_i - i \cdot a'_i \equiv i \cdot (a_i - a'_i) \not\equiv 0$

Satz: Für $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$ gilt:

$$p \nmid a \text{ und } p \nmid b \Rightarrow p \nmid a \cdot b$$

Beweis: Es gelte $p \nmid a$ und $p \nmid b$. Da $p \in \mathbb{P}$, kommt p weder in der Primfaktorzerlegung von a noch in der Primfaktorzerlegung von b vor. Daher auch nicht in der Primfaktorzerlegung von $a \cdot b$. D.h. p teilt $a \cdot b$ nicht. □

Übung: Vertippe dich irgendwo und überprüfe, dass die checksum es registriert.

Wenn du dich 2x vertippst, wann merkt es die checksum nicht?

23. 4. 19

Recap ISBN-10 an einem selbstgewählten Beispiel

→ Marco Polo : Reiseführer München

3 - 8297 - 2843 - **3**

ISBN-10 : $\sum_{k=1}^{9} k \cdot a_k \mod 11 \equiv a_{10}$

also $1\cdot 3 + 2\cdot 8 + 3\cdot 2 + 4\cdot 9 + 5\cdot 7 + 6\cdot 2 + 7\cdot 8 + 8\cdot 4 + 9\cdot 3 \equiv$

$\equiv 4 + 5 - 5 + 3 + 2 + 1 + 1 - 1 + 5$

$\equiv 14 \equiv 3$ ✓

Selbständig lesen/verstehen : **Vertauscher** (Skript p. 54)

Osterformel von Gauss (Skript p. 55)

Wie immer : Teste mit selbst gewählten Beispielen.

Modulo 17 Gruppe

Betrachte Potenzen von 3 mod 17

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
3^n	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	3

$\langle \mathbb{Z}_{17}^*, \cdot \rangle$ Gruppe

$\mathbb{Z}_{17}^* = \{1, 2, 3, \dots, 16\}$

Für $a \in \mathbb{Z}_{17}^*$, dann ist $a^{16} \equiv 1$

Beweis: $a^{16} \Rightarrow \exists k \in \mathbb{N}$ mit $a = 3^k$

$$\Rightarrow a^{16} = (3^k)^{16} = (3^{16})^k = 1^k = 1 \qquad \square$$

Eine erste Idee von "Verschlüsselung"

$a^1 \equiv a$, $a^{17} \equiv a^{16} \cdot a \equiv 1 \cdot a \equiv a$

$a^? \equiv a$ z.B. $? = 33$

$a^{49} \equiv a$

$a^{65} \equiv a$

Nimm z.B. $a^{65} \equiv a$

Bem.: $65 = 5 \cdot 13$

Wir schicken ein $c \sim 3$ an Wa]

Verschlüsseln $3^5 \bmod 17 \equiv 5$

$5^{13} \bmod 17 \equiv 3$

-> Mache selber Beispiele.

da $(3^5)^{13} \equiv 3^{65} \equiv 3 \mod 17$

Üben könnte man z.B. auch mod 29
(so kann man alle Buchstaben (26) miteinbeziehen).
Es gilt dann für $a \in \mathbb{Z}_{29}^*$

$a^{28} \equiv 1 \mod 29$

Modulo 17 Gruppe

Betrachte Potenzen von 3

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
3^n	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	3

$\cdot 3$ $\cdot 3$

$$\mathbb{Z}_{17}^* = \{1, 2, 3, \dots, 15, 16\}$$

$$\langle \mathbb{Z}_{17}^*, \cdot \rangle$$

Wie viel gibt, für $a \in \mathbb{Z}_{17}^*$, $a^{16} \equiv$? Gibt immer 1.

In der Tat: $a^{16} \Rightarrow \exists k \in \{0, \dots, 16\}$ mit $a = 3^k$

$$\Rightarrow a^{16} \equiv (3^k)^{16} \equiv (3^{16})^k \equiv (1)^k \equiv 1. \qquad \square$$

$a^{16} \equiv 1$

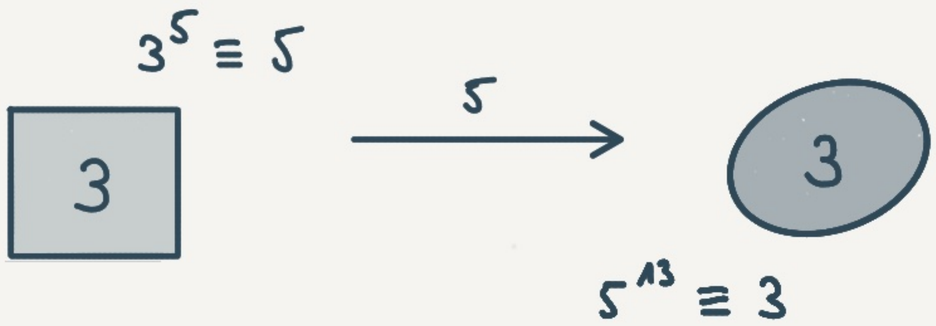
$a^{17} \equiv a^{16} \cdot a \equiv 1 \cdot a \equiv a$

$a^{?} \equiv a \qquad ? = 33$

$a^{49} \equiv a$
$a^{65} \equiv a \qquad a^{65} \equiv (a^5)^{13}$
$a^{81} \equiv a$

Verschlüsseln : $c \rightsquigarrow 3$

$3^5 \equiv 5 \mod 17$
$\downarrow$ send
$5^{13} \equiv 3 \mod 17$



(Funktioniert, da $(3^5)^{13} \equiv 3^{65} \equiv 3 \mod 17$)

Übung mod 29

ver- & entschlüsseln

Bem.: Es gilt für $a \in \mathbb{Z}_{29}^*$

$$a^{28} \equiv 1 \mod 29$$

Häppchenweise... (siehe $2^{666} \mod 9$)

$13^4 \equiv 25$

$13^{16} \equiv (13^4)^4 \equiv 25^4 \equiv 24$

$13^{19} \equiv 13^{16} \cdot 13^3 \equiv 24 \cdot 13^3 \equiv 6$

VIGENÈRE KNACKEN

Crash Course
Wahrscheinlichkeitsrechnung

Wkeit für eine "5" beim Würfeln: $\frac{1}{6} = \frac{g}{m}$ ← "möglich" ← "günstig"

Wkeit keine "5": $\frac{5}{6} = 1 - \frac{1}{6}$

Wkeit mit 2 Würfeln eine Doppelsechs zu werfen? ("66")

$$\frac{1}{6} \cdot \frac{1}{6} = \frac{1}{36}$$

Wkeit mit 2 Würfeln die Augenzahl 10 zu werfen?

$$\frac{1}{6} \cdot \frac{1}{6} + \frac{1}{6} \cdot \frac{1}{6} + \frac{1}{6} \cdot \frac{1}{6} = \frac{3}{36}$$

Friedmann

$\frac{1}{26}$ (Kunstsprache)

$$K_G = \frac{1}{n} \cdot K_M + \left(1 - \frac{1}{n}\right) \cdot (3.85\,\% + \varepsilon)$$

mit n Kasiski-Spalten

↑ vermutete Schlüsselwortlänge

$$\Rightarrow \quad n = \frac{K_M - 3.85\,\% - \varepsilon}{K_G - 3.85\,\% - \varepsilon}$$