Prof. Dr. M. Helbig
Mathematik – Übung

Hochschule Rosenheim
University of Applied Sciences

Kongruenzen

Fragen?

- $115 + 238 \equiv 5 + 3 = 8 \equiv 3 \pmod 5$

  (115: 111 → 5; 238: 111 → 3)

- $115 \equiv 0 \pmod 5$ $\qquad 115 = q \cdot 5 + 0$

  0: Rest

  oder Rest + $q \cdot 5$

- Prüfzifferberechnung? Dabei muss man Module/mit Kongruenzen rechnen!

Kongruenzen, Teil 1. Begründen Sie:

* 1. $17 \equiv 22 \pmod 5$

2. $15 \equiv 3 \pmod{12}$

Lösung.

1. nach Def: $17 \bmod 5 = 2$ (Rest), $22 \bmod 5 = 2$ ✓ (Div. mit Rest!)

[NR: $17 = 3 \cdot 5 + 2$, $22 = 4 \cdot 5 + 2$]

ODER

Satz: $5 \mid -5 = 17 - 22$ ✓

Bemerkung: $\exists\, q \in \mathbb{Z}: \; 5 \cdot q = 17 - 22 \iff \exists\, q \in \mathbb{Z}: \; 17 = 22 + 5 \cdot q$

d.h. $17 = 22$ „bis auf ein Vielfaches von 5"

2. $15 \bmod 12 = 3 = 3 \bmod 12 \implies 15 \equiv 3 \pmod{12}$.

Eigener Lösungsversuch.

Kongruenzen, Teil 2. Berechnen Sie:

* 1. $1243 + 25689 \equiv ?\ (\mathrm{mod}\ 5)$

2. $1243 + 25689 \equiv ?\ (\mathrm{mod}\ 2)$

3. $1243 \cdot 25689 \equiv ?\ (\mathrm{mod}\ 3)$

4. $1293^{128} \equiv ?\ (\mathrm{mod}\ 8)$

Lösung.

1. $1243 + 25689 \equiv 3 + 4 = 7 \equiv 2 \pmod 5$.

2. $1243 + 25689 \equiv 1 + 1 = 2 \equiv 0 \pmod 2$

3. $1243 \cdot 25689 \equiv 1 \cdot 0 = 0 \pmod 3$

$1243 = 414 \cdot 3 + 1$ (1242) $\qquad 25689 = 8563 \cdot 3 + 0$ oder Quersumme 30 durch 3 teilbar!

4. $1293^{128} \equiv 5^{128} = (5^2)^{64} \equiv 1^{64} = 1 \pmod 8$

$1293 = 161 \cdot 8 + 5$ $\qquad 5^2 = 25 \equiv 1$

Algorithmus schnelles Potenzieren:

$$a^{2193} = a^{1071 \cdot 2 + 1} = (a^2)^{1071} \cdot a = (a^2)^{535 \cdot 2 + 1} \cdot a$$

$$= ((a^2)^2)^{535} \cdot a^2 \cdot a = (((a^2)^2)^{267} \cdot (a^2)^2 \cdot a^2 \cdot a = \ldots$$

Berechne anstatt $\underbrace{a \cdot a \cdot a \cdot \ldots \cdot a}_{2193\times}$ nur iterierte Quadrate $a, a^2, (a^2)^2, ((a^2)^2)^2, \ldots$

↑ viel weniger Multiplikationen!

Eigener Lösungsversuch.

Anwendungen modulo-Rechnung.

- → Homepage
- Download Dateien: Hashwert mit md5, CRC32, SHA (Demo Cygwin: ~~md5sum~~)
- IBAN
- ISBN

sha512 ↓ Secure Hash Algorithm

sha512 eclipse download

In Cygwin: sha512sum ecl....exe

ISBN-10. Beispiel auf amzaon.de:

Produktinformation

Taschenbuch: 608 Seiten
Verlag: Goldmann Verlag; Auflage: Goldmann Verlag (3. September 2012)
Sprache: Deutsch
ISBN-10: 3442478960 ← Prüfziffer!
ISBN-13: 978-3442478965
Originaltitel: Fifty Shades Darker

Wikipedia sagt dazu:

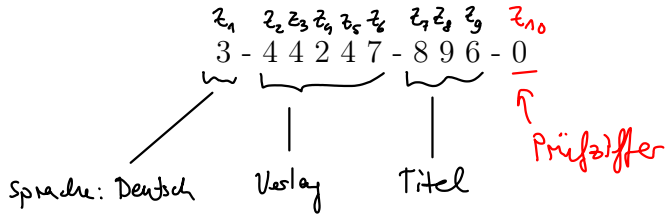
ISBN-10 [Bearbeiten]

Bei der ISBN-10 wird die Prüfziffer wie folgt berechnet: Bezeichnet man die ersten neun Ziffern mit z_1 bis z_9, so gilt für die Prüfziffer an der zehnten Stelle:

$$z_{10} = \left(\sum_{i=1}^{9} i \cdot z_i\right) \mod 11$$
$$= (1 \cdot z_1 + 2 \cdot z_2 + 3 \cdot z_3 + 4 \cdot z_4 + 5 \cdot z_5 + 6 \cdot z_6 + 7 \cdot z_7 + 8 \cdot z_8 + 9 \cdot z_9) \mod 11$$

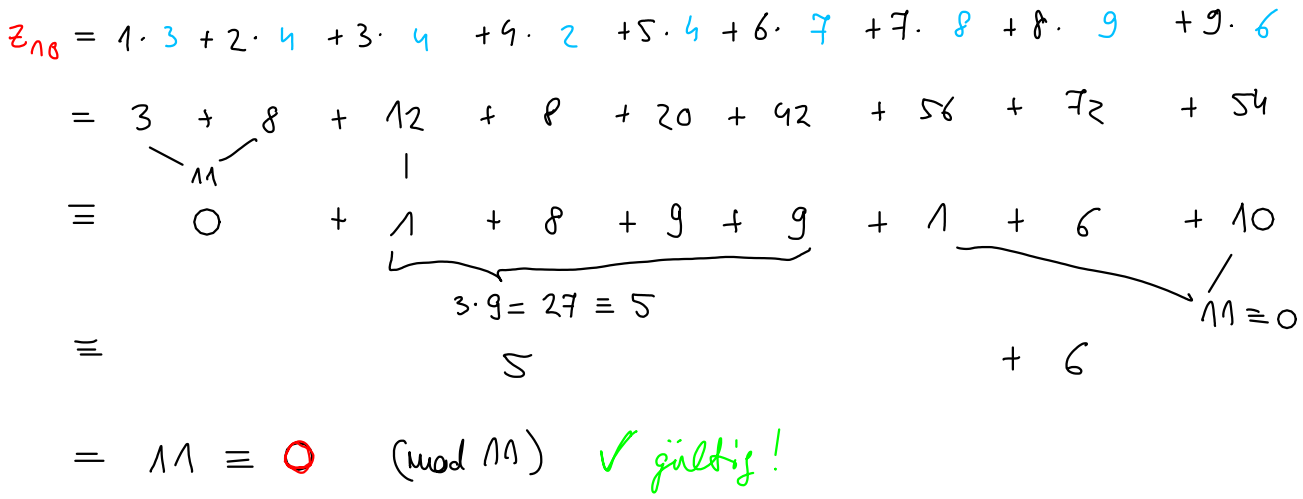
ODER: $0 = (10 \cdot z_1 + 9\, z_2 + \ldots + 2 z_9 + 1 z_{10}) \mod 11 \iff z_{10} = \underbrace{-10}_{\equiv 1} z_1 + \underbrace{(-9)}_{\equiv 2} z_2 + \ldots + \underbrace{(-2)}_{\equiv 9} z_9 \mod 11$

Aufbau der ISBN-10:



ISBN-10. Ist obige ISBN 3-44247-896-0 gültig?
Zusatz: Schreiben Sie in C einen Validator!

Lösung.



Eigener Lösungsversuch.