Anwendungen in Codierungstheorie und Kryptographie

Codierungstheorie $\rightsquigarrow$ Sicherung von Kommunikation gegen Übertragungsfehler

Kryptographie $\rightsquigarrow$ Geheimhaltung der Kommunikation

1. Codierungstheorie

Zwei Aufgaben:

- Erkennen von Fehlern
- Korrigieren —"—

Idee: Vergrößere zu übertragende Nachricht durch zusätzliche Zeichen

Prüfziffer-Verfahren

Bsp. (alte) ISBN

3-540-29854-0

(10-stellige Zahl)

Aufbau: 9-stellige Zahl

$a_1 a_2 \dots a_9$

Prüfziffer a_{10}

a_{10} wird so gewählt, daß

$$1 \cdot a_1 + 2 \cdot a_2 + \dots + 9 \cdot a_9 + 10 \cdot a_{10} \equiv 0 \mod 11$$

obiges Beispiel:

$$1 \cdot 3 + 2 \cdot 5 + 3 \cdot 4 + 4 \cdot 0 + 5 \cdot 2 + 6 \cdot 9 + 7 \cdot 8 + 8 \cdot 9 + 9 \cdot 4 = 253$$

$$\rightsquigarrow \quad 253 + 10\, a_{10} \equiv 0 \mod 11$$

$$253 = 23 \cdot 11 \quad \Rightarrow \quad a_{10} = 0$$

weiteres Beispiel:

3-528-06752-2.

$\Rightarrow 194 + 10 a_{10} \equiv 0 \mod 11$

$194 = 17 \cdot 11 + 7$

$\Rightarrow 7 + 10 a_{10} \equiv 0 \mod 11$

$\Rightarrow 10 a_{10} \equiv 4 \mod 11$

$-1 \cdot 10 + 1 \cdot 11 = 1$

multiplikatives Inverses zu 10 mod 11 $= -1 \equiv 10 \mod 11$

$\Leftrightarrow a_{10} \equiv 40 \mod 11$

$\equiv 7 \mod 11$

Bsp.: EAN (neue ISBN)

13-stellige Zahlen

979 - 3 - 540 - 29854 - 6

12 Ziffern = eigentliche EAN

$a_1 a_2 \dots a_{12}$

a_{13} Prüfziffer

$$a_1 + 3a_2 + a_3 + 3a_4 + \dots + a_{11} + 3a_{12} + a_{13} \equiv 0 \mod 10$$

Bsp.: $124 + a_{13} \equiv 0 \mod 10$

Beispiel eines fehlerkorrigierenden Codes

Ziel: übertrage Worte mit vier Buchstaben

1. Schritt: Ersetze Buchstaben in Zahlen um

A $\to$ 1, B $\to$ 2, ..., Z $\to$ 26

Bsp.: WORT $\to$ 23, 15, 18, 20

allgemein: $w = a_2 a_3 a_4 a_5$

$a_i \in \{1, 2, \ldots, 26\}$

Codierung: füge am Anfang zwei Zeichen $a_0, a_1 \in \mathbb{Z}_{31}$ an, so daß

$$a_0 + a_1 + a_2 + a_3 + a_4 + a_5 \equiv 0 \mod 31$$

$$a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 \equiv 0 \mod 31$$

Bsp.: $w = 23, 15, 18, 20$

$$\Rightarrow \quad a_0 + a_1 + 76 \equiv 0 \mod 31$$

$$a_1 + 263 \equiv 0 \mod 31$$

$$\Rightarrow \quad a_0 + a_1 \equiv 17 \mod 31$$

$$a_1 \equiv 16 \mod 31$$

$$\Rightarrow a_0 = 1, \quad a_1 = 16$$

$\Rightarrow$ übertragen wird $1, 16, 23, 15, 18, 20$