Prüfziffern & die ISBN-Nummer

Anfang 2007 wurde die neue ISBN (ISBN-13) Nummer eingeführt. Dies ist eine 13-stellige Nummer, die zur Kennzeichnung von Büchern oder anderen Veröffentlichungen dient.

Die ISBN-13 Nummer hat die bis 2007 gültige ISBN-10 Nummer abgelöst, da die gültigen ISBN-10 Nummern im englischsprachigen Raum knapp wurden.

Die neue ISBN-13 Nummer besteht aus 5 Bestandteilen, (A)-(E).

Die Länge von (A)-(D) beträgt genau 12 Ziffern.

(A) = 3-stellige Ländernummer, ähnlich der EAN (=european article number)

(B) = Gruppennummer für geografische oder Sprach- oder ähnliche Gruppen z.B. 0, 1 engl. sprachiger Raum (USA, England, Simbabwe)
2 franz. sprachiger Raum

(C) = Verlagsnummer (2-7 Stellen)

(D) = Band oder Titelnummer (2-7 Stellen)

(E) = Prüfziffer = Einstellige Nummer, die die formale Richtigkeit der ISBN garantiert.

Eine 13-stellige Nummer $(x_1 \dots x_{13})$ ist eine gültige ISBN-13 Nummer, falls

$x_1 + 3x_2 + x_3 + \dots + 3x_{12} + x_{13} \equiv 0 \mod 10$ erfüllt ist.

(Insb. lässt sich eine gültige Prüfziffer x_{13} zu einer beliebigen 12-stelligen Nummer basteln.)

ISBN-13 Nummern sind häufig stabil gegenüber Übertragungsfehlern.

Was passiert, wenn sich ein Fehler beim Eintippen der ISBN-13 einschleicht? 05.06.18

Häufigste Fehler:

1) falsch eingetippte Ziffer

2) Vertauschen zweier Ziffern

zu 1) Da nach Satz 4.9. Kongruenzen der Form

$3x \equiv b \mod 10$

$x \equiv b \mod 10$

eindeutige Lösungen modulo 10 haben, wird eine ISBN-13 ungültig, falls eine der Ziffern x_i, $i \in \{1, \dots, 13\}$ falsch eingegeben wird.

zu 2) Zwei Ziffern werden vertauscht: Sei $(x_1 \dots x_{13})$ eine gültige ISBN-13 Nummer und $(y_1 \dots y_{13}) = (x_1 \dots x_{i-1} x_{i+1} x_{i+2} \dots x_{13})$

(i) Ist i gerade, so haben wir $3x_{i+1} + x_i$ statt $x_{i+1} + 3x_i$ in $y_1 + 3y_2 + \dots + y_{13} \equiv 0 \mod 10$ "eingebracht".

(ii) Ist i ungerade, so haben wir $x_{i+1} + 3x_i$ statt $3x_{i+1} + x_i$ „eingebracht".

Da $(x_1 \dots x_{13})$ eine gültige ISBN-13 war, ist $(y_1 \dots y_{13})$ genau dann eine gültige ISBN-13, wenn

$3x_{i+1} + x_i \equiv x_{i+1} + 3x_i \mod 10$.

$\Leftrightarrow 2(x_{i+1} - x_i) \equiv 0 \mod 10$

$\overset{\text{Kürzungs-}}{\underset{\text{satz}}{\Leftrightarrow}}$ $x_{i+1} - x_i \equiv 0 \mod 5$

$(y_1 \dots y_{13})$ ist also genau dann eine gültige ISBN-13, wenn x_i und x_{i+1} sich um ± 5 unterscheiden.

Teilbarkeitskriterien

Wir schreiben eine Zahl n im 10er System als

$n = (a_k \dots a_0)_{10} := a_k \cdot 10^k + a_{k-1} 10^{k-1} + \dots + a_1 \cdot 10 + a_0$

- Um zu überprüfen, ob n durch 2 oder 5 teilbar ist, reicht es sich die letzte Stelle a_0 anzuschauen

- Um zu überprüfen, ob eine Zahl durch $4 = 2^2$ oder $25 = 5^2$ teilbar ist, reicht es sich die letzten beiden Stellen der Zahl n anzuschauen.
(Analog kann man Teilbarkeitskriterien für höhere Potenzen 2 und 5 finden.)

Lemma 4.15 (Dreierregel)
Eine Zahl $n = (a_k \dots a_0)_{10}$ ist genau dann durch 3 teilbar, wenn die Quersumme $Q_1(n) = \sum_{i=0}^{k} a_i$ durch 3 teilbar ist.

Beweis:

$10 \equiv 1 \mod 3 \Rightarrow 10^i \equiv 1^i \equiv 1 \mod 3$

Also $n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv 0 \mod 3 \Leftrightarrow \underbrace{\sum_{i=0}^{k} a_i}_{Q_1(n)} \equiv 0 \mod 3$ ▨

Wir möchten weitere solcher Teilbarkeitsregeln herleiten:
Für eine Zahl $n = (a_k \dots a_0)_{10}$ definieren wir die alternierende Quersumme $Q_1'(n) = \sum_{i=0}^{k} (-1)^i a_i$

Allgemeiner definieren wir:

$Q_s(n) = \sum_{i \geq 0} (a_{is+s-1} \dots a_{is+1} a_{is})_{10} = (a_{s-1} \dots a_0) + (a_{2s-1} \dots a_s)$
die Quersumme der Stufe s. (= Summe aller s-stelligen Zahlen, die rechts beginnend aus n gebildet werden können)
&
$Q_s'(n) = \sum_{i \geq 0} (-1)^i (a_{is+s-1} \dots a_{is})_{10}$ die alternierende Quersumme der Stufe s.

Satz 4.16

Seien $n, s \in \mathbb{N}$. Dann gilt:

$n \equiv Q_s(n) \bmod 10^s - 1$

$n \equiv Q_s(n) \bmod 10^s + 1$

Beweis:

Sei $n = (a_k \dots a_0)_{10} = \sum_{j=0}^{k} a_j \cdot 10^j$

Es ist $\sum_{i \geq 0} \left(\sum_{\ell=0}^{s-1} a_{i \cdot s + \ell} \cdot 10^\ell \right) \cdot 10^{i \cdot s}$

$\overset{(i=0)}{=} (a_{s-1} \cdot 10^{s-1} + \dots + a_0 \cdot 10^0) 10^0 \overset{(i=1)}{+} (a_{2s-1} \cdot 10^{s-1} + \dots + a_s \cdot 10^0) 10^s$

$= \sum_{j=0}^{k} a_j \cdot 10^j = n$

Also $n = \sum_{j \geq 0} a_j 10^j = \sum_{i \geq 0} (a_{is+s-1} \dots a_{is+1} a_{is})_{10} \cdot 10^{is}$ (*)

Wegen:

$10^s \equiv 1 \bmod (10^s - 1)$ ist

$10^{is} \equiv 1^i \bmod (10^s - 1)$ (*a)

$\Rightarrow n \overset{(*)}{=} \sum_{i \geq 0} (a_{is+s-1} \dots a_{is})_{10} \cdot 10^{is}$

$\overset{(*a)}{\equiv} \underbrace{\sum_{i \geq 0} (a_{is+s-1} \dots a_{is})_{10} \cdot 1}_{= Q_s(n)} \bmod 10^{s+1}$

Für die zweite Formel bemerken wir, dass

$10^s \equiv -1 \bmod (10^s + 1)$

$\rightsquigarrow 10^{is} \equiv (-1)^i \bmod (10^s + 1)$

$\Rightarrow n \equiv \underbrace{\sum_{i \geq 0} (a_{is+s-1} \dots a_{is})_{10} \cdot (-1)^i}_{Q_s(n)} \bmod 10^s + 1.$ ∎

Korollar 4.17

Für $s = 1$ sagt der obige Satz, dass

$10^1 - 1 = 9 \mid n \iff 9 \mid Q_1(n)$

$10^1 + 1 = 11 \mid n \iff 11 \mid Q_1(n)$

Allgemeiner:

Ist p ein Primteiler von 10^3-1 (bzw. 10^3+1) so folgt mit dem Kürzungssatz, dass p genau dann n teilt, wenn p $Q_3(n)$ (bzw. $Q_3'(n)$) teilt.

Wegen $10^3-1 = 999 = 3^3 \cdot 37$ und $1001 = 7 \cdot 11 \cdot 13$ erhält man so:

$7 \mid n \iff 7 \mid Q_3'(n)$

$13 \mid n \iff 13 \mid Q_3'(n)$ oder

$37 \mid n \iff 37 \mid Q_3(n)$

① Der Satz von Euler & der kleine Satz von Fermat

Wir haben bereits gesehen, dass eine Kongruenz $a \cdot x \equiv 1 \mod m$ genau dann eine Lösung hat, wenn $ggT(a,m) = 1$.

Dies bedeutet, dass in diesem Fall das Element $[a] \in \mathbb{Z}/m\mathbb{Z}$ ein multiplikatives Inverses hat.

Mit dem erweiterten Euklidischen Algorithmus können wir dieses inverse Element berechnen.

Da $ggT(a,m) = 1$ $\exists x,y \in \mathbb{Z}$ mit $1 = a \cdot x + y \cdot m$

Da $a \cdot x \equiv 1 \mod m$ ist für $[x] \in \mathbb{Z}/m\mathbb{Z}$.

$[x] \cdot [a] = [1] \in \mathbb{Z}/m\mathbb{Z}$. $\overset{=}{x}$ (ab sofort, werden die Kl. weggelassen)

Wir schreiben auch $x = a^{-1}$ für das Inverse von $a \in \mathbb{Z}/m\mathbb{Z}$.

Definition 4.18

(a) $(\mathbb{Z}/m\mathbb{Z})^* = \{a \in \mathbb{Z}/m\mathbb{Z} \mid ggT(\underset{\text{Repräsentant der Klasse von } a}{a}, m) = 1$

$\iff a \in \mathbb{Z}/m\mathbb{Z}$ hat ein multipl. Inverses$\}$

↑ Klasse

heißt die Einheitengruppe von $\mathbb{Z}/m\mathbb{Z}$.

Elemente in $(\mathbb{Z}/m\mathbb{Z})^*$ heißen Einheiten

$(\mathbb{Z}/m\mathbb{Z})^*$ ist in der Tat bzgl. der durch die Multiplikation induzierten Verknüpfung eine Abelsche Gruppe.

(b) Ein reduziertes Restsystem modulo m ist eine Menge ganzer Zahlen, sodass jede ganze Zahl, die teilerfremd zu m ist zu genau einer Zahl aus dem Restsystem kongruent modulo m ist.

Die Menge $\{0 < a < m \mid ggT(a,m) = 1\}$ ist beispielsweise ein solches reduziertes Restsystem modulo m.

(c) Die Kardinalität eines reduzierten Restsystems, also die Ordnung der Gruppe $(\mathbb{Z}/m\mathbb{Z})^*$ bezeichnen wir mit $\varphi(m)$.

Die Funktion $\varphi: \mathbb{N} \to \mathbb{N}$, $m \to \varphi(m)$ heißt die Eulersche φ-Funktion.

Beispiel 4.19

Sei $m = 12$. Die Menge $\{1,5,7,11\}$ ist ein reduziertes Restsystem modulo 12.

Es gilt also $|(\mathbb{Z}/12\mathbb{Z})^*| = \varphi(12) = 4$

Lemma 4.20

Für eine Primzahl p ist $\varphi(p) = p-1$

Beweis:

$\forall j \in \{1, \dots, p-1\}$ gilt $ggT(j,p) = 1$ ☒

SATZ 4.21 (Euler)

Sei $a \in \mathbb{Z}$, $m \in \mathbb{N}$ mit $ggT(a,m) = 1$. Dann gilt: $a^{\varphi(m)} \equiv 1 \bmod m$.

Beweis:

Wir setzen $t = \varphi(m)$ und betrachten ein reduziertes Restsystem modulo m.

$R = \{r_1, \dots, r_t\}$.

Da $ggT(a,m) \overset{n.V.}{=} 1$ folgt mit dem Kürzungssatz, dass

$a \cdot r_i \equiv a \cdot r_j \bmod m$ genau dann, wenn

$r_i \equiv r_j \bmod m$.

Da die r_i ein reduziertes Restsystem bilden ist

$r_i \not\equiv r_j \bmod m \ \forall i \neq j$

$\Rightarrow a \cdot r_i \not\equiv a \cdot r_j \bmod m \ \forall i \neq j$.

$\Rightarrow$ Die Menge $A = \{a \cdot r_1, \dots, a \cdot r_t\}$ ist ebenfalls ein reduziertes Restsystem modulo m.

$$\Rightarrow \prod_{i=1}^{t} r_i \equiv \prod_{i=1}^{t} (a \cdot r_i) \equiv a^t \cdot \prod_{i=1}^{t} r_i \bmod m$$

Da die r_i teilerfremd zu m sind ist auch $\prod_{i=1}^{t} r_i$ teilerfremd zu m. $\Rightarrow a^t \equiv 1 \bmod m$.

$a^{\varphi(m)}$ ☒

Korollar 4.22 (Der kleine Satz von Fermat)

Sei $a \in \mathbb{Z}$ und p eine Primzahl. Dann gilt

(a) $p \nmid a$ so ist $a^{p-1} \equiv 1 \bmod p$

(b) Es gilt $a^p \equiv a \bmod p$

Beweis:

(a) Da $\varphi(p) = p-1$ folgt (a) aus dem Satz von Euler (4.21.)

(b) Gilt $p \nmid a$ so folgt (b) aus (a) wegen:

$$a^{p-1} \equiv 1 \bmod p \overset{\text{multipl. } a}{\Rightarrow} \underbrace{a \cdot a^{p-1}}_{=a^p} \equiv \underbrace{1 \cdot a}_{=a} \bmod p$$

Gilt $p \nmid a$ so ist $a \equiv 0 \mod p$. Also insbesondere $a = a^p \equiv 0 \mod p$ ☐

Definition 4.23

Sei $(G, \circ)$ eine Gruppe. Die Ordnung $ord(g)$ ist die kleinste Zahl r, für die gilt, dass $\underbrace{g \circ \dots \circ g}_{r\text{-mal}} = e_G$. Existiert kein solches r hat g unendliche Ordnung.

Die Ordnung $Ord_m(a)$ ist also die kleinste natürliche Zahl r mit $a^r \equiv 1 \mod m$. ($Ord_m(a) = Ord\,[a] \in (\mathbb{Z}/m\mathbb{Z})^*$)

Beispiel 4.24

Wir haben bereits gesehen, dass $\varphi(12) = 4$

Es ist $5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \mod 12$

Also $ord_{12}(5) = ord_{12}(7) = ord_{12}(11) = 2$

Lemma 4.25

Sei $a \in (\mathbb{Z}/m\mathbb{Z})^*$, dann teilt $ord_m(a)$ die Ordnung von $(\mathbb{Z}/m\mathbb{Z})^*$ also $\varphi(m)$.

Beweis:

Wir definieren $r := ord_m(a)$. Es gilt also $a^r \equiv 1 \mod m$.

Nach dem Satz von Euler gilt auch, dass $a^{\varphi(m)} \equiv 1 \mod m$.

Wir schreiben $g := ggT(r, \varphi(m)) = x \cdot r + y \cdot \varphi(m)$.

$\Rightarrow a^g = a^{x \cdot r} \cdot a^{y \cdot \varphi(m)} \equiv 1 \mod m$.

Da r die kleinste Zahl ist mit der Eigenschaft $a^r \equiv 1 \mod m$ folgt $r \mid g \Rightarrow g = z \cdot r$. Da $g = ggT(r, \varphi(m))$ ist $z = 1$ also $g = r$.

Insbesondere ist $r = ggT(r, \varphi(m))$ ein Teiler von $\varphi(m)$. ☐