Aufgabe 8.1

Die Berechnung der Prüfziffer für ISBN-Nummern basiert auf dem Modul 11, also kann der Rest zwischen 0 und 10 liegen. Statt 10 schreibt man X um nur ein Zeichen schreiben zu müssen.

$$1\cdot 1+2\cdot 2+3\cdot 3+4\cdot 9+5\cdot 0+6\cdot 9+7\cdot 0+8\cdot 2+9\cdot 9+10\cdot z_0=201+10\cdot z_0$$

Für ISBN Nummern muss gelten $11 \mid 201+10\cdot z_0$, also

$$201\equiv -10\cdot z_0 \bmod 11$$

$$\Leftrightarrow \quad 3\equiv z_0 \bmod 11$$

Die Prüfziffer ist also 3.

Aufgabe 8.2

Zu zeigen: $\forall n\in\mathbb{N}: \sum_{0\le k<n} q^k = 1+q+q^2+\ldots+q^{n-1}=\frac{1-q^n}{1-q}=\frac{q^n-1}{q-1}$

I.A.: Wir zeigen, die Aussage gilt für ein beliebiges, festes n, wir wählen $n=0$:

$$\forall n\in\mathbb{N}: \sum_{0\le k<0} q^k = 0 = \frac{1-q^0}{1-q}=\frac{q^0-1}{q-1}$$ (wahre Aussage)

I.S.: Wir zeigen: Gilt die Aussage für ein beliebiges, festes n, dann gilt sie auch für $n+1$:

$$\sum_{0\le k<n+1} q^k = \frac{1-q^n}{1-q}+q^n$$

$$\Leftrightarrow \quad \sum_{0\le k<n+1} q^k = \frac{1-q^n}{1-q}+\frac{(1-q)q^n}{1-q}$$

$$\Leftrightarrow \quad \sum_{0\le k<n+1} q^k = \frac{1-q^n+(1-q)q^n}{1-q}$$

$$\Leftrightarrow \quad \sum_{0\le k<n+1} q^k = \frac{1-q^n+q^{n+1}}{1-q}$$

$$\Leftrightarrow \quad \sum_{0\le k<n+1} q^k = \frac{1-q^{n+1}}{1-q}$$

■

Aufgabe 8.3

$$x \equiv 46\,199^{-1} \bmod 66\,013$$
$$\Leftrightarrow \quad 46\,199x = 1 \bmod 66\,013$$

Ermittlung von $ggT(46199, 66013)$ mithilfe des EEA:

i	r_i	q_i	s_i	t_i
0	66 013		1	0
1	46 199	1	0	1
2	19 814	2	1	-1
3	6 571	3	-2	3
4	101	65	7	-10
5	6	16	-457	653
6	5	1	7 319	-10 458
7	1	5	-7 776	11 111
8	0		46 199	66 013

Also: $46\,199^{-1} \equiv 11\,111 \bmod 66\,013$

Wir berechnen zunächst 5^{-1} und multiplizieren dann mit 26.

$$x \equiv 5^{-1} \bmod 828\,321$$
$$\Leftrightarrow \quad 5x \equiv 1 \bmod 828\,321$$

Ermittlung von $ggT(828\,321, 5)$ mithilfe des EEA:

i	r_i	q_i	s_i	t_i
0	828 321		1	0
1	5	165 664	0	1
2	1	5	1	-165 664
3	0		-5	828 321

Also: $x \equiv -165\,664 \bmod 828\,321$

$$\Leftrightarrow \quad x \equiv 662\,657 \bmod 828\,321$$

Multipliziert mit 26 ergibt sich:

$$5^{-1} \cdot 26 \equiv 26 \cdot 662\,657 \equiv 662\,662 \bmod 828\,321$$

Aufgabe 8.4

$$\mathbb{Z}_3 = \{[0],[1],[2]\}$$
$$\mathbb{Z}_3^x = \{[1],[2]\}$$
$$\varphi(3) = 3-1 = 2$$

$$\mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$$
$$\mathbb{Z}_5^x = \{[1],[2],[3],[4]\}$$
$$\varphi(5) = 5-1 = 4$$

$$\mathbb{Z}_{15} = \{[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11],[12],[13],[14]\}$$
$$\mathbb{Z}_{15}^x = \{[1],[2],[4],[7],[8],[11],[13],[14]\}$$
$$\varphi(15) = \varphi(3\cdot 5) = \varphi(3)\cdot\varphi(5) = 2\cdot 4 = 8$$

$$\mathbb{Z}_3 = \{[0],[1],[2]\}$$
$$\mathbb{Z}_3^x = \{[1],[2]\}$$
$$\varphi(3) = 3-1 = 2$$

$$\mathbb{Z}_9 = \{[0],[1],[2],[3],[4],[5],[6],[7],[8]\}$$
$$\mathbb{Z}_9^x = \{[1],[2],[4],[5],[7],[8]\}$$
$$\varphi(9) = \varphi\left(3^2\right) = 3^2 - 3^1 = 6$$

$$\mathbb{Z}_{27} = \left\{\begin{matrix}[0],[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11],[12],[13],[14],[15],\\ [16],[17],[18],[19],[20],[21],[22],[23],[24],[25],[26]\end{matrix}\right\}$$
$$\mathbb{Z}_{27}^x = \left\{\begin{matrix}[1],[2],[3],[4],[5],[6],[7],[8],[9],[10],[11],[12],[13],[14],[15],\\ [16],[17],[18],[19],[20],[21],[22],[23],[24],[25],[26]\end{matrix}\right\}$$
$$\varphi(27) = \varphi\left(3^3\right) = 3^3 - 3^2 = 18$$

Aufgabe 8.5

$$\varphi(101) = 100$$
$$17^{10\ 000} \equiv 17^{100\cdot 100} = \left(17^{100}\right)^{100} \equiv 1^{100} \equiv 1 \text{ rem } 101$$

$$\varphi(15) = \varphi(3\cdot 5) = 8$$
$$2^{10\ 000} \equiv 2^{8\cdot 1250} \equiv \left(2^{8}\right)^{2150} \equiv 1^{1250} \equiv 1 \text{ rem } 15$$

$$\varphi(81) = \varphi\left(3^4\right) = 54$$
$$11^{10\ 000} \equiv 11^{54\cdot 185+10} \equiv 11^{185}\cdot 11^{10} \equiv 11^{10} \equiv 43 \text{ rem } 81$$

Aufgabe 8.6

Zu zeigen: $c \equiv c' \bmod pq$ mit p, q teilerfremd und c, c' Lösungen des Systems
$x \equiv a \bmod p, x \equiv b \bmod q$.

Aus $c \equiv c' \equiv a \bmod p$ und $c \equiv c' \equiv b \bmod q$ folgt: $p \mid c - c'$ und $q \mid c - c'$

Da p, q teilerfremd, ist $kgV(p, q) = p \cdot q$. Also gilt nach Definition des kgV:

$p \cdot q \mid c - c' \Leftrightarrow c \equiv c' \bmod pq$

■

Aufgabe 8.7

$x \equiv 7 \bmod 37$
$x \equiv 1 \bmod 51$

Berechnung von $ggT(51, 37)$ mithilfe des EEA:

i	r_i	q_i	s_i	t_i
0	51		1	0
1	37	1	0	1
2	14	2	1	-1
3	9	1	-2	3
4	5	1	3	-4
5	4	1	-5	7
6	1	4	8	-11
7	0		-37	51

$ggT(51, 37) = 1 = 8 \cdot 51 + (-11) \cdot 37$

Seien $u = s_6 r_0 = 8 \cdot 51 = 408$ und $v = t_6 r_1 = -11 \cdot 37 = -407$, dann gilt nach dem Chinesischen Restsatz: $x = 7 \cdot 408 - 1 \cdot 407 = 2449$

Nach 8.6 gilt dann: $2449 \equiv 562 \bmod 51 \cdot 37$

$\Leftrightarrow \quad 2449 \equiv 562 \bmod 1887$

Somit ist $x = 562$ eine mögliche Lösung.

$x \equiv 7 \bmod 373$
$x \equiv 1 \bmod 513$

Berechnung von $ggT(513, 373)$ mithilfe des EEA:

i	r_i	q_i	s_i	t_i
0	513		1	0
1	373	1	0	1
2	140	2	1	-1
3	93	1	-2	3
4	47	1	3	-4
5	46	1	-5	7
6	1	46	8	-11
7	0		-373	513

$ggT(513, 373) = 1 = 8 \cdot 513 + (-11) \cdot 373$

Seien $u = s_6 r_0 = 8 \cdot 513 = 4104$ und $v = t_6 r_1 = -11 \cdot 373 = -4103$, dann gilt nach dem Chinesischen Restsatz: $x = 7 \cdot 4104 - 1 \cdot 4103 = 24625$

Nach 8.6 gilt dann: $x' = 24\,625 \bmod 191\,349$

$$\Leftrightarrow \quad 191\,349 \mid x' - 24\,625$$

$$\Rightarrow \quad 191\,349 \cdot i = x' - 24\,625 \qquad (\text{mit } i \in \mathbb{Z})$$

$$\Leftrightarrow \quad x' = 191\,349 \cdot i + 24\,625$$

Somit sind alle $x = 191\,349 \cdot i + 24\,625$ mit $i \in \mathbb{Z}$ mögliche Lösungen.

$x \equiv 7 \bmod 373$
$x \equiv 1 \bmod 513$
$x = 3 \bmod 982$

Da für $x \equiv 7 \bmod 373$ und $x \equiv 1 \bmod 513$ schon in ii ein gemeinsames x berechnet wurde, reicht es ein gemeinsames x zu finden für $x \equiv 24625 \bmod 191349$ und $x \equiv 3 \bmod 982$

Berechnung von $ggT(191349, 982)$

i	r_i	q_i	s_i	t_i
0	191 349		1	0
1	982	194	0	1
2	841	1	1	-194
3	141	5	-1	195
4	136	1	6	-1 169
5	5	27	-7	1 364
6	1	5	195	-37 997
7	0		-982	191 349

$ggT(191\,349, 982) = 1 = 195 \cdot 191\,349 + (-37\,997) \cdot 982$

Seien $u = t_6 r_1 = -37\,997 \cdot 982 = -37\,313\,054$ und $v = s_6 r_0 = 195 \cdot 191\,349 = 37\,313\,055$, dann gilt nach dem Chinesischen Restsatz:

$x = 24625 \cdot (-37\,313\,054) + 3 \cdot 195\,191\,349 = -918\,722\,015\,585$

Nach 8.6 gilt dann: $-918\,722\,015\,585 \equiv 132\,055\,435 \bmod 982 \cdot 191\,349$

$$\Leftrightarrow \quad -918\,722\,015\,585 \equiv 132\,055\,435 \bmod 187\,904\,718$$

Somit ist $x = 132\,055\,435$ eine mögliche Lösung.

Frohe Weihnachten! Als Geschenk gibt's diesen tollen Bastelbogen:

Coca-Cola Weihnachtstruck - Bastelanleitung

Drucke zuerst diesen Bastelbogen aus - am besten farbig, schwarzweiß tut's aber auch. Nun brauchst Du Schere und Klebstoff. Schneide den Coca-Coca Weihnachtstruck an den durchgezogenen Linien aus. Dann knickst Du das Papier an den gestrichelten Linien. Falze nun die Knicke, indem Du kräftig mit dem Fingernagel darüberstreichst: Das fertige Modell hält dann besser! Danach bestreichst Du die weißen Klebelaschen dünn mit Klebstoff. Warte bis der Klebstoff ein wenig angetrocknet ist. Drücke dann die Klebestellen fest zusammen. Fertig!

Hast Du Lust, den Coca-Cola Weihnachtstruck auch "in groß" zu sehen? Dann solltest Du unbedingt noch einmal auf unserer Website vorbeischauen.
Unter www.coca-cola.de findest Du alle Termine der Weihnachtstour. Coca-Cola wünscht Dir viel Spaß und frohe Weihnachten.