Kongruenzen, Restklassen und Arithmetik mod n

Auf $\mathbb{Z}$ – der Menge der ganzen Zahlen – kann man eine Äquivalenzrelation definieren

$$x \equiv y \mod n \quad , n \text{ fest},$$

die die Menge $\mathbb{Z}$ in Restklassen partitioniert.

$$[x] = \{ y \in \mathbb{Z} \mid y = k \cdot n + x , k \in \mathbb{Z} \}$$

Die Menge der Restklassen mod n bezeichnet man mit

$$\mathbb{Z}_n = \underbrace{\{0, \ldots, n-1\}}_{n \text{ Restklassen}}.$$

Auf $\mathbb{Z}_n$ lässt sich eine Additions- und eine Multiplikations-operation einführen

$$\oplus_n : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$z = (x+y) \mod n$$

Addition mod n

und

$$\otimes_n : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$

$$z = (x \cdot y) \mod n$$

Multiplikation mod n.

Beispiele $n = 5$

$\oplus_5$ $\quad x + y \bmod 5$

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

0 neutrales Element

$\forall x \in \mathbb{Z}_5$

$\exists (-x) \in \mathbb{Z}_5$

$x + (-x) = 0$

und

$\otimes_5$ $\quad x \cdot y \bmod 5$

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

[1] ist neutrales Element

$\forall x \in \mathbb{Z}_5 \setminus \{0\}$

$\exists x^{-1} \in \mathbb{Z}_5 \setminus \{0\}$

mit $x \cdot x^{-1} \equiv 1 \bmod 5$

$\mathbb{Z}_2$ $\quad n = 2$

$\oplus$	0	1
0	0	1
1	1	0

und

$\otimes$	0	1
0	0	0
1	0	1

Kleine Übung zum Warm-up:

Lösen Sie das folgende Gleichungssystem in $\mathbb{Z}_2$

$$x_1 + x_2 + x_3 = 1 \qquad (i)$$

$$x_1 + x_2 = 0 \qquad (ii)$$

$$x_2 + x_3 = 0 \qquad (iii)$$

Aus (ii) folgt $x_1 = -x_2 = x_2$ | weil auf $\mathbb{Z}_2$ $x = -x$

Analog folgt aus (iii) : $x_2 = x_3$

$\Rightarrow x_1 = x_2 = x_3$

Einsetzen in (i):

$$x_1 + x_2 + x_3 = 1$$

$$x_1 + x_1 + x_1 = 1 \Rightarrow x_1 = 1$$

$$(x+y)^2 = x^2 + y^2 \quad \text{auf } \mathbb{Z}_2$$

$n = 9$ Multiplikation

·	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Für $x = 1, 2, 4, 5, 7, 8$ existiert ein $x^{-1} \in \mathbb{Z}_9 \setminus \{0\}$

mit $x \cdot x^{-1} \equiv 1 \mod 9$

aber für $x = 3, 6$ existiert kein x mit

$x \cdot x^{-1} \equiv 1 \mod 9$.

D.h. die Menge $(\mathbb{Z}_9, \oplus_9, \otimes_9)$ hat nicht die Struktur eines endlichen Körpers (da nicht zu jedem $x \in \mathbb{Z}_9 \setminus \{0\}$ ein x^{-1} existiert.

Betrachte $\mathbb{Z}_9^* = \{\underbrace{1, 2, 4, 5, 7, 8}_{x \cdot y \mod 9}\}$

	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

Es gilt die Aussage

Falls $ggT(x, 9) = 1$, dann existiert ein $x^{-1} \in \mathbb{Z}_9 \setminus \{0\}$

mit $x \cdot x^{-1} \equiv 1 \mod 9$.

Wegen $\phi(n)$: Anzahl der Elemente $1 \leq a < n$ mit $ggT(a, n)$, hat $\mathbb{Z}_n^*$ immer $\phi(n)$ Elemente.

Satz

Sei $a \equiv b \mod n$

und $c \equiv d \mod n$.

Dann gilt:

$a + c \equiv (b+d) \mod n$ (+)

$a \cdot c \equiv (b \cdot d) \mod n$

$k \cdot a \equiv k \cdot b \mod n \quad \forall k \in \mathbb{Z}$

Dies besagt, dass man mit Kongruenzen addieren, subtrahieren und multiplizieren kann wie mit ganzen Zahlen.

Beweis: von (+)

$a \equiv b \mod n \Rightarrow a - b = k \cdot n$

$c \equiv d \mod n \Rightarrow c - d = l \cdot n \qquad k, l \in \mathbb{Z}$

Addition: $a - b + c - d = k \cdot n + l \cdot n$

$\Leftrightarrow (a+c) - (b+d) = (k+l) \cdot n$

$\Leftrightarrow (a+c) \equiv (b+d) \mod n$.

Beispiel: Der Nutzen dieser Beziehungen wird durch folg. Bsp. deutlich

$143 \equiv 3 \mod 7$

$36 \equiv 1 \mod 7$

$\left(\begin{array}{l} a \equiv b \mod n \\ c \equiv d \mod n \end{array} \right)$

$$143 \cdot 36 = 5148 \equiv 3 \bmod 7$$

$$\Downarrow \quad \downarrow$$

$$3 \quad 1 = 3 \bmod 7$$

$$
\begin{aligned}
54 \cdot 12 \bmod 7 &= \left[(54 \bmod 7)\,(12 \bmod 7)\right] \bmod 7 \\
&= (5 \cdot 5) \bmod 7 \\
&\equiv \underline{4 \bmod 7}
\end{aligned}
$$

<u>Hieraus folgt</u>

$$
\boxed{
\begin{aligned}
(a \pm b) \bmod n &\equiv (a \bmod n \pm b \bmod n) \bmod n \\
(a \cdot b) \bmod n &\equiv \left[(a \bmod n) \cdot (b \bmod n)\right] \bmod n
\end{aligned}
}
$$

<u>Bsp:</u>

$$
\begin{aligned}
11 \cdot 15 \bmod 8 &\equiv \left[(11 \bmod 8) \cdot (15 \bmod 8)\right] \bmod 8 \\
&\equiv (3 \cdot 7) \bmod 8 \\
&\equiv \underline{5 \bmod 8}
\end{aligned}
$$

$$11 \cdot 15 = 165 \bmod 8 \equiv 5 \bmod 8$$

Division:

Coprim - Eigenschaft

Seien $a, b, c, n \in \mathbb{Z}$, $n \neq 0$ und $\boxed{ggT(a,n) = 1}$.

Wenn $(a \cdot b) \equiv (a \cdot c) \bmod n \quad | \cdot a^{-1}$

$\Rightarrow \quad b \equiv c \bmod n.$

Beispiel:

Man löse die Gleichung

$$2x + 7 \equiv 3 \bmod 17.$$

$$\Leftrightarrow \quad 2x \equiv (3-7) \bmod 17$$
$$\equiv -4 \bmod 17$$
$$\equiv 13 \bmod 17$$

$\Rightarrow \quad x \equiv 2^{-1} \cdot 13 \bmod 17$ erlaubt, weil $ggT(2,17) = 1$

Man benötigt die Zahl $2^{-1} \in \{1, \dots, 16\}$ mit

$$2 \cdot 2^{-1} \equiv 1 \bmod 17.$$

Berechnen von 2^{-1}

1. Raten
2. Tabelle erstellen
3. $\underbrace{\text{Verwende ein systematisches Verfahren.}}$

(1) liefert $2^{-1} \equiv \cancel{18}\ 9 \bmod 17$, ✓

weil $2 \cdot 9 = 18 = 1 \cdot 17 + 1$

$$\Rightarrow \quad x \equiv 2^{-1} \cdot 13 \mod 17$$
$$\equiv (9 \cdot 13) \mod 17$$
$$= 117 \mod 17$$
$$\equiv 15 \mod 17$$

$6 \cdot 17 = 102$

Übung: Lösen Sie die Gl.

$$5x + 6 \equiv 13 \mod 11.$$

$$5x \equiv 7 \mod 11$$

$$x = 5^{-1} \cdot 7 \mod 11$$

$$5 \cdot 5^{-1} \equiv 1 \mod 11 \quad , \quad 5^{-1} \in \{1, \dots, 10\}$$

	5
11	10
22	15
33	20
44	25
55	30
66	35
⋮	40
	45
	⋮

$$5 \cdot 9 = 45 = 4 \cdot 11 + 1$$

$$\underline{5^{-1} \equiv 9 \mod 11}$$

$$x = 9 \cdot 7 \mod 11 = 63 \mod 11$$
$$\equiv \underline{\underline{8 \mod 11}}$$

Check: $5x + 6 \equiv 13 \mod 11$

$$\equiv 2 \mod 11$$

$46 \equiv 2 \mod 11$ ✓

Intermezzo: Wozu braucht man das alles?

Hier mal der RSA-Algorithmus in voller Pracht:

1. Man wähle zwei zufällige, große Primzahlen p, q (je 512, 1024, 2048 oder 4096 Bit)

$$n = p \cdot q$$

2. Berechne $\phi(n) = (p-1)(q-1)$.

3. Wähle zufällige Zahl e mit

$$1 < e < \phi(n), \quad ggT(e, \phi(n)) = 1$$

4. Berechne d mit

$$\boxed{e \cdot d \equiv 1 \bmod \phi(n)}$$

5. $$\boxed{\begin{aligned} K_{pub} &= (e, n) \\ K_{priv} &= (d, n) \end{aligned}}$$

Verschlüsselung: Sei M der Klartext, als Zahl geeignet codiert, z.B. ASCII-Wert.

$$BA \rightarrow \boxed{66}\boxed{65}$$
 B A

$M < n$

$$\boxed{C = M^e \bmod n}$$

Entschlüsselung:

$$M = C^d \bmod n \qquad K_{priv.} = (d, n)$$

Modulare Exponentiation

In vielen Krypto-Algorithmen der Public-Key-Kryptographie hat man Zahlen der Form

$$z = x^y \bmod n$$

zu berechnen, z. B.

$$z = 2^{1234} \bmod 789 .$$

Schlecht: berechne 2^{1234} und dann mod 789

Bleistift + Papier - Methode

(1) Man zerlegt den Exponenten in eine Summe von 2er-Potenzen.

$$1234 = 1024 + 128 + 64 + 16 + 2$$

$$z = 2^{1234} \bmod 789$$

$$= 2^{1024+128+64+16+2} \bmod 789$$

Potenzr.

$$= (2^{1024} \cdot 2^{128} \cdot 2^{64} \cdot 2^{16} \cdot 2^{2}) \bmod 789$$

$$(a \cdot b) \bmod n = [(a \bmod n) \cdot (b \bmod n)] \bmod n$$

$$= [(2^{1024} \bmod 789) \cdot (2^{128} \bmod 789)(2^{64} \bmod 789)$$

$$(2^{16} \bmod 789) \cdot (4 \bmod 789)] \bmod 789$$

ND.

$$2^{2} \bmod 789 = 4$$

$$2^{4} \bmod 789 = 16$$

$$2^{8} \bmod 789 = 256$$

$$2^{16} \bmod 789 = 256 \cdot 256 \bmod 789 = 49$$

$$2^{32} \bmod 789 = (2^{16} \cdot 2^{16}) \bmod 789$$

$$= \left[(2^{16} \bmod 789)(2^{16} \bmod 789)\right] \bmod 789$$

$$= (49 \cdot 49) \bmod 789$$

$$= 34$$

$$2^{64} = 367$$

$$2^{128} = 559$$

$$2^{256} = 37$$

$$2^{512} \equiv 580$$

$$2^{1024} = 286$$

$$z = (286 \cdot 559 \cdot 367 \cdot 49 \cdot 4) \bmod 789$$

$$\equiv 481 \bmod 789$$

Übung: Berechnen Sie

$$z = 7^{25} \bmod 13$$

$25 = 16 + 8 + 1$

$13, 26, 52, 78, 91$

13
26
39
52
65
78
91
104
117
130

$7^2 = 49 = 10$

$7^4 = 100 = 9$

$7^8 = 81 = 3$

$7^{16} = 9$

$$7^{25} = (9 \cdot 3 \cdot 7) \bmod 13$$

$$= \overset{27}{\cancel{81}} \cdot 7 \bmod 13$$

$$= \cancel{21}\,7 \bmod 13$$

$$= \underline{\underline{\cancel{5}7}}$$

$z = 7^{25} \bmod 13$

$= 7^{16+8+1} \bmod 13$

$= \left[(7^{16} \bmod 13)(7^{8} \bmod 13)(7 \bmod 13) \right] \bmod 13$

NR.

$7^2 \bmod 13 = 49 \bmod 13 \equiv 10 \bmod 13$

$7^4 \bmod 13 \equiv 100 \bmod 13 \equiv 9 \bmod 13$

$7^8 \bmod 13 \equiv 81 \bmod 13 \equiv 3 \bmod 13$

$7^{16} \bmod 13 = 3 \cdot 3 \bmod 13 = 9$

$7^{25} \bmod 13 = (9 \cdot 3 \cdot 7) \bmod 13$

$= [\underbrace{27 \bmod 13}_{1} \cdot 7 \bmod 13] \bmod 13$

$= \underline{\underline{7}}$

Algorithmus Modulare Exponentiation.

Der folgende Algorithmus berechnet $\text{fastexp} = x^y \bmod n$

Input Drei positive ganze Zahlen x, y, n

Drei Hilfsvariable a, b, c.

Initialisierung Setze $a \leftarrow x$

$b \leftarrow 1$

$c \leftarrow y$

Falls c gerade, setze (*)

$$a \leftarrow a^2 \bmod n$$
$$b \leftarrow b$$
$$c \leftarrow \frac{c}{2}$$

Falls c ungerade, setze

$$a \leftarrow a$$
$$b \leftarrow a \cdot b \bmod n$$
$$c \leftarrow c - 1$$

Falls $c \neq 0$ weiter mit (*), sonst STOP

output $b = \text{fastex} = x^y \bmod n$

<u>Bsp</u> $2 = 7^{15} \bmod 13$

$x = 7,\ \underline{\underline{y = 15}},\ n = 13$

$$a \leftarrow x = 7$$
$$b \leftarrow 1$$
$$c \leftarrow 25$$

1. Runde c ungerade

$$a \leftarrow 7$$
$$b \leftarrow 1 \cdot 7 \bmod 13 = 7$$
$$c \leftarrow 24$$

2. Runde c gerade

$$a \leftarrow a^2 \bmod n = 49 \bmod 13 \equiv 10$$
$$b \leftarrow 7$$
$$c \leftarrow 7$$

3. Runde $\quad c$ ungerade

$a \leftarrow 10$

$b \leftarrow a \cdot b \bmod n = 70 \bmod 13 \equiv 5$

$c \leftarrow c - 1 = 6$

4. Runde $\quad c$ gerade

$a \leftarrow a^2 \bmod n = 100 \bmod 13 \equiv 9$

$b \leftarrow 5$

$c \leftarrow 3$

5. Runde $\quad c$ ungerade

$a \leftarrow 9$

$b \leftarrow 5 \cdot 9 \bmod 13 = 6$

$c \leftarrow 2$

6. Runde $\quad c$ gerade

$a \leftarrow 81 \bmod 13 \equiv 3$

$b \leftarrow 6$

$c \leftarrow 1$

7. Runde $\quad c$ ungerade

$a \leftarrow 3$

$b \leftarrow 3 \cdot 6 \bmod 13 = 18 \bmod 13 = 5$

$c \leftarrow 0$

$\longrightarrow \quad 7^{15} \bmod 13 = \underline{\underline{5}}$

Der erweiterte EUKLIDische Algorithmus

Beispiel: Berechne das multiplikative Inverse von 510 mod 1001, d.h. gesucht ist die Zahl $x \in \mathbb{Z}_{1001}$ mit

$$x \cdot 510 \equiv 1 \mod 1001.$$

1. Dividiere 1001 durch 510

$$1001 = 1 \cdot 510 + 491$$

Schreibe die Reste in jedem Schritt als Linear-kombination von 510 und 1001

$$\boxed{491 = 1 \cdot 1001 - 1 \cdot 510}$$

2. Dividiere 510 durch 491

$$510 = 1 \cdot 491 + 19$$

$$\begin{aligned} 19 &= 510 - 1 \cdot 491 \\ &= 510 - 1 \cdot (1 \cdot 1001 - 1 \cdot 510) \\ &= 2 \cdot 510 - 1 \cdot 1001 \end{aligned}$$

3) Dividiere 491 durch 19

$$491 = 25 \cdot 19 + 16$$

$$16 = 491 - 25 \cdot 19$$

$= 1 \cdot 1001 - 1 \cdot 510 - 25\,(2 \cdot 510 - 1 \cdot 1001)$

$= 26 \cdot 1001 - 51 \cdot 510$

16

4) Division 19 durch 16

$19 = 1 \cdot 16 + 3$

$3 = 19 - 16$

$= 2 \cdot 510 - 1 \cdot 1001 - 26 \cdot 1001 + 51 \cdot 510$

$= 53 \cdot 510 - 27 \cdot 1001$

---

5) Division 16 durch 3

$16 = 5 \cdot 3 + 1$

$1 = 16 - 5 \cdot 3$

$= 26\ 1001 - 51 \cdot 510 - 5\,(53 \cdot 510 - 27 \cdot 1001)$

$= 161 \cdot 1001 - 316 \cdot 510$

$$\boxed{1 = 161 \cdot 1001 - 316 \cdot 510}$$

$\Rightarrow \quad -316 \cdot 510 = \underbrace{-161}_{\in \mathbb{Z}} \cdot 1001 + 1$

$-316 \cdot 510 \equiv 1 \mod 1001$

$\Rightarrow \quad 510^{-1} \cdot 510 \equiv 1 \mod 1001$

$$510^{-1} \mod 1001 \equiv -316 \mod 1001$$
$$\equiv \underline{\underline{685 \mod 1001}}$$

Check: $510 \cdot 685 = 349\,350$
$$= 349\,349 + 1$$
$$= \underline{349 \cdot 1001 + 1} \checkmark$$

Algorithmus Erweiterter EUKLID

Input: Zwei positive ganze Zahlen a, b,

o.B.d.A. $a < b$

Hilfsvariable X_1, X_2, X_3

Y_1, Y_2, Y_3

T_1, T_2, T_3

Q.

Initialisierung

$X_1 \leftarrow 1 \qquad Y_1 \leftarrow 0$

$X_2 \leftarrow 0 \qquad Y_2 \leftarrow 1$

$X_3 \leftarrow b \qquad Y_3 \leftarrow a$

(*) Wenn $Y_3 = 0$ STOP return $X_3 = ggT(a,b)$

Kein Inverses.

Wenn $Y_3 = 1$ STOP return $\boxed{Y_2 = a^{-1} \mod b}$

Sonst Berechne $Q = \left\lfloor \frac{X_3}{Y_3} \right\rfloor$

$$\left[\begin{array}{l} \lfloor x \rfloor = \text{Gauss-Klammer von } x \\ \qquad\;\; = \text{größte ganze Zahl} \le x. \\ \lfloor \pi \rfloor = 3 \end{array}\right]$$

Berechne
$$T_1 \leftarrow X_1 - QY_1$$
$$T_2 \leftarrow X_2 - QY_2$$
$$T_3 \leftarrow X_3 - QY_3$$

Setze
$$X_1 \leftarrow Y_1 \qquad Y_1 \leftarrow T_1$$
$$X_2 \leftarrow Y_2 \qquad Y_2 \leftarrow T_2$$
$$X_2 \leftarrow Y_3 \qquad Y_3 \leftarrow T_3$$

Weiter mit (*)

Beispiel: $a = 510$, $b = 1001$

$$X_1 \leftarrow 1 \qquad Y_1 \leftarrow 0$$
$$X_2 \leftarrow 0 \qquad Y_2 \leftarrow 1$$
$$X_3 \leftarrow 1001 \qquad Y_3 \leftarrow 510$$

$Y_3 = 0$? $Y_3 = 1$? Nö

$$Q = \left\lfloor \frac{X_3}{Y_3} \right\rfloor = \left\lfloor \frac{1001}{510} \right\rfloor = 1$$

$$T_1 = X_1 - QY_1 = 1$$
$$T_2 = X_2 - QY_2 = -1$$
$$T_3 = X_3 - QY_3 = 1001 - 510 = \underline{\underline{491}}$$

$X_1 \leftarrow 0 \qquad Y_1 \leftarrow 1$

$X_2 \leftarrow 1 \qquad Y_2 \leftarrow -1$

$X_3 \leftarrow 510 \qquad Y_3 \leftarrow 491$

$$Q = \left\lfloor \frac{X_3}{Y_3} \right\rfloor = 1$$

$$T_1 = X_1 - QY_1 = -1$$

$$T_2 = X_2 - QY_2 = 2$$

$$T_3 = X_3 - QY_3 = 19$$

$X_1 \leftarrow 1 \qquad Y_1 \leftarrow -1$

$X_2 \leftarrow -1 \qquad Y_2 \leftarrow 2$

$X_3 \leftarrow 491 \qquad Y_3 \leftarrow 19$

$$Q = \left\lfloor \frac{491}{19} \right\rfloor = 25$$

$$T_1 = X_1 - QY_1 = 1 + 25 = 26$$

$$T_2 = X_2 - QY_2 = -1 - 50 = -51$$

$$T_3 = X_3 - QY_3 = 16$$

$X_1 \leftarrow -1 \qquad Y_1 \leftarrow 26$

$X_2 \leftarrow 2 \qquad Y_2 \leftarrow -51$

$X_3 \leftarrow 19 \qquad Y_3 \leftarrow 16$

$$Q = \left\lfloor \frac{19}{16} \right\rfloor = 1$$

$$T_1 \leftarrow -1 - 26 = -27$$

$$T_2 \leftarrow 2 + 51 = 53$$

$$T_3 \leftarrow 19 - 16 = 3$$

$X_1 \leftarrow 26 \qquad Y_1 \leftarrow -27$

$X_2 \leftarrow -51 \qquad Y_2 \leftarrow 53$

$X_3 \leftarrow 16 \qquad Y_3 \leftarrow 3$

$$Q = \left\lfloor \frac{16}{3} \right\rfloor = 5$$

$$T_1 = X_1 - QY_1 = 26 + 5 \cdot 27 = 161$$

$$T_2 = X_2 - QY_2 = -51 - 5 \cdot 53 = -316$$

$$T_3 = X_3 - QY_3 = 16 - 15 = 1$$

$X_1 \leftarrow -27 \qquad Y_1 \leftarrow 161$

$X_2 \leftarrow 53 \qquad Y_2 \leftarrow -316$

$X_3 \leftarrow 3 \qquad Y_3 = 1$

$Y_3 = 1$ STOP $\quad y_2 = 510^{-1} \bmod 1001$

$= -316$