Modulo-Rechnung-Lehrtext

Modul $\mathbb{Z}_5 = \{0,1,2,3,4\}$ Das sind die Reste, die beim Teilen durch 5 auftreten können.

Im Modul $\mathbb{Z}_5$ kann man gemäß den folgenden **Verknüpfungstafeln** rechnen.

Rechnen modulo 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	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

Diese Tafeln transportieren die gesamte Information, die man zum Rechnen im Modul $\mathbb{Z}_5$ braucht.

Man liest in der Mathematik immer die Zeile zuerst und dann die Spalte.

$3 \cdot 4 \underset{5}{\equiv} 2$

Aber man muss die Zahlen gar nicht ablesen, sondern kann sie auch selber ausrechnen:

$3 \cdot 4 = 12 \underset{5}{\equiv} 2$ oder $4 + 2 = 6 \underset{5}{\equiv} 1$. Hat man also Zahlen, die nicht in

$\mathbb{Z}_5 = \{0,1,2,3,4\}$ enthalten sind, nimmt man die Reste, die sich beim Teilen durch 5 ergeben.

Das **Additiv-Inverse** von a ist die Zahl, die zu a addiert die 0 ergibt.

Das **Multipliaktiv Inverse** von a ist die Zahl, die mit a multipliziert die 1 ergibt.

$1 + 4 = 5 \underset{5}{\equiv} 0$ Also sind 1 und 4 in $\mathbb{Z}_5$ additiv invers zueinander, also $(-1) \underset{5}{\equiv} 4$.

$2 \cdot 3 = 6 \underset{5}{\equiv} 1$ Also sind 2 und 3 in $\mathbb{Z}_5$ multiplikativ invers zueinander.

Das zweite Ergebnis ist verblüffend. In den üblichen Zahlen ist die Lösung von $2 \cdot x = 1$ $x = \frac{1}{2}$, also ein Bruch. Im Modul $\mathbb{Z}_5$ ist $x = 3$, es gibt eine Lösung, obwohl es keine Brüche gibt.

Genau da liegt für die Kryptografie die Bedeutung des Rechnens im Modul

Im Modul $\mathbb{Z}_m$ kann es Multiplikativ-Inverse geben, die keine Brüche sind.

Subtraktion, Abziehen, negative Zahlen

Zu der Subtraktion $a - b = x$ gehört als Probe $b + x = a$. Also sieht man in der Zeile von b nach wo a erscheint und liest im zugehörigen Spaltenkopf das x ab.

Wenn klar ist, in welchem Moldul man rechnet, schreibt man auch einfach $=$ *statt* $\underset{5}{\equiv}$

Methode mit Tabelle

$2 - 3 = x \Leftrightarrow 3 + x = 2$ $\quad 3 \rightarrow 4 \rightarrow 2$ $\quad 3 + 4 = 2 \Leftrightarrow 2 - 3 = 4 = x$

Methode für den Kopf:

Man rechnet normal und addiert bei negativem Ergebnis eine 5.

$2 - 3 = -1 \underset{5}{\equiv} -1 + 5 \underset{5}{\equiv} 4$ Das geht natürlich viel schneller. Die Begründung sieht man oben, 4 ist das additiv-Inverse von 1.