Modulo – Grundlage zum Rechnen in Kryptografie

Es geht um eine natürliche Zahl **m** und die positiven **Reste**, die beim Teilen von ganzen Zahlen durch dieses m auftreten können. Diese Reste bilden **den Modul** $\mathbb{Z}_m$.

Die modulo-Funktion $mod : \mathbb{Z} \to \mathbb{Z}_m$ ordnet jeder ganzen Zahl a ihren Rest in $\mathbb{Z}_m$ zu.

Es gibt dafür einige Schreibweisen, dargestellt im Beispiel modolo 5.:

$$mod : 678 \to 3 \in \mathbb{Z}_5 \;\; // \;\; mod(678,5) = 3 \;\; // \;\; 678 \; mod \; 5 = 3 \;\; // \;\; 678 \underset{5}{\equiv} 3$$

Man sagt in Worten: **678 modulo 5 ist 3** oder **673 ist kongruent 3 modulo 5**

Für negative Zahlen bestimmt man den positiven Rest, indem man ein hinreichend großes Vielfaches von m addiert.

$$-47 \; mod \; 5 = (-47 + 50) \; mod \; 5 = 3 \quad // \quad -47 \underset{5}{\equiv} 50 - 47 \underset{5}{\equiv} 3$$

Jede ganze Zahl hat also ihr Bild, ihren Vertreter, ihre Restklasse. Die Restklasse der 3 im Modul $\mathbb{Z}_5$ kann man auch als Menge der Zahlen {....-7, -2, 3, 8 13, 18, 23,...} aufffassen.

Will man diesen Aspekt betonen, schreibt man auch $\overline{3} = \overline{8} = \overline{-47} = \overline{678} = ...$. Der Nachteil dieser Schreibweise ist außer der Unhandlichkeit des Querstrichs auch, dass die 5 als Grundlage für diesen Modul nicht erscheint. In dieser Vorlesung sollen daher nur die beiden erstgenannten Schreibweisen verwendet werden.
Die Schreibweise mit den drei Stichen ist für das Rechnen von Hand am besten.

Die wichtigen Begriffe "**Klasse**" und "**Klasseneinteilung**" kann man sich so wie in der Schule vorstellen: "jedes Element gehört zu **genau einer** Klasse."
oder: "jedes Element gehört zu **einer und nur einer** Klasse."
oder: "jedes Element ist **in einer** Klasse und **kein** Element gehört **zu zwei oder mehr** Klassen."
Die Mathematiker formulieren gern knapp aber präzise. Zum Verstehen sind manchmal aber die längeren Sätze besser. Auch die Juristen und überhaupt alle Wissenschaftler haben die für ihr Fach typischen Redeweisen und Vokabeln, die so maches Mal sogar vom allgemeinen Gebrauch abweichen. Oft ist für Anfänger hilfreich, den Sachverhalt mit eigenen Worten auszudrücken und sich über die Deutung mit anderen auszutauschen. Schon für Ihre ersten Klausuren wird es wichtig sein, dass Sie die Fragen **genau** verstehen.

Im Modul $\mathbb{Z}_m$ kann man auf die übliche Art rechnen. Das Ergebnis wird aber wieder in den Modul $\mathbb{Z}_m$ abgebildet. Dabei ist es erstaunlicherweise egal, an welchen Stellen des Rechenweges, man von einem Zwischenergebnis nur noch den Rest betrachtet.
Die Mathematiker sagen: Die modulo-Funktion ist "**strukturerhaltend**", sie ist ein "Homomorphismus".

$$678 + 4711 \underset{5}{\equiv} 3 + 1 \underset{5}{\equiv} 4 \quad \text{oder} \quad 678 + 4711 \underset{5}{\equiv} 5389 \underset{5}{\equiv} 4$$

$$17036 \cdot 1711 \underset{17}{\equiv} 2 \cdot 11 \underset{17}{\equiv} 22 \underset{17}{\equiv} 5$$, hier wäre es sehr ungeschickt, wirklich die großen Zahlen zu multiplizieren. Vielfache von m kann man überall einfach weglassen.