Äquivalenzrelation und modulo-Rechnen.

Äquivalenz

Bspl "modulo n" $\left(\equiv_n\right)$ $a,b \in \mathbb{Z}$ $a \equiv_n b :\Leftrightarrow \exists k \in \mathbb{Z}: a-b = kn$

1. $\equiv_n$ ist Äquivalenzrelation

a) reflexiv $a \equiv_n a$ denn $a-a = 0 = 0 \cdot n$ mit $0 \in \mathbb{Z}$

b) symmetrisch $a \equiv_n b \Rightarrow b \equiv_n c$ denn $a-b = kn \Rightarrow b-a = (-k)n$ mit $(-k) \in \mathbb{Z}$

c) transitiv $a \equiv_n b \wedge b \equiv_n c \Rightarrow a \equiv_n c$ $\Rightarrow \exists k, q \in \mathbb{Z}$: ($k+q \in \mathbb{Z}$)

$a-b = kn \wedge b-c = qn \Rightarrow a-c = a-b+b-c = kn+qn = (k+q)n$

2. $\mathbb{Z}$ wird dadurch in nichtleere disjunkte Klassen aufgeteilt.

Bew. $[a] := \{x \mid x \equiv_n a\}$

$[a] \neq \emptyset$ denn $a \equiv_n a$ (reflexiv)

$m \in [a] \cap [b] \Rightarrow [a] = [b]$

Bew $m \in [a] \Rightarrow a \equiv_n m$
$m \in [b] \Rightarrow m \equiv_n b$ $\Big\}$ tr. $\Rightarrow a \equiv_n b$ $\Big\}$ tr $\Rightarrow x \equiv_n b \Rightarrow x \in [b] \Rightarrow [a] \subseteq [b]$

ebenso $[b] \subseteq [a]$ $\overset{\text{sys.}}{\Rightarrow}$ $[a] = [b]$

Jedes $z \in \mathbb{Z}$ gehört zu einer Klasse und die Klassen sind disjunkt.

In der Zahlentheorie schreibt man $\bar{a}$ statt $[a]$

$\bar{0} = n \cdot \mathbb{Z}$ $\bar{1} = n\mathbb{Z}+1$ $\bar{2} = n\mathbb{Z}+2$ usw.

$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2} \ldots \overline{n-1}\} =: \mathbb{Z}_n$

$\mathbb{Z}_n$ "erbt" die Verknüpfungen

$\bar{a} + \bar{b} := \overline{a+b} = \{x \mid x \equiv_n a+b\}$

$\bar{a} \cdot \bar{b} := \overline{a \cdot b} = \ldots\ldots \equiv_n a \cdot b$

Wohldefiniertheit

$\bar{a} = \bar{a'} \wedge \bar{b} = \bar{b'}$ $\quad \overline{a'} + \overline{b'} := \overline{a'+b'}$

$a \equiv_n a' \wedge b \equiv_n b'$ $\quad a - a' = kn \wedge b - b' = qn$

$a' + b' = a - kn + b - qn = a + b + (-k-q) \cdot n$ ($-k-q \in \mathbb{Z}$)

$a'+b' - (a+b) = z \cdot n$

$\bar{a'} + \bar{b'} = \overline{a'+b'} = \overline{a+b} = \bar{a} + \bar{b}$

$\Rightarrow$ Repräsentantenunabhängigkeit

$(\mathbb{Z},+)$ ist Gruppe, daher ist $(n\mathbb{Z},+)$ auch Gruppe
$\bar{r} = n\mathbb{Z}+r$ mit $1 \le r \le n-1$ sind additive Neben-Klassen.
sie sind keine Gruppen.
sie nicht abgeschlossen gegenüber +

$(n\mathbb{Z},+) = \{0, n, -n, 2n, -2n, \dots\}$

$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ ist bezgl + auch Gruppe = Faktorgruppe
"nach"
$|\mathbb{Z}_n| = n$ = Index von $(n\mathbb{Z},+)$ in $(\mathbb{Z},+)$

Algebraische Auffassung $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$
mit $a, b \in \mathbb{Z}_n$ $a+b := (a+b) \bmod n$
$a \cdot b := (a \cdot b) \bmod n$

In der algebraischen Auffassung hat man eine Menge , in der man zwei Verküpfungen definiert.
Mit diesen Verküpfungen erhält man Ringe. Genau wenn n Primzahl ist, sind die Ringe sogar Körper.

Bleibt man bei den Restklassen hat man Restklassenringe und Restklassenkörper.
In der Kyptografie ist es üblich, keine Querstriche zu schreiben, sondern die Zahlen 0 bis n-1 als eigene Objekte zu betrachten.

Eine weitere sinnvolle Auffassung ist die folgende:
Nach dem Satz von der Divison mit Rest (Seite 3 Kryptoheft) lässt sich jeder ganzen Zahl eindeutig ein positiver Rest bei der Division durch n zuordnen.
Fasst man $\mathbb{Z}_n$ als die Menge der möglichen Reste auf und nimmt $(\mathbb{Z}_n, +, \cdot)$ als algebraische Struktur, dann ist diese Abbildung ein Homomorphismus bezgl. + und $\cdot$ eine strukturerhaltende Abbildung, denn das Bild einer Summe ist gleich der Summe der Bilder.

z.B. $n = 10$ $17+28 = 45 \longrightarrow 5$
$17 \longrightarrow 7$
$28 \longrightarrow 8$
$7+8 \equiv 5 \pmod{10}$

Ebenso bei Mal.
Hier liegt der Grund, warum man einfach beim Modulo-rechnen ganz beliebig in $\mathbb{Z}$ oder $\mathbb{Z}_n$ rechen kann. Dieses hilft in Mathe für alle das Gegebiet „intuitiv" zu handhaben.

In der Kryptografie betrachtet man in vielen Zusammenhängen die Mengen der zu n teilerfemden Elemente und fasst sie in der Menge $\mathbb{Z}_n^*$ $(\mathbb{Z}_n^*, \cdot)$ zusammen. Bezüglich der Multiplikation sind die Gruppen. Für sie gelten also die Ergebnisse der Gruppentheorie.

Dazu gehört z.B., dass alle Nebenklassen (jetzt multiplikativ) einer Untergruppe gleich groß sind, dass ihre Anzahl (der Index der Untergruppe in der Gruppe) die Gruppenordnung teilt (Eulerscher Satz) u.s.w. .

Im Lehrgang LBS-Mathematik sind dies die wesentliche Elemente, die sonst in „Algebra"-Vorlesungen ausgebreitet und ausgebaut werden.

aequi-modulo.docx