5 Modulo

5.1 Division mit Rest

5.1.1 Lemma

Seien $a, m \in \mathbb{Z}$ und $m > 1$. Dann existiert ein $k \in \mathbb{Z}$ und ein $r \in \{0, \ldots, m-1\}$, so dass

$$a = km + r \ .$$

Beweis: Sei $k \in \mathbb{Z}$ die größte ganze Zahl mit $km \leq a$. Dann ist

$$r := a - km \in \{0, \ldots, m-1\} \ .$$

□

5.1.2 Bezeichnung

Möchte man nicht nur sagen, dass eine Variable gleich einem Ausdruck ist, sondern darauf hinweisen, dass diese Variable an dieser Stelle neu eingeführt, also *definiert* wird, verwendet man gerne das Zeichen „:=“ (gesprochen „definitionsgemäß gleich“ oder „definiert als“).

Aufgrund von Lemma 5.1.1 können wir nun eine weitere Rechenoperation definieren:

5.1.3 Definition

Seien $a, b, m \in \mathbb{Z}$ und $m > 1$ und sei $a = km + r$ mit $r \in \{0, \ldots, m-1\}$.
Dann ist r der *Rest* bei der Division von a durch m:

$$r = a \bmod m \qquad \text{(gesprochen „}n \text{ modulo } m\text{“)} \ .$$

Ist auch $b \bmod m = r$ (haben a und b also den gleichen Rest modulo m), so schreibt man auch

$$a = b \pmod{m} \ .$$

5.1.4 Beispiele

Es gilt

$$10 \bmod 3 = 1$$
$$10 \bmod 11 = 10$$
$$10 \bmod 5 = 0$$

und

$$10 = 4 \pmod{3}$$
$$12 = 22 \pmod{10}$$

5.1.5 Korollar

Nach Definition 5.1.3 gilt

$$a = 0 \pmod{m} \quad \Leftrightarrow \quad m | a \ .$$

5.1.6 Lemma

Seien $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ und sei $m \in \mathbb{Z}$ mit $m > 1$, wobei

$$a_1 = b_1 \pmod m \qquad \text{und} \qquad a_2 = b_2 \pmod m \ .$$

Dann ist

(1) $a_1 + a_2 = b_1 + b_2 \pmod m$,

(2) $a_1 a_2 = b_1 b_2 \pmod m$.

5.1.7 Beispiel

$$\begin{aligned} 37 + 65 &= 1 + 2 \pmod 3 \\ &= 3 \pmod 3 \\ &= 0 \pmod 3 \ , \end{aligned}$$

es gilt also $3|(37 + 65)$.

Beweis: [von Lemma 5.1.6]

Nach Voraussetzung existieren $k_1, k_2, k_1', k_2' \in \mathbb{Z}$ und $r, r' \in \{0, \ldots, m-1\}$ mit

$$\begin{aligned} a_1 &= k_1 m + r \quad \text{und} \quad b_1 = k_1' m + r \\ a_2 &= k_2 m + r' \quad \text{und} \quad b_2 = k_2' m + r' \ . \end{aligned}$$

(1) Wir haben

$$\begin{aligned} a_1 + a_2 &= k_1 m + r + k_2 m + r' = (k_1 + k_2)m + r + r' \\ b_1 + b_2 &= k_1' m + r + k_2' m + r' = (k_1' + k_2')m + r + r' \end{aligned}$$

Für $r + r'$ gibt es nun $K \in \mathbb{Z}$ und $R \in \{0, \ldots, m-1\}$ mit $r + r' = Km + R$ und insgesamt

$$\begin{aligned} a_1 + a_2 &= (k_1 + k_2 + K)m + R \\ b_1 + b_2 &= (k_1' + k_2' + K)m + R \\ \Rightarrow \quad a_1 + a_2 &= b_1 + b_2 \pmod m \ . \end{aligned}$$

(2) Analog. (Als Übungsaufgabe.)

□

5.2 Anwendungen

Für das folgende Beispiel benötigen wir einen weiteren Begriff:

5.2.1 Definition

Die *Quersumme* $Q(n)$ einer natürlichen Zahl n mit Dezimaldarstellung $n = n_k \ldots n_1 n_0$ ist

$$Q(n) = n_k + \cdots n_1 + n_0 \ .$$

Die Dezimaldarstellung ist uns allen bekannt, schauen wir sie uns einmal näher an: Die einzelnen Stellen entsprechen den 10er-Potenzen:

$$9823 = 9 \cdot 10^3 + 8 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$$

und allgemein

$$n = n_k \dots n_1 n_0 = n_k \cdot 10^k + \dots + n_1 \cdot 10^1 + n_0 \cdot 10^0 \ .$$

5.2.2 Satz

Eine Zahl $n \in \mathbb{N}$ ist genau dann durch 3 teilbar, wenn ihre Quersumme $Q(n)$ durch 3 teilbar ist.

Beweis:

Wir zeigen, dass $n = Q(n) \pmod 3$:

Sei $n = n_k \dots n_1 n_0$ die Dezimaldarstellung, dann ist, da $10 \mod 3 = 1$, nach Lemma 5.1.6

$$\begin{aligned} n &= n_k \dots n_1 n_0 \\ &= n_k \cdot 10^k + \dots + n_1 \cdot 10^1 + n_0 \cdot 10^0 \\ &= n_k \cdot 1^k + \dots + n_1 \cdot 1^1 + n_0 \cdot 1^0 \pmod 3 \\ &= n_k + \dots n_1 + n_0 \pmod 3 \\ &= Q(n) \pmod 3 \end{aligned}$$

Mit diesem Ergebnis ist nun

$$3|n \quad \Leftrightarrow \quad n = 0 \pmod 3 \quad \Leftrightarrow \quad Q(n) = 0 \pmod 3 \quad \Leftrightarrow \quad 3|Q(n) \ .$$

□

Als letztes Beispiel schauen wir uns das Prüfsummenverfahren von IBANs an. Die IBAN einer Bank in Deutschland besteht aus den Buchstaben „DE“, gefolgt von zwei Ziffern, die eine Prüfsumme darstellen, und weiteren i.a. 18 Ziffern.

Die Prüfsumme wird nach der Norm ISO 7064 MOD 97-10 berechnet. Durch sie wird sicher gestellt, dass ein einzelnes falsches Zeichen immer sowie ein einzelner Zahlendreher zweier benachbarter oder fast benachbarter Zeichen fast immer erkannt werden.

Das Verfahren funktioniert, indem die IBAN als Zahl dargestellt modulo 97 berechnet wird:

(1) Verschiebe die beiden Buchstaben „DE“ und die beiden Ziffern der Prüfsumme an das Ende der IBAN.

(2) Ersetze die Buchstaben durch einen Zahlenwert: A=10, B=11,... Aus „DE“ wird daher 1314.

(3) Berechne diese Zahl modulo 97.

Ist das Ergebnis dieses Verfahrens eine 1, so wird die IBAN akzeptiert.

5.2.3 Beispiel

Betrachten wir die (fiktive) IBAN

DE68 2105 0170 0012 3456 78 .

(1) Verschieben von „DE68“ ans Ende liefert 210501700012345678DE68 .

(2) Die Übersetzung von „DE“ in „1314“ ergibt 210501700012345678131468 .

(3) $210501700012345678131468 \mod 97 = 1$ und damit wird die IBAN akzeptiert.

5.3 Kongruenz

Wir wollen uns einmal die Modulo-Rechnung aus einer ganz anderen Perspektive anschauen. Eigentlich machen wir nichts Neues, wir verwenden nur ein paar neue Begriffe.

5.3.1 Definition

a und b heißen *kongruent* modulo m, wenn $a = b \pmod m$.

Seien $a, b, c \in \mathbb{Z}$. Es gilt recht offensichtlich

(1) a ist kongruent zu a. (Reflexivität)

(2) Ist a kongruent zu b, dann ist auch b kongruent zu a. (Symmetrie)

(3) Ist a kongruent zu b und ist b kongruent zu c, dann ist auch a kongruent zu c. (Transitivität)

Eine solche Beziehung nennt man eine *Äquivalenzrelation*. (Gleichheit „=“ ist z.B. eine Äquivalenzrelation.)

Durch diese Äquivalenzrelation werden die ganzen Zahlen $\mathbb{Z}$ aufgeteilt in die Mengen der Zahlen, die bei Division durch m alle den gleichen Rest haben:

5.3.2 Definition

$[a] = \{n \in \mathbb{Z} : n = km + a \text{ für ein } k \in \mathbb{Z}\}$ heißt *Restklasse* modulo m.

Es gibt m verschiedene Restklassen: $[0], [1], \ldots, [m-1]$. Für $m = 4$ ist beispielsweise

$$\begin{aligned}
[0] &= \{\ldots, -8, -4, 0, 4, 8, \ldots\}\ , \\
[1] &= \{\ldots, -7, -3, 1, 5, 9, \ldots\}\ , \\
[2] &= \{\ldots, -6, -2, 2, 6, 10, \ldots\}\ , \\
[3] &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}\ .
\end{aligned}$$

Weiter wäre $[4] = [0]$, $[5] = [1]$ usw.

Das Interessante hierbei ist, dass man mit diesen Restklassen rechnen kann, indem man einfach mit einem *Repräsentanten* (einem beliebigen Element der Restklasse) rechnet:

$$1 + 2 = 3 \ \Rightarrow\ [1] + [2] = [3]$$

Dies funktioniert auch mit jedem anderen Repräsentanten, z.B.:

$$-3 + 10 = 7 \ \Rightarrow\ [1] + [2] = [3]$$

allgemein ist $[a] + [b] = [a + b]$, denn nach Lemma 5.1.6 liefert die Addition von kongruenten Zahlen wieder kongruente Zahlen.

Analog gilt das auch für die Multiplikation, z.B.

$$6 \cdot 7 = 42 \ \Rightarrow\ [2] \cdot [3] = [2]\ .$$

Additions- und Multiplikationstabellen dieser Restklassen modulo 4 sehen also folgendermaßen aus (es ist üblich, beim Rechnen mit Restklassen die eckigen Klammern einfach wegzulassen und nur den Repräsentanten aufzuschreiben):

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Rechnen kann man also nicht nur mit natürlichen Zahlen, ganzen Zahlen, usw., sondern es gibt eine Vielzahl von Objekten, die sich ähnlich verhalten. Hier haben wir eine endliche Menge aus nur vier Elementen, in der sich addieren und multiplizieren lässt.

Inhaltsverzeichnis

1 Einleitung . . . 2
1.1 Organisation . . . 2
1.2 Kursziele . . . 2
1.3 Voraussetzungen . . . 2
1.4 Aussagen, Sätze, Definitionen,. . . 3
1.5 Logische Schlussfolgerungen . . . 4
2 Beweise . . . 6
2.1 Direkter Beweis . . . 6
2.2 Beweis durch Kontraposition . . . 7
2.3 Beweis durch Widerspruch . . . 8
2.4 Vollständige Induktion . . . 9
3 Mengenlehre . . . 12
3.1 Mengen und ihre Elemente . . . 12
3.2 Teilmengen . . . 12
3.3 Vereinigung, Schnittmenge & Co. . . . 13
4 Abbildungen . . . 15
4.1 Beispiele . . . 15
4.2 Bilder und Urbilder . . . 16
4.3 Injektionen, Surjektionen und Bijektionen . . . 17
5 Modulo . . . 20
5.1 Division mit Rest . . . 20
5.2 Anwendungen . . . 21
5.3 Kongruenz . . . 23