Schüler-Propädeutikum Mathematik 2023
Vortrag 1: Modulorechnung

Andreas Lochmann

31. Oktober 2023

1 Division mit Rest

Mit $\mathbb{Z}$ bezeichnen wir die Menge aller ganzen Zahlen, also

$$\mathbb{Z} \;=\; \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

und mit $\mathbb{N}$ die Menge der natürlichen Zahlen; darunter wollen wir die positiven ganzen Zahlen verstehen, also $\mathbb{N} = \{1, 2, 3, \ldots\}$ ohne die Null.

Definition: (Division mit Rest)
Es seien $n, m \in \mathbb{Z}$ mit $m > 0$. Dann gibt es genau eine Kombination $x \in \mathbb{Z}$, $y \in \mathbb{Z}$ mit

$$n = xm + y \;\text{ und }\; 0 \leq y < m\,, \;\text{ also }\; \frac{n}{m} = x + \frac{y}{m}\,.$$

y heißt **Rest der Division von** n **durch** m, und wir bezeichnen ihn mit $n \,\%\, m$.

Man kann den Rest einer Division $a \,\%\, b$ durch schriftliche Division von Hand bestimmen; man kann ihn aber auch mit Hilfe eines normalen Vierspezies-Taschenrechners berechnen, z.B. wie folgt:

1. Dividiere a durch b.
2. Notiere den Ganzteil des Ergebnisses.
3. Ziehe den Ganzteil vom Ergebnis ab.
4. Multipliziere mit b, das Ergebnis ist der Rest der Division.

Beginnt man mit $a, b \in \mathbb{Z}$, so muss bei diesem Verfahren am Ende eine ganze Zahl übrig bleiben. Aufgrund numerischer Rundungsfehler kann es sein, dass der Taschenrechner ein geringfügig zu großes oder zu kleines Ergebnis ausspuckt; man muss dann zur nächsten ganzen Zahl runden.

Beispiel:
Wir berechnen den Rest von 5397 bei Division durch 19 mit Hilfe eines einfachen Taschenrechners:

$$\begin{aligned} 5397 : 19 &= 284,0526\ldots \\ \ldots - 284 &= \quad 0,0526\ldots \\ \ldots \cdot 19 &= \quad 0,999\ldots, \end{aligned}$$

also ist $5397 = 19 \cdot 284 + 1$ und $5397 \,\%\, 19 = 1$.

2 Teilbarkeit

Definition:
Seien $n, m \in \mathbb{Z}$, $m > 0$. Ist $n \,\%\, m = 0$ sagen wir: n ist durch m **teilbar** bzw. m teilt n, oder in Zeichen: $m \mid n$ (senkrechter Strich zwischen m und n). Dies ist gleichbedeutend zu: Es gibt ein $x \in \mathbb{Z}$ mit $n = mx$. n heißt dann Vielfaches von m, und m heißt Teiler von n.

Frage:
Was sind die Teiler von 21?

Satz:
Es sei $n \in \mathbb{N}$. Von n aufeinander folgenden ganzen Zahlen ist stets genau eine durch n teilbar.

Beweis:
Es sei a die größte der n Zahlen. Es sei $a = nx + y$ mit $x, y \in \mathbb{Z}$, $0 \leq y < n$. Dann ist $a - y$ durch n teilbar und wegen $0 \leq y < n$ eine der n Zahlen. Eindeutigkeit folgt aus der Eindeutigkeit der Division mit Rest. □

Definition: Eine **Primzahl** ist eine positive ganze Zahl $p > 1$, die nur 1 und sich selbst als Teiler besitzt.

Beispiel: Die ersten Primzahlen lauten 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.

3 Kongruenzen

Definition:
Es seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ beliebig. Wir sagen a und b sind zueinander *kongruent* modulo m, in Zeichen $a \equiv b \pmod{m}$ oder einfach $a \equiv b\ (m)$, wenn $a \,\%\, m = b \,\%\, m$ gilt. Die Zahl m in einer Kongruenz wird *Modul* genannt („der Modul“, mit Betonung auf dem „o“).

Eine Zahl ist genau dann durch m teilbar, wenn sie kongruent Null modulo m ist, denn $a \equiv 0\ (m)$ gilt genau dann, wenn $m \mid a - 0$.

Lemma:
Es seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ beliebig. Es gilt $a \equiv b\ (m)$ genau dann, wenn $m \mid a-b$ gilt. Insbesondere ist a genau dann durch m teilbar, wenn $a \equiv 0 \pmod{m}$ gilt.

Beweis:
"$\Rightarrow$": Es sei $a \,\%\, m = b \,\%\, m$. Dann gibt es Zahlen $k, l \in \mathbb{Z}$ mit $a = km + (a \,\%\, m)$ und $b = lm + (b \,\%\, m) = lm + (a \,\%\, m)$, also $a - b = (k-l)m$. Folglich ist $m \mid a - b$.

"$\Leftarrow$": Es sei $m \mid a - b$. Aufgrund der Division mit Rest gibt es Zahlen $k, l \in \mathbb{Z}$ mit $a = km + (a \,\%\, m)$ und $b = lm + (b \,\%\, m)$, also $a - b = (k-l)m + (a \,\%\, m) - (b \,\%\, m)$. Nach Voraussetzung ist $m \mid a - b$, also gibt es $n \in \mathbb{Z}$ mit $a - b = nm$, also

$$(n - k + l)m \;=\; (a \,\%\, m) - (b \,\%\, m)\,.$$

Außerdem wissen wir, dass $0 \leq a \,\%\, m < m$ und $0 \leq b \,\%\, m < m$ gelten, also $-m < (a \,\%\, m) - (b \,\%\, m) < m$. Nun muss aber $(a \,\%\, m) - (b \,\%\, m)$ durch m teilbar sein; das geht nur für $(a \,\%\, m) - (b \,\%\, m) = 0$. □

Erste Rechenregeln für $\equiv$:
Seien $a, b, c \in \mathbb{Z}$ und $m \in \mathbb{N}$.

a) Stets ist $a \equiv a\ (m)$.

b) Ist $a \equiv b\ (m)$, so ist auch $b \equiv a\ (m)$.

c) Ist $a \equiv b\ (m)$ und $b \equiv c\ (m)$, so ist $a \equiv c\ (m)$.

In dieser Hinsicht verhält sich $\equiv$ also wie ein Gleichheitszeichen. Es *ist* zwar kein Gleichheitszeichen (denn beispielsweise ist ja $2 \equiv 7\ (5)$, obwohl $2 \neq 7$ ist), aber es zeigt ein ähnliches Verhalten und ähnliche Rechenregeln. So etwas nennt man auch eine **Äquivalenzrelation**.

Wenn wir Gleichungen umformen, wendet man oft links und rechts die gleiche Operation an. Geht das auch für Kongruenzen?

Prüfen Sie an Beispielen:
Seien $a, b, c, m \in \mathbb{Z}$ beliebig und $m > 0$. Sei $a \equiv b \pmod{m}$. Welche Kongruenzen

sind dann stets richtig?

$$\begin{aligned} a+c &\equiv b+c \pmod m \ ? \\ a-c &\equiv b-c \pmod m \ ? \\ a\cdot c &\equiv b\cdot c \pmod m \ ? \\ a:c &\equiv b:c \pmod m \ ? \\ c:a &\equiv c:b \pmod m \ ? \\ a^c &\equiv b^c \pmod m \ ? \\ c^a &\equiv c^b \pmod m \ ? \\ \sqrt{a} &\equiv \sqrt{b} \pmod m \ ? \end{aligned}$$

(Die Division ist nur sinnvoll, wenn die jeweiligen Divisionen ganz aufgehen. Die letzte Frage ist nur sinnvoll, wenn a und b Quadratzahlen sind.)

Mehr Rechenregeln für $\equiv$:
Seien $a, b, c, m \in \mathbb{Z}$ beliebig und $m > 0$. Sei $a \equiv b \pmod m$. Dann gelten auch:

$$\begin{aligned} a+c &\equiv b+c \pmod m \\ a-c &\equiv b-c \pmod m \\ a\cdot c &\equiv b\cdot c \pmod m \end{aligned}$$

Ist $c \geq 0$ gilt außerdem $a^c \equiv b^c \pmod m$.

Beweis:
Wegen $a \equiv b \pmod m$ ist $m \mid a-b$.

1) Dann ist auch $m \mid (a+c)-(b+c)$ und daher $a+c \equiv b+c$.

2) Analog gilt $m \mid (a-c)-(b-c)$ und daher $a-c \equiv b-c$.

3) Ist m ein Teiler von $a-b$, so ist m auch ein Teiler von $(a-b)\cdot c = ac-bc$, und daher $ac \equiv bc$.

4) Folgt aus wiederholter Anwendung von Regel (3). □

Sofern es also die Addition, Subtraktion, Multiplikation und Potenzen mit natürlichen Zahlen betrifft, können Zahlen in einer Rechnung gegen kongruente Zahlen ersetzt werden. Beispielsweise ist

$$7\cdot 5 \ = \ 35 \ \equiv \ 3 \ (4)\,,$$

und da $7 \equiv 3$ ist, ist auch

$$3\cdot 5 \ = \ 15 \ \equiv \ 3 \ (4)\,.$$

Beispiel:
Wir wollen wissen, was der Rest von $123 \cdot 458$ bei Division durch 7 ist. Dazu berechnen wir zunächst $123 = 70 + 53 = 70 + 49 + 4$, also $123 \,\%\, 7 = 4$, sowie $458 = 420 + 38 = 420 + 35 + 3$, also $456 \,\%\, 7 = 3$. Damit ist $123 \equiv 4 \ (7)$ und $456 \equiv 3 \ (7)$, also $123 \cdot 456 \equiv 12 \ (7)$. Es reicht daher aus, den Rest von 12 bei Division durch 7 zu berechnen, und das ist 5, also $(123 \cdot 458) \,\%\, 7 = 5$.

Aufgabe:
Was ist $23^7 \,\%\, 11$? Rechnen Sie im Kopf.

Vorsicht bei der Division! Es ist im allgemeinen nicht möglich, aus einer Kongruenz zu kürzen. Beispielsweise ist $2 \cdot 8 \equiv 2 \cdot 3 \ (10)$, aber $8 \not\equiv 3 \ (10)$. Auch in einem Nenner modulo zu rechnen ist gefährlich, solange Nenner und Modul nicht teilerfremd sind:

$$2 \;=\; \frac{4}{2} \;\not\equiv\; \frac{4}{-4} \;=\; -1 \pmod 6 .$$

Auch **Wurzelziehen** ist im allgemeinen nicht möglich. Es gilt zwar $16 \equiv 25 \ (9)$, aber $4 \not\equiv 5 \ (9)$.

Potenzieren mit einer festen, natürlich-zahligen Potenz ist letztlich nur mehrfache Multiplikation und daher kann die Basis einer Potenz gegen eine kongruente Zahl ersetzt werden, Beispiel:

$$7^3 \;=\; 343 \;\equiv\; 3 \,(4)\,, \text{ ebenso ist } 3^3 \;=\; 27 \;\equiv\; 3 \,(4)\,.$$

4 Knobelaufgaben für zu Hause

Knobelaufgabe 1:
Zeigen Sie: Für $x \in \mathbb{Z}$ ist $x^2 + 2$ niemals durch 5 teilbar.

Hinweis: Stellen Sie eine Liste von $(x^2 + 2) \,\%\, 5$ auf. Schauen Sie sich an, welche Reste möglich sind, und welche nicht.

Knobelaufgabe 2:
Es sei p eine Primzahl mit $p \equiv 2 \pmod 7$. Zeigen Sie: $p + 12$ ist durch 7 teilbar und $(p + 12)/7$ ist nicht durch 3 teilbar.

Knobelaufgabe 3:
Es sei n eine ungerade Zahl. Zeigen Sie, dass dann $2n + 5$ keine Quadratzahl sein kann.