# Matheschülerzirkel Klasse 7/8

Tim Baumann



Notation. Wir verwenden die folgenden Bezeichnungen:

- Menge der natürlichen Zahlen
- $\{..., -2, -1, 0, 1, 2, ...\}$  $\frac{1}{3}, \frac{-17}{2}, 1 \in \mathbb{Q}$  $\mathbb{Z}$ Menge der ganzen Zahlen
- Menge der rationalen Zahlen

22. November 2013

## Unmöglichkeitsbeweise über Invarianten

Wird demnächst nachgetragen!

Aufgabe. Auf einer Insel leben 345 gelbe, 346 grüne und 347 blaue Chamäleons. Wann immer sich zwei Chamäleons gleicher Farbe begegnen, passiert nichts. Wenn sich aber zwei Chamäleons unterschiedlicher Farbe begegnen, so nehmen beide die dritte Farbe an. Beispielsweise hätten wir nach einem Treffen eines gelben und einer grünen Chameleons nur noch 344 gelbe, 345 grüne, aber dafür 349 blaue Chameleons. Frage: Ist es möglich, dass zu einem Zeitpunkt genau gleich viele Chameleons jeder Farbe auf der Insel leben?

Grundsätzlich könnte diese Situation eintreten, da 345 + 346 + 347 = 1038 durch 3 teilbar ist. Wenn wir allerdings versuchen, eine Liste von Begegnungen zu erstellen, sodass nach diesen Begegnungen die Anzahl der Chamäleons jeder Farbe gleich ist, scheitern wir. Deshalb vermuten wir, dass dieses Problem nicht lösbar ist.

6. Dezember 2013

## 2 Rechnen mit Restklassen

### 2.1 Teilbarkeit

**Definition 1.** Eine Zahl  $b \in \mathbb{Z}$  ist durch  $a \in \mathbb{Z}$  teilbar, wenn es eine Zahl  $c \in Z$  gibt mit

$$a \cdot c = b$$
.

**Notation.** Wir verwenden dann die Kurzschreibweise  $a \mid b$ , gesprochen "a teilt b". Wir sagen auch, dass a ein *Teiler* von b ist oder dass b ein Vielfaches von a ist. Im Fall, dass die Zahl a die Zahl b nicht teilt, d. h. keine Zahl  $c \in \mathbb{Z}$  existiert mit  $a \cdot c = b$ , schreiben wir  $a \nmid b$ .

Beispiel. Folgende Aussagen stimmen:

• 3 | 6

5 ∤ 13

8 | −8

• 3 | 12345

2 ∤ 1001

**Exkurs.** Der Ausdruck  $a \mid b$  ist eine mathematische Aussage. Andere Beispiele für mathematische Aussagen sind:

•  $\sqrt{2}$  ist irrational

• 3 > 5

• *n* ist gerade

 $\bullet$  *m* ist eine Primzahl

• Jeder Winkel lässt sich mit Zirkel und Lineal halbieren.

• Für  $n \in \mathbb{N}$  mit  $n \ge 2$  gibt keine Zahlen  $a, b, c \in \mathbb{N}$ , sodass  $a^n + b^n = c^n$  stimmt.

• Es gibt unendlich viele Primzahlenzwillinge, das sind Primzahlen p und q, mit q = p + 2.

Mathematische Aussagen sind entweder richtig oder falsch. Beispielsweise ist in den obigen Beispielen die erste wahr, die zweite falsch und über die nächsten beiden können wir nichts sagen, da sie Zahlen n und m beinhalten, die erst noch genauer definiert werden müssen. Die vorletzte Aussage trägt den Namen "Fermats letzter Satz" und ist richtig, doch hat es über 300 Jahre gedauert, bis sie bewiesen werden konnte. Von der letzten Aussage wird vermutet, dass sie stimmt, es existiert jedoch kein Beweis.

**Frage.** Gibt es eine Zahl  $a \in \mathbb{Z}$ , die Teiler von 0 ist, d. h.  $a \mid 0$ ?

**Antwort.** Ja, wir können sogar jede beliebige Zahl  $a \in Z$  nehmen: Setze c := 0, dann ist  $a \cdot c = a \cdot 0 = 0$  und somit ist die Definition erfüllt.

**Frage.** Gibt es andersherum eine Zahl  $b \in \mathbb{Z}$ , die durch 0 teilbar ist, also  $0 \mid b$ ?

**Antwort.** Ja, aber nur die Zahl 0 selber. Mit a = 0, ist für ein beliebiges c nämlich  $a \cdot c = 0 \cdot c = 0$ , also muss b = 0 sein.

**Exkurs.** Sei  $z \in \mathbb{Z}$  eine ganze Zahl. Wenn z ungerade ist, so ist z nicht durch 8 teilbar. Um nicht immer "wenn …, dann …" schreiben zu müssen, verwenden Mathematiker folgende Notation:

$$z$$
 ist ungerade  $\implies z \nmid 8$ 

Dabei stehen auf der linken und rechten Seite des  $\Rightarrow$ -Zeichens mathematische Aussagen P und Q. Die Zeile  $(P\Rightarrow Q)$  ist wiederum selbst eine mathematische Aussage, nämlich die Aussage, dass wenn P stimmt, dann auch Q stimmt. Dabei ist es wichtig, dass links P steht und rechts Q, denn in unserem Beispiel stimmt die Aussage andersrum nicht: Wenn z nicht durch 8 teilbar ist, dann muss z noch nicht unbedingt ungerade sein. Z. B. ist z=4 nicht durch 8 teilbar, aber gerade.

Ein anderes Beispiel: Eine ganze Zahl m ist ungerade, wenn die Zahl (m+1) gerade ist. Andersrum ist (m+1) gerade, wenn m ungerade ist. Hier ist also die Umkehrung erfüllt, im Gegensatz zum vorherigen Beispiel. Also ist m immer dann und nur dann ungerade, wenn (m+1) ungerade ist. Mathematiker verwenden dafür eine besondere Notation:

$$n$$
 ist ungerade  $\iff$   $(n+1)$  ist gerade

Auf beiden Seiten des  $\Leftrightarrow$ -Zeichens stehen dabei wieder mathematische Aussagen. Der Pfeil  $\Leftrightarrow$  bedeutet, dass die linke Aussage nur dann stimmt, wenn die rechte Aussage stimmt.

Wir wollen nun ein paar Tatsachen über die Teilbarkeit beweisen.

Behauptung 1. Seien  $n, p, q \in \mathbb{Z}$  ganze Zahlen. Dann gilt:

- (i)  $n \mid p \text{ und } p \mid q \implies n \mid q$
- (ii)  $n \mid p \implies n \mid (p \cdot q)$
- (iii)  $n \mid p \text{ und } n \mid q \implies n \mid (p+q)$

Beweis. Zu (i): Aus der Definition von Teilbarkeit wissen wir, dass es  $c, d \in \mathbb{Z}$  gibt mit

$$n \cdot c = p$$
 und  $p \cdot d = q$ 

Um zu zeigen, dass  $n \mid q$  gilt, müssen wir nach derselben Definition eine Zahl für die Leerstelle finden, sodass die Gleichung

$$n \cdot \underline{\hspace{0.5cm}} = q$$

erfüllt ist. Wir behaupten, dass die Zahl  $(c \cdot d)$  dies leistet. Wir rechnen nämlich nach:

$$n \cdot (c \cdot d) = \underbrace{(n \cdot c) \cdot d}_{=p} \cdot d = q.$$

Dabei haben wir im ersten Schritt das Assoziativgesetz gebraucht.

Zu (ii): Aus der Definition von Teilbarkeit erhalten wir ein  $c \in \mathbb{Z}$  mit

$$n \cdot c = p$$
.

Wir müssen folgene Leerstelle sinnvoll ersetzen:

$$n \cdot \underline{\hspace{1cm}} = p \cdot q.$$

Wir nehmen dafür die Zahl  $(c \cdot q)$  und rechnen

$$n \cdot (c \cdot q) = \underbrace{(n \cdot c) \cdot q}_{=n} = p \cdot q$$

Zu (iii): Aus der Definition erhalten wir  $c, d \in \mathbb{Z}$  mit

$$n \cdot c = p$$
 und  $n \cdot d = q$ .

Es soll folgende Gleichung gelten:

$$n \cdot \underline{\hspace{1cm}} = p + q$$

Wir setzen (c+d) für \_\_ und rechnen

$$n \cdot (c+d) = \underbrace{n \cdot c}_{=p} + \underbrace{n \cdot d}_{=q} = p+q.$$

Im ersten Schritt haben wir dabei das Distributivgesetz angewendet.

Achtung. Folgendes Rechengesetz gilt nicht:

$$p \mid n \text{ und } q \mid n \implies (p \cdot q) \mid n$$

Ein Gegenbeispiel dafür ist p = 4, q = 6, n = 12.

**Exkurs.** In den natürlichen Zahlen  $\mathbb{N}$ , den ganzen Zahlen  $\mathbb{Z}$  und den rationalen Zahlen  $\mathbb{Q}$  gelten folgende Rechenregeln:

- Kommutativgesetz: a + b = b + a und  $a \cdot b = b \cdot a$
- Assoziativgesetz: a + (b + c) = (a + b) + c und  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
- Distributivgesetz:  $a \cdot (b + c) = a \cdot b + a \cdot c$

Es ist eine gute Übung, sich zu überlegen, welche Plus- und Mal-Zeichen wir durch Minus- und Divisions-Zeichen ersetzen dürfen, sodass die Regeln immer noch stimmen.

#### 2.2 Restklassen

Sei n eine natürliche Zahl und p,q natürliche Zahlen, die bei der Division durch n den gleichen Rest r haben, also

$$p: n = a \text{ Rest } r$$
  
 $q: n = b \text{ Rest } r$ 

für zwei Zahlen  $a, b \in \mathbb{Z}$ . Wir können dabei außerdem annehmen, dass r eine Zahl zwischen 0 bis n-1 ist (warum?). Wenn wir obige Gleichungen umschreiben, erhalten wir

$$p = n \cdot a + r,$$
$$q = n \cdot b + r.$$

Wir rechnen:

$$p - q = (n \cdot a + r) - (n \cdot b + r) = n \cdot a + r - n \cdot b - r = n \cdot a + n \cdot b = n \cdot (a + b).$$

Wir haben also  $n \cdot (a + b) = p - q$ , folglich nach Definition von Teilbarkeit  $n \mid (p - q)$ . Dies ist unser erstes halbwegs interessantes Ergebnis: Zwei Zahlen p und q, die bei Division durch n den gleichen Rest haben, unterscheiden sich nur durch ein Vielfaches von n.

**Definition 2.** Für zwei Zahlen p und q, die sich nur durch ein Vielfaches von  $n \in N$  unterscheiden (d. h.  $n \mid (p-q)$ ) schreiben wir

$$p \equiv q \pmod{n}$$
.

Wir sprechen: "p ist gleich q modulo n".

**Notation.** Falls  $p \equiv q \pmod{n}$  nicht stimmt, schreiben wir  $p \not\equiv q \pmod{n}$ .

Beispiel. Folgende Aussagen stimmen:

- $1 \equiv 4 \pmod{3}$   $-4 \equiv 3 \pmod{7}$   $4 \not\equiv 2 \pmod{4}$
- $0 \equiv 16 \pmod{8}$   $-1001 \equiv -1003 \pmod{2}$   $0 \not\equiv -101 \pmod{3}$

**Achtung.** Wir dürfen den Teil in Klammern auf keinen Fall weglassen! Es gilt nämlich  $4 \equiv 7 \pmod{3}$ , aber nicht  $4 \equiv 7 \pmod{6}$ !

**Behauptung 2.** Sei  $n \in \mathbb{N}$  und die Zahlen  $a, a_1, a_2, b, b_1, b_2, c \in \mathbb{Z}$ . Dann gilt:

- (i)  $a \equiv a \pmod{n}$
- (ii)  $a \equiv b \pmod{n}$  und  $b \equiv c \pmod{n} \implies a \equiv c \pmod{n}$
- (iii)  $a_1 \equiv a_2 \pmod{n}$  und  $b_1 \equiv b_2 \pmod{n} \implies a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$
- (iv)  $a_1 \equiv a_2 \pmod{n}$  und  $b_1 \equiv b_2 \pmod{n} \implies a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{n}$

Beweis. Zu (i): Es ist a - a = 0 und somit gilt  $n \mid (a - a)$ , da 0 von jeder beliebigen Zahl geteilt wird.

Zu (ii): Es gilt nach Vorraussetzung  $n \mid (a-b)$  und  $n \mid (b-c)$ , also nach unserem Wissen über Teilbarkeit

$$n \mid \underbrace{((a-b) + (b-c))}_{=(a-c)}.$$

Zu (iii): Nach Vorraussetzung gilt  $n \mid (a_1 - a_2)$  und  $n \mid (b_1 - b_2)$ . Somit

$$n \mid \underbrace{((a_1 - a_2) - (b_1 - b_2))}_{=(a_1 + b_1) - (a_2 + b_2)}.$$

Zu (iv): Nach Vorraussetzung gilt  $n \mid (a_1 - a_2)$  und  $n \mid (b_1 - b_2)$ . Somit gilt auch

$$n \mid (a_1 - a_2) \cdot b_1$$
 und  $n \mid a_2 \cdot (b_1 - b_2)$ ,

also auch  $n \mid ((a_1 - a_2) \cdot b_1 + a_2 \cdot (b_1 - b_2))$ . Es gilt aber

$$(a_1 - a_2) \cdot b_1 + a_2 \cdot (b_1 - b_2) = a_1 \cdot b_1 - a_2 \cdot b_1 + a_2 \cdot b_1 - a_2 \cdot b_2 = a_1 \cdot b_1 - a_2 \cdot b_2,$$

somit ist dies zu  $n \mid (a_1 \cdot b_1 - a_2 \cdot b_2)$ .