## *Rechenregeln in mod*

### *Die modulare Multiplikation: a mod c · b mod c ≡ (a · b) mod c*

1. *Beispiel: a = 7 , b = 8 , c = 5*

- *Trage die Zahlen in die Tabelle unten ein und ergänze die Spalten.*
- *Ergänze die nächsten drei Zeilen durch eigene Beispiele.*

| a | b | c | a · b | a mod c | b mod c | a mod c · b mod c | (a · b) mod c |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

2. ***Beachte auch hier wieder den Unterschied zwischen ≡ und =***
*Formuliere die Aussage der Überschrift wie bei „Addition“ als Gleichung:*

_____

3. *Gibt es bei deinen Beispielen ebenfalls Unterschiede in den letzten beiden Spalten? Konstruiere Beispiele, bei denen sich die letzten beiden Spalten unterscheiden/nicht unterscheiden.*

| a | b | c | a · b | a mod c | b mod c | a mod c · b mod c | (a · b) mod c |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

4. *Unter welchen Bedingungen unterscheiden sich die beiden letzten Einträge?*

5.* *Beweise den Satz allgemein. Beachte die bereitgestellten Hilfen: Schätze ein, wie stark du dir helfen lassen willst und wähle die Stufe (rot – geringste Hilfe , gelb – schwache Hilfe, blau – starke Hilfe, grün - Nachvollzug)*

***Für die Lehrkraft:*** *gestufte Hilfen zur Auslage im Klassenraum. Ausdrucke auf farbigem Papier erleichtern die Zuordnung für die SuS (Farben siehe auf dem Arbeitsblatt).*

## Stufe 1 - geringste Hilfe

Erinnere: Der Ausdruck a mod c ist definiert als Division einer natürlichen Zahl a mit Rest q.

- Erzeuge diese Darstellungen von a mod c und b mod c
- Zeige damit, dass die beiden Seiten der Behauptung gleich sind.

## Stufe 2 - mittlere Hilfe

Erinnere: für natürliche Zahlen a, b, c, k, p, r, q ist „... mod...“ festgelegt durch

$a \bmod c = p \Leftrightarrow a = k \cdot c + p$ und $b \bmod c = q \Leftrightarrow b = r \cdot c + q$

- Setze diese Darstellungen jeweils in eine Seite der Behauptung ein.
- Vereinfache mit dem Ziel, bei beiden Seiten den gleichen Term zu erhalten.

## Stufe 3 - starke Hilfe: Beweispuzzle

*Es sei* $a = k \cdot c + p$ *und* $b = r \cdot c + q$ , *o.B.d.A* $c \nmid p, q$

$\Rightarrow a \bmod c = p$ *und* $b \bmod c = q$

*1)* $(a \bmod c \cdot b \bmod c) \bmod c$

$= ((k \cdot c + p) \bmod c \cdot (r \cdot c + q) \bmod c) \bmod c$

$= (p \cdot q) \bmod c$

*2)* $a \cdot b$

$= (k \cdot c + p) \cdot (r \cdot c + q)$

$= (k \cdot r) \cdot c^2 + p \cdot r \cdot c + k \cdot q \cdot c + p \cdot q$

$= (k \cdot r \cdot c + p \cdot r + k \cdot q) \cdot c + p \cdot q$

$= n \cdot c + p \cdot q$

$\Rightarrow (a \cdot b) \bmod c$

$= (n \cdot c + p \cdot q) \bmod c$

$= (p \cdot q) \bmod c$

$\Rightarrow (a \bmod c \cdot b \bmod c) \bmod c = (a \cdot b) \bmod c$ ■

## Stufe 4: Nachvollzug

*Unten siehst du den Beweis.Übertrage ihn Schritt für Schritt ins Heft. Vollziehe dabei jeden Schritt nach und halte jeweils auf der rechten Seite daneben fest, was in dem jeweiligen Schritt getan wird, welche Gesetze zur Anwendung kommen usw.*

***zu zeigen:*** $(a \bmod c \cdot b \bmod c) \bmod c = (a \cdot b) \bmod c$

*Beweis:* Es sei $a = k \cdot c + p$ und $b = r \cdot c + q$ , o.B.d.A $c \nmid p, q$

$\Rightarrow a \bmod c = p$ und $b \bmod c = q$

1) $(a \bmod c \cdot b \bmod c) \bmod c$

$= ((k \cdot c + p) \bmod c \cdot (r \cdot c + q) \bmod c) \bmod c$

$= (p \cdot q) \bmod c$

2) $a \cdot b$

$= (k \cdot c + p) \cdot (r \cdot c + q)$

$= (k \cdot r) \cdot c^2 + p \cdot r \cdot c + k \cdot q \cdot c + p \cdot q$

$= (k \cdot r \cdot c + p \cdot r + k \cdot q) \cdot c + p \cdot q$

$= n \cdot c + p \cdot q$

$\Rightarrow (a \cdot b) \bmod c$

$= (n \cdot c + p \cdot q) \bmod c$

$= (p \cdot q) \bmod c$

1) & 2) $\Rightarrow (a \bmod c \cdot b \bmod c) \bmod c = (a \cdot b) \bmod c$ ■