

Rechenregeln in mod

Die modulare Multiplikation: $a \bmod c \cdot b \bmod c \equiv (a \cdot b) \bmod c$

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

a	b	c	$a \cdot b$	$a \bmod c$	$b \bmod c$	$a \bmod c \cdot b \bmod c$	$(a \cdot b) \bmod c$
7	8	5	56	2	3	6	1

Individuell

2. Formuliere die Aussage der Überschrift wie bei „Addition“ als Gleichung:

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

3. Konstruiere Beispiele, bei denen sich die letzten beiden Spalten unterscheiden/nicht unterscheiden.

a	b	c	$a \cdot b$	$a \bmod c$	$b \bmod c$	$a \bmod c \cdot b \bmod c$	$(a \cdot b) \bmod c$
<i>Individuell</i>							

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

Sie unterscheiden sich, wenn das Produkt der Reste größer ist als die Modulzahl c , also wenn $(a \bmod c) \cdot (b \bmod c) > c$.