

17.04.2007

4. Entscheiden Sie mit Hilfe einer Wahrheitstafel, ob die folgenden Äquivalenzen richtig sind.

① 
$$a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c)$$

a	b	c	$b \vee c$	$a \wedge (b \vee c)$	$a \wedge b$	$a \wedge c$	$(a \wedge b) \vee (a \wedge c)$
0	0	0	0	0	0	0	0
0	0	1	1	0	0	0	0
0	1	0	1	0	0	0	0
0	1	1	1	0	0	0	0
1	0	0	0	0	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

=  
Äquivalenz gilt! (s.a. Distributivgesetz)

6. Wie 4

$$a \leftrightarrow b \Leftrightarrow (a \rightarrow b) \rightarrow \neg(b \rightarrow a)$$

a	b	$a \leftrightarrow b$	$a \rightarrow b$	$b \rightarrow a$	$\neg(b \rightarrow a)$	$(a \rightarrow b) \rightarrow \neg(b \rightarrow a)$
0	0	1	1	1	0	0
0	1	0	1	0	1	1
1	0	0	0	1	0	1
1	1	1	1	1	0	0

≠  
Äquivalenz gilt NICHT!

79 Lösen Sie die folgenden Kongruenzen (d.h. Gleichungen in Restklassen

17.4.2007

in  $\mathbb{Z}$ ) bzw. beweisen Sie die Unlösbarkeit (in  $\mathbb{Z}$ ):

② a)  $x^2 - 3x + 2 \equiv 0 \pmod{5}$

b)  $x^2 - 3x + 2 \equiv 0 \pmod{6}$

a)  $x^2 - 3x + 2 \equiv 0 \pmod{5}$

$$(x-1)(x-2) \equiv 0 \pmod{5} \Leftrightarrow$$

$$5 \mid (x-1)(x-2) \Rightarrow (x-1) = 0 \vee (x-2) = 0 \Rightarrow$$

$$\underline{x = \bar{1}, \bar{2} \in \mathbb{Z}_5}$$

$(x-1) = 5 \vee (x-2) = 5$  ist in  $\mathbb{Z}_5$  nicht lösbar!

b)  $x^2 - 3x + 2 \equiv 0 \pmod{6}$

$$(x-1)(x-2) \equiv 0 \pmod{6} \Leftrightarrow$$

$$6 \mid (x-1)(x-2) \Leftrightarrow$$

$$2 \cdot 3 \mid (x-1)(x-2) \quad \text{da entweder } (x-1) \vee (x-2) \text{ immer gerade}$$

ist, gilt  $2 \mid (x-1)(x-2)$  immer!

$$3 \mid (x-1)(x-2) \Rightarrow (x-1) = 0 \vee (x-2) = 0 \Rightarrow$$

$$x = \bar{1}, \bar{2} \in \mathbb{Z}_3$$

$$\text{Lösung in } \mathbb{Z}_6 = \{ \bar{1}, \bar{2}, \overline{1+3}, \overline{2+3} \} =$$

$$\underline{\underline{\{ \bar{1}, \bar{2}, \bar{4}, \bar{5} \in \mathbb{Z}_6 \}}}$$



Lösen Sie folgende Kongruenzen (d.h. Gleichungen in Restklassen

11.04.2007

in  $\mathbb{Z}$ ) bzw. beweisen Sie die Lösbarkeit (in  $\mathbb{Z}$ ):

③

a)  $6x \equiv 3 \pmod{9}$

b)  $6x \equiv 4 \pmod{9}$

Definition:

$a \equiv b \pmod{m}$  gilt, wenn  $m \mid a-b$

a) • Ist a) lösbar? Wieviele Lösungen gibt es?

$\text{ggT}(6,9) = 3 \quad 3 \mid 3 \rightarrow$  Es existieren 3 Lösungen!

Lösbarkeit:

$ax \equiv b \pmod{m}$   
ist lösbar, wenn  $\text{ggT}(a,m) \mid b$

$6x \equiv 3 \pmod{9}$

$2x \cdot 3 \equiv 1 \cdot 3 \pmod{3 \cdot 3}$

$2x \equiv 1 \pmod{3}$

•  $\text{ggT}(2,3) = 1 \quad 1 \mid 1 \rightarrow$  Es existiert genau 1 Lsg!

$x = \bar{2} \in \mathbb{Z}_3$

Anzahl d. Lösungen:

$\text{ggT}(a,m)$

in  $\mathbb{Z}_q$ ?

$x_1 = \bar{2} + 0 = \bar{2}$

$x_2 = \bar{2} + 3 = \bar{5}$

$x_3 = \bar{2} + 6 = \bar{8}$

Warum? Gesucht sind 3 Lsg, die in  $\mathbb{Z}_3$  kongruent, in  $\mathbb{Z}_9$  jedoch inkongruent sind!

$x = \{ \bar{2}, \bar{5}, \bar{8} \} \in \mathbb{Z}_9$

Rechenregeln:

•  $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$   
 $\Rightarrow a+c \equiv b+d \pmod{m}$

•  $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$   
 $\Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$

•  $a \cdot c \equiv b \cdot c \pmod{m} \wedge$   
 $\text{ggT}(c,m) = 1$

$\Rightarrow a \equiv b \pmod{m}$

•  $a \cdot c \equiv b \cdot c \pmod{m} \wedge$   
 $c \neq 0$   
 $\Rightarrow a \equiv b \pmod{\frac{m}{\text{ggT}(c,m)}}$

b) • Ist b) lösbar?

$\text{ggT}(6,9) = 3 \quad 3 \nmid 4 \rightarrow$  b) ist unlösbar!

Warum?  $6x \equiv 4 \Leftrightarrow 9 \mid (6x-4) \Leftrightarrow 9 \cdot k = 6x-4, k \in \mathbb{Z} \Leftrightarrow$

$9k+4 = 6x \Leftrightarrow \frac{9k+4}{6} = x \Leftrightarrow$

$\frac{3}{2}k + \frac{2}{3} = x$  ! Da  $k \in \mathbb{Z}$  ist keine Lösung möglich!

QED