Euklid

à la Übungsleitung

Carlos Camino

www.carlos-camino.de/ds

Wintersemester 2015/16

„Bitte genau an dieses Format halten, das wird genauso in der Klausur verlangt werden, sollte eine entsprechende Aufgabe vorkommen.“

- Die Übungsleitung

Erinnerung

Was macht der erweiterte Euklidische Algorithmus?

Erinnerung

Was macht der erweiterte Euklidische Algorithmus?

Für zwei gegebene Zahlen $a, b \in \mathbb{N}$ beantwortet er folgende Fragen:

1. Was ist $\mathrm{ggT}(a, b)$?
2. Für welche $s, t \in \mathbb{Z}$ gilt folgende Gleichung?

$$as + bt = \mathrm{ggT}(a, b)$$

Erinnerung

Was macht der erweiterte Euklidische Algorithmus?

Für zwei gegebene Zahlen $a, b \in \mathbb{N}$ beantwortet er folgende Fragen:

1. Was ist $\mathrm{ggT}(a, b)$?
2. Für welche $s, t \in \mathbb{Z}$ gilt folgende Gleichung?

$$as + bt = \mathrm{ggT}(a, b)$$

Falls $\mathrm{ggT}(a, b) = 1$, dann gilt $a \in \mathbb{Z}_b^*$ und es entsteht die Frage:

3. Was ist das Inverse a^{-1} zu a in $\mathbb{Z}_b^*$?

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100			

21 und 100 eintragen.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21 16	100	4		

$100 \div 21 = 4$ Rest 16.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21			

21 kopieren.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5				

$21 \div 16 = 1$ Rest 5.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5	16			

16 kopieren.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5	16	3		
1				

$16 \div 5 = 3$ Rest 1.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5	16	3		
1	5			

5 kopieren.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5	16	3		
1	5	5		
0				

$5 \div 1 = 5$ Rest 0.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5	16	3		
1	5	5		
0	–	–		–

Sobald 0 als Rest rauskommt, ist die linke Hälfte fertig.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5	16	3		
1	5	5		
0	–	–		–

Für die rechte Hälfte braucht man nur k.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5	16	3		1
1	5	5	1	0
0	–	–	0	–

s und t mit 0 und 1 initialisieren.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		
5	16	3	-3	1
1	5	5	1	0
0	–	–	0	–

$$0 - (3 \cdot 1) = -3.$$

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1		-3
5	16	3	-3	1
1	5	5	1	0
0	–	–	0	–

-3 kopieren.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		
16	21	1	4	-3
5	16	3	-3	1
1	5	5	1	0
0	–	–	0	–

$$1 - (1 \cdot (-3)) = 4.$$

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4		4
16	21	1	4	-3
5	16	3	-3	1
1	5	5	1	0
0	–	–	0	–

4 kopieren.

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4	-19	4
16	21	1	4	-3
5	16	3	-3	1
1	5	5	1	0
0	–	–	0	–

$$-3 - (4 \cdot 4) = -19.$$

Beispiel

Für $a = 21$ und $b = 100$ erhalten wir:

a	b	k	s	t
21	100	4	-19	4
16	21	1	4	-3
5	16	3	-3	1
1	5	5	1	0
0	–	–	0	–

Daraus folgt:

1. $\mathrm{ggT}(21, 100) =$ 1 (d.h. $21 \in \mathbb{Z}_{100}^*$).
2. 21 $\cdot$ (-19) $+$ 100 $\cdot$ 4 $=$ 1 .
3. $21^{-1} =$ (-19) mod 100 $= 81$.

Noch ein Beispiel

Für $a = 28$ und $b = 74$ erhalten wir:

a	b	k	s	t
28	74	2	8	-3
18	28	1	-3	2
10	18	1	2	-1
8	10	1	-1	1
2	8	4	1	0
0	–	–	0	–

Noch ein Beispiel

Für $a = 28$ und $b = 74$ erhalten wir:

a	b	k	s	t
28	74	2	8	-3
18	28	1	-3	2
10	18	1	2	-1
8	10	1	-1	1
2	8	4	1	0
0	–	–	0	–

Daraus folgt:

1. $\mathrm{ggT}(28, 74) = 2$ (d.h. $28 \notin \mathbb{Z}_{74}^*$).
2. $28 \cdot 8 + 74 \cdot (-3) = 2$.
3. Wegen $28 \notin \mathbb{Z}_{74}^*$ besitzt 28 somit kein Inverses in $\mathbb{Z}_{74}^*$.

Viel Spaß beim Üben!