EZT Übungsblatt 6

1.) (1) $3 \cdot x + 17 \cdot y = 158$

Erw. Euklidischer Algo: für (17, 3):

$17 = 5 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$\Rightarrow ggT(17, 3) = 1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (17 - 5 \cdot 3)$

$= 6 \cdot 3 - 1 \cdot 17$

$\Rightarrow 3 \cdot 6 - 17 \cdot 1 = 1 \quad | \cdot 158$

$\Rightarrow 3 \cdot 948 - 17 \cdot 158 = 158$

$\Rightarrow$ Partikulärlsg. $(x_0, y_0) = (948, -158)$

Alle Lösungen (Satz 4.18): $\mathbb{L} = \{(x_0 + t \cdot 17, y_0 - t \cdot 3) \mid t \in \mathbb{Z}\}$ (unendl. viele)

(2) $9 \cdot x + 16 \cdot y = 35$

Erw. Euklidischer Algo für (16, 9):

$16 = 1 \cdot 9 + 7$

$9 = 1 \cdot 7 + 2$

$7 = 3 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$\Rightarrow ggT(16, 9) = 1 = 7 - 3 \cdot 2 = 7 - 3 \cdot (16 - 1 \cdot 9) - 3 \cdot 2$

$= 16 - 1 \cdot 9 - 3 \cdot (9 - 1 \cdot 7)$

$= 16 - 1 \cdot 9 - 3 \cdot 9 + 3 \cdot (16 - 1 \cdot 9)$

$= 4 \cdot 16 - 7 \cdot 9$

$\Rightarrow$ Partikulärlsg. $(x_0, y_0) = (-7 \cdot 35, 4 \cdot 35)$

$= (-245, 140)$

$\Rightarrow$ Alle Lösungen $\mathcal{L} = \{ (x_0 + t \cdot 16), (y_0 - t \cdot 9) \mid t \in \mathbb{Z} \}$
(unendlich viele)

2.)

- Lösbare lineare diophantische Gleichung:

$$3 \cdot x + 17 \cdot y = 198423178910$$

(klar, da $ggT(3, 17) = 1$. Daher

$$\operatorname{im}(\underbrace{3 \cdot x + 17 \cdot y}_{\text{als Polynom } \mathbb{Z}[x,y]}) = \mathbb{Z} \cdot ggT(3, 17) = \mathbb{Z})$$

- Unlösbare lineare Diophantische Gleichung:

$$18 \cdot x + 24 \cdot y = 17$$

$ggT(\cdot,\cdot) = 6$

unlösbar über $\mathbb{Z}$, da $\underset{ggT(18,24)}{\underset{\shortparallel}{6}} \nmid 17$

$ggT(a,b) = 1$ ✓

- **Lemma 1:** Wenn $a \cdot x + b \cdot y = c$ mit $a, b, c \in \mathbb{Z}$ lösbar für ein $(x_0, y_0) \in \mathbb{N} \times \mathbb{N}$, so gibt es $(x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$ mit $x_1 < 0 \lor y < 0$.

Bew.:

Satz 4.18 $\Rightarrow$ alle Lösungen $\mathcal{L} = \{ (x_0 + t \cdot b, y_0 - t \cdot a) \mid t \in \mathbb{Z} \}$

~~Wähle $t^* = \frac{-x_0 - 1}{b}$~~

~~$\Rightarrow (x^*, y^*) = (x_0 + \frac{-x_0 - 1}{b} \cdot b, \ldots)$~~

~~$= t$~~

Klar, dass für geeignete t erste oder zweite Komponente < 0 werden. $\square$

Korollar: Lemma 1 gilt auch mit $ggT(a,b) \neq 1$

Bew.:

Wenn $ax + by = c$ lösbar, dann $ggT(a,b) \mid c$.

$$\Rightarrow \underbrace{\frac{a}{ggT(a,b)}}_{a'} x + \underbrace{\frac{b}{ggT(a,b)}}_{b'} y = \underbrace{\frac{c}{ggT(a,b)}}_{c'}$$ hat dieselbe Lösungsmenge.

und

$$ggT(a', b') = 1.$$

Wende nun Lemma 1 auf $a'x + b'y = c'$ an. □

4.)
$$[3^{80}]_{10} = [3]_{10}^{80} \underset{NR}{=} [3]_{10}^{[80]_4} = [3]_{10}^{[0]_4} = [1]_{10}$$

NR: in Monoid $(\mathbb{Z}/10\mathbb{Z}, *)$ generiert $[3]_{10}$:

$([1]_{10}, [3]_{10}, [9]_{10}, [7]_{10})$

$[27]_{10} \dashrightarrow [21]_{10} = [1]_{10}$

d.h. $ord([3]_{10}) = 4$

Im Allgemeinen zur Berechnung von der letzten Ziffer von a^b, $a, b \in \mathbb{N}_{\geq 1}$:

$$[a^b]_{10} = [a]_{10}^{[b]_{ord([a]_{10})} \text{ in } \mathbb{Z}/10\mathbb{Z}}$$ falls $ord([a]_{10})$ existiert

Beispiele:

- 7^{65}: $ord([7]_{10}) = 4$, $[65]_4 = 1$

  $1, 7, 9, 3, 1$ (49) (63) (21)

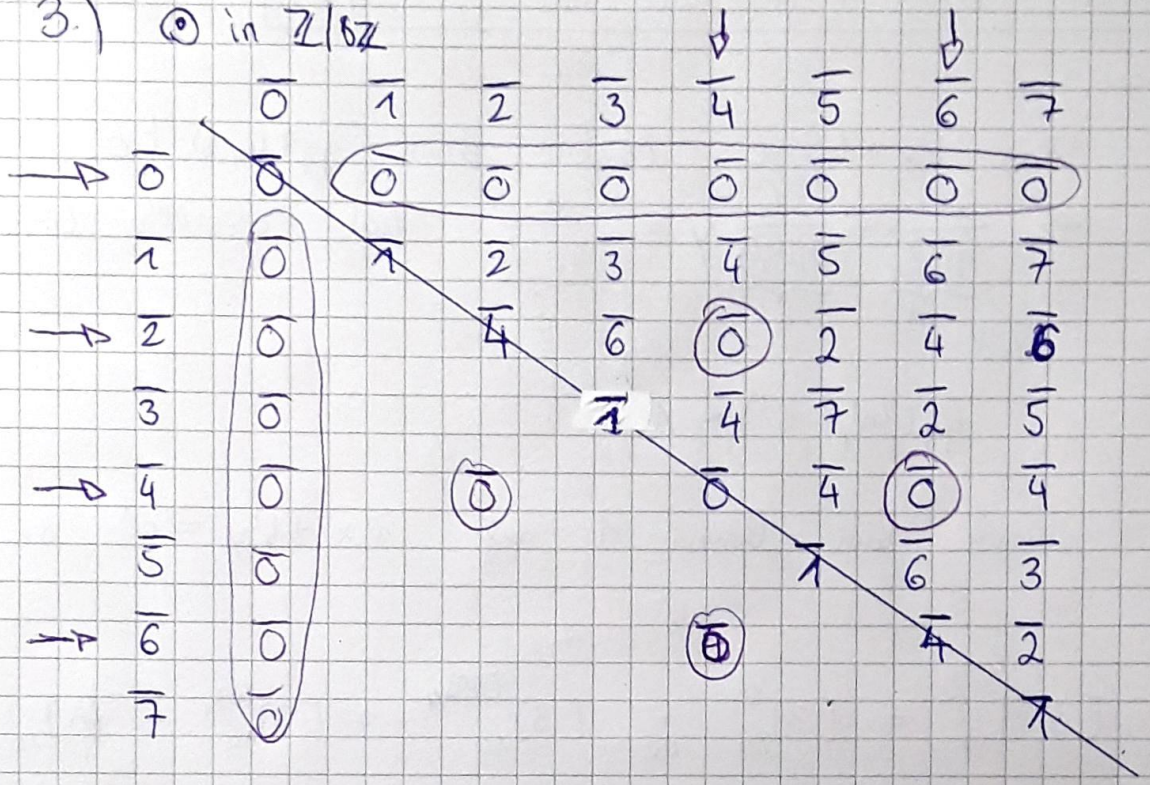
  $\Rightarrow [7^{65}]_{10} = [7]_{10}^{1} = [7]_{10}$

- 9^{33}: $ord([9]_{10}) = 2$, $[33]_2 = 1$

  $1, 9, 1$ (81)

  $\Rightarrow [9^{33}]_{10} = [9]_{10}^{1} = [9]_{10}$

3) ⊙ in $\mathbb{Z}/8\mathbb{Z}$



$\mathbb{Z}/N\mathbb{Z}$ kommutativer Ring → Multiplikationstafel symmetrisch

Zero Divisors: $\{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$, i.e. all numbers $0 \leq i < 8$ that are not coprime to 8

(In this lecture, $\bar{0}$ apparently is not considered a zero divisor, so please ignore it above.)