

**Aufgabe 1.**

- a) Für  $a = 868318803$  und  $b = 1601135481$  gilt  $\gcd(a, b) = 3531$ ,  $u = -104598$  und  $v = 56725$ .  
Für  $a = 911761172$  und  $b = 573241334$  gilt  $\gcd(a, b) = 958$ ,  $u = -146941$  und  $v = 233715$ .

**Aufgabe 2.**

- a) Alle  $x \in [6]_{\equiv 13}$ , bzw. alle  $x \in \{13y + 6 : y \in \mathbb{Z}\}$ .  
b) Alle  $x \in [3]_{\equiv 12}$ , bzw. alle  $x \in \{12y + 3 : y \in \mathbb{Z}\}$   
c) Es gibt keine derartigen  $x$ .  
d) Alle  $x \in [4]_{\equiv 12}$ , bzw. alle  $x \in \{12y + 4 : y \in \mathbb{Z}\}$

**Aufgabe 3.** Behauptet ist

$$\exists [y]_{\equiv m} \in \mathbb{Z}_m : [x]_{\equiv m} \cdot [y]_{\equiv m} = [1]_{\equiv m} \iff \gcd(x, m) = 1.$$

„ $\Rightarrow$ “ Angenommen es gibt ein solches  $[y]_{\equiv m}$ . Es gilt also  $xy \equiv_m 1$  beziehungsweise  $\text{mod}(xy, m) = \text{mod}(1, m)$ , woraus folgt  $\text{mod}(xy, m) = 1$  nachdem  $\text{mod}(1, m) = 1 - m \lfloor 1/m \rfloor = 1 - m \cdot 0 = 1$ . (Nachdem  $m \geq 2$  gilt für alle  $m$ , dass  $\lfloor 1/m \rfloor = 0$ .) Weiters gilt  $\gcd(xy, m) = 1$  nachdem

$$\begin{aligned} \{g, g'\} &= \{xy, m\} \\ \{g, g'\} &= \{m, \text{mod}(xy, m)\} \\ \{g, g'\} &= \{1, \text{mod}(m, 1)\} \\ \{g, g'\} &= \{1, 0\}, \end{aligned}$$

wobei der Algorithmus bei  $g' = 0$  mit  $\gcd(xy, m) = g = 1$  terminiert. (Nachdem  $m \in \mathbb{N}$  gilt für alle  $m$ , dass  $\lfloor m/1 \rfloor = m$  und ergo  $\text{mod}(m, 1) = 0$ .)

Die Primfaktorzerlegungen von  $xy = \chi_1 \chi_2 \dots \chi_i$  und  $m = m_1 m_2 \dots m_j$  sind nun also voneinander verschieden (haben eine leere Schnittmenge). Das Produkt  $xy$  kann weiter in die Primfaktoren von  $x$  und  $y$ , also  $xy = x_1 x_2 \dots x_k y_1 y_2 \dots y_l$  zerlegt werden. Nachdem die Primfaktoren von  $xy$  und  $m$  voneinander verschieden sind, müssen auch die Primfaktoren von  $x$  und  $m$  (und  $y$  und  $m$ ) voneinander verschieden sein. Demzufolge gilt  $\gcd(x, m) = 1$  (und  $\gcd(y, m) = 1$ ), was zu zeigen war.

„ $\Leftarrow$ “ Angenommen es gilt  $\gcd(x, m) = 1$ . Zu zeigen ist, dass es ein  $[y]_m \in \mathbb{Z}$  gibt mit  $xy \equiv_m 1$  beziehungsweise  $\text{mod}(xy, m) = 1$ .

Nachdem  $\gcd(x, m) = 1$  gibt es  $y, v \in \mathbb{Z}$  mit  $yx + vm = 1$ . Dann gilt

$$[1]_{\equiv m} = [y]_{\equiv m} [x]_{\equiv m} + \underbrace{[vm]_{\equiv m}}_{=[0]_{\equiv m}} = [y]_{\equiv m} [x]_{\equiv m},$$

woraus folgt, dass  $[y]_{\equiv m}$  das gesuchte multiplikative Inverse von  $[x]_{\equiv m}$  ist, wie zu zeigen war.