Aufgaben: Die ganzen Zahlen

1. Bestimme zwei ganze Zahlen x, y sodass $223x + 157y = 1$ gilt.

   Lösung:

   Wir wenden den Euklidischen Algorithmus an. Wir finden sukzessive

   $$\begin{aligned} 223 &= 157 + 66, \\ 157 &= 2 \cdot 66 + 25, \\ 66 &= 2 \cdot 25 + 16, \\ 25 &= 16 + 9, \\ 16 &= 9 + 7, \\ 9 &= 7 + 2, \\ 7 &= 3 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

   Durch Rückwärtseinsetzen erhalten wir

   $$\begin{aligned} 1 &= 7 - 3 \cdot 2, \\ &= 7 - 3 \cdot (9 - 7) = 4 \cdot 7 - 3 \cdot 9, \\ &= 4 \cdot (16 - 9) - 3 \cdot 9 = 4 \cdot 16 - 7 \cdot 9, \\ &= 4 \cdot 16 - 7 \cdot (25 - 16) = 11 \cdot 16 - 7 \cdot 25, \\ &= 11 \cdot (66 - 2 \cdot 25) - 7 \cdot 25 = 11 \cdot 66 - 29 \cdot 25, \\ &= 11 \cdot 66 - 29 \cdot (157 - 2 \cdot 66) = 69 \cdot 66 - 29 \cdot 157, \\ &= 69 \cdot (223 - 157) - 29 \cdot 157, \\ &= 69 \cdot 223 + (-98) \cdot 157. \end{aligned}$$

   Da 223 und 157 teilerfremd sind lässt sich leicht zeigen, dass nun *alle* Lösungen der Form $(x, y) = (69 + 157k, -98 - 223k)$ mit $k \in \mathbb{Z}$ sind.

2. Sei $0 \neq c \in \mathbb{Z}$ eine ganze Zahl und $a \in \mathbb{Z}$ eine weitere ganze Zahl. Zeige, dass a ein multiplikatives Inverses modulo c besitzt genau dann, wenn a und c teilerfremd sind. Ferner zeige, dass jenes multiplikative Inverse eindeutig modulo c bestimmt ist und jene Kongruenzklasse nur von der Kongruenzklasse von a modulo c abhängt.

   Lösung:

   Falls a und c teilerfremd sind, so gibt es nach dem Satz von Bézout zwei ganze Zahlen $x, y \in \mathbb{Z}$, sodass $ax + yc = 1$. Es folgt, dass $ax \equiv 1 \mod (c)$. Insbesondere ist x ein Multiplikatives Invereses von a modulo c. Umgekehrt, sei x ein Mutliplikatives Inverses von a modulo c. So gilt $ax \equiv 1 \mod (c)$, d.h. wir können ein $y \in \mathbb{Z}$ finden, sodass $ax + yc = 1$. Falls nun d ein gemeinsamer Teiler von a und c ist, gilt auch $d \mid ax + yc = 1$. Es folgt, dass 1 ein grösster gemeinsamer Teiler von a und c ist, d.h. a und c sind teilerfremd.

   Sei nun a und c teilerfremd und x, x' zwei Multiplikative Inverse von a modulo c. Dann gilt

   $$ax \equiv 1 \equiv ax' \mod (c) \quad \Rightarrow \quad c \mid a(x - x').$$

   Da a und c teilerfremd sind gilt nach einem Lemma der Vorlesung sogar $c \mid x - x' \Leftrightarrow x \equiv x' \mod (c)$.

Seien a und c teilerfremd und $[x]_c$ die Kongruenzklasse von multiplikativen Inversen von a modulo c. Sei a' eine weitere ganze zu c teilerfremde Zahl und $[x']_c$ die Kongruenzklasse von multiplikativen Inversen von a' modulo c. Es gilt zu zeigen, dass falls $a \equiv a' \mod (c)$, dann ist $[x]_c = [x']_c$. Wir finden, dass

$$a'x \equiv ax \equiv 1,$$

das heisst, dass x auch ein Multiplikatives Inverses von a' modulo c ist. Das heisst $x \in [x']_c$, aber dies ist gerade äquivalent zu $[x]_c = [x']_c$.

3. Bestimme die Ordnung von 3 modulo 13.

Lösung:

Wir finden der Reihe nach $3^2 \equiv 9 \equiv -4 \mod (13)$, $3^3 \equiv -12 \equiv 1 \mod (13)$. Das heisst 3 ist die Multiplikative Ordnung von 3 modulo 13.