Einführung i. d. Kryptopgraphie - Übung 4

12.11.2024

Aufgabe 1

Zeigen Sie das $11^{49} + 4^{49}$ durch 15 teilbar ist (ohne Taschenrechner).

$\varphi(15) = 8$, wir wissen also, dass alle Exponenten die ein Vielfaches von 8 sind in der Modulo Division 1 ergeben. Sie bilden ein Multiplikatives Inverses.

$$\begin{aligned} 11 &\equiv -4 \mod 15 \\ 11^{49} + 4^{49} &\mod 15 = 0 \\ = 11^{48} \cdot 11 + 4^{48} \cdot 4 &\mod 15 = 0 \\ = 11 + 4 &\mod 15 = 0 \\ = -4 + 4 &\mod 15 = 0 \\ = 0 &\mod 15 = 0 \end{aligned}$$

Aufgabe 2

Zeigen Sie an einem Beispiel, dass die Kürzungsregel in der Halbgruppe $(Z/mZ, \cdot)$ im allgemeinen nicht gilt

$$\begin{aligned} a \cdot b &= a \cdot c \\ b \cdot a &= c \cdot a \\ a^{-1} \cdot a \cdot b &= a^{-1} \cdot a \cdot c \\ &= e \cdot b = e \cdot c \end{aligned}$$

Dies impliziert jeweils $b = c$.

$$\begin{aligned} ab &= ac \\ &= ab - ac = 0 \\ &= a(b - c) = 0 \end{aligned}$$

Beispiel $(Z/10Z, \cdot =$:

$$3 \cdot 7 \cdot x = 3 \cdot 7 \cdot y \mod 10$$
$$1 \cdot x = 1 \cdot y \mod 10$$

$$2 \cdot x = 2 \cdot y \mod 10$$