Arbeitsblatt: Modulares Potenzieren

Für das Modulo-Rechnen gelten u.a. die folgenden Rechenregeln:

$$\begin{aligned}(a \cdot b) \bmod m &= (a \bmod m \cdot b \bmod m) \bmod m \\ (a^b) \bmod m &= (a \bmod m)^b \bmod m\end{aligned}$$

Aufgaben:

1. Versuche in Worte zu fassen, welche Ansätze bei den folgenden Rechenbeispielen verwendet werden, um $7^4 \bmod 12$ und $82^{17} \bmod 20$ zu berechnen.

$$\begin{aligned}7^4 \bmod 12 &= 7^2 \cdot 7^2 \bmod 12 \\ &= 49 \cdot 49 \bmod 12 \\ &= (49 \bmod 12 \cdot 49 \bmod 12) \bmod 12 \\ &= (1 \cdot 1) \bmod 12 \\ &= 1 \bmod 12 \\ &= 1\end{aligned}$$

$$\begin{aligned}82^{17} \bmod 20 &= 2^{17} \bmod 20 \\ &= 2^{16} \cdot 2^1 \bmod 20 = (2^4)^4 \cdot 2 \bmod 20 \\ &= 16^4 \cdot 2 \bmod 20 = (-4)^4 \cdot 2 \bmod 20 \\ &= (-4)^2 \cdot (-4)^2 \cdot 2 \bmod 20 \\ &= 16^2 \cdot 2 \bmod 20 \\ &= (-4)^2 \cdot 2 \bmod 20 = 16 \cdot 2 \bmod 20 \\ &= 32 \bmod 20 \\ &= 12\end{aligned}$$

2. Berechne

   (a) $8^9 \bmod 7$

   (b) $6^9 \bmod 7$

   (c) $54^{16} \bmod 55$

   (d) $3^{333} \bmod 26$ (Tip: Benutze $3^3 \bmod 26 = 27 \bmod 26 = 1 \bmod 26 = 1$)

   (e) $2^{268} \bmod 17$ (Tip: Benutze $2^4 \bmod 17 = 16 \bmod 17 = (-1) \bmod 17$)

   (f) $2^{269} \bmod 17$ (Tip: Verwende das Ergebnis von (e) oder benutze, dass $2^4 \bmod 17 = 16 \bmod 17 = (-1) \bmod 17$)

   (g) $2^{270} \bmod 19$ (Tip: Benutze, dass $2^9 \bmod 19 = -1 \bmod 19$.)

   (h) $2^{271} \bmod 19$ (Tip: Verwende das Ergebnis von (g) oder benutze, dass $2^9 \bmod 19 = -1 \bmod 19$.

   (i) $3^{333} \bmod 15$
   Tip: Zeige zunächst, dass $3^4 \bmod 15 = 6 \bmod 15$, und nutze außerdem, dass $6^k \bmod 15 = 6$ ist.