FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
18.10.2023

Musterlösung zum 3. Übungsblatt zur Vorlesung Kryptologie

Übung 1

d) ist richtig, der Rest ist falsch.

Übung 2

Nein. Sei $n = \lceil \mathrm{ld}\ p \rceil$ die Anzahl an Binärstellen von p, also $p \approx 2^n$. Dann ist der Aufwand an Operationen in der Größenordnung von $p = 2^n$, also (bezüglich der Problemgröße „Stellenanzahl“) von exponentieller Komplexität.

Übung 3

Der Algorithmus liefert tatsächlich das Richtige, allerdings ist seine Laufzeit exponentiell:

Der Algorithmus braucht $\lfloor a/m \rfloor$ viele Schleifendurchläufe, bei $a \approx 2^k$ und $m \approx 2^l$ also ungefähr $2^k/2^l = 2^{k-l}$ Durchläufe. Wenn a beispielsweise doppelt so viele Stellen hat wie m, also $k = 2l$, ergeben sich $2^{2l-l} = 2^l$ Durchläufe.

Übung 4

Ja, denn da B polynomial ist, gibt es ein k, so dass B bei einer Eingabe der Größe n eine Laufzeit $\approx n^k$ hat. A ruft B polynomial oft auf, also $\approx n^l$ mal (mit einem festen l). Die Gesamtlaufzeit ist dann $\approx n^l \cdot n^k = n^{k+l}$, also wieder polynomial.

Übung 5

a) Modulo 9 gilt:

$$\begin{aligned}
& 5^2 = 7 \\
\Rightarrow\ & 5^4 = 7^2 = 49 = 4 \\
\Rightarrow\ & 5^8 = 4^2 = 16 = 7 \\
\Rightarrow\ & 5^{16} = 7^2 = 49 = 4 \\
\Rightarrow\ & 5^{32} = 4^2 = 16 = 7
\end{aligned}$$

b) Modulo 18 gilt:

$$\begin{aligned} & 11^2 = 13 = -5 \\ \Rightarrow\ & 11^4 = (-5)^2 = 25 = 7 \\ \Rightarrow\ & 11^8 = 7^2 = 49 = 13 \\ \Rightarrow\ & 11^{16} = 13^2 = 7 \end{aligned}$$

$$\Rightarrow\ 11^{27} = 11^{16} \cdot 11^8 \cdot 11^2 \cdot 11 = 7 \cdot 13 \cdot 13 \cdot 11 = 7 \cdot 7 \cdot 11 = (-5) \cdot (-7) = 17$$

c) Modulo 11 gilt:

$$\begin{aligned} & 8^2 = 64 = -2 \\ \Rightarrow\ & 8^4 = (-2)^2 = 4 \\ \Rightarrow\ & 8^8 = 4^2 = 16 = 5 \\ \Rightarrow\ & 8^{16} = 5^2 = 25 = 3 \\ \Rightarrow\ & 8^{32} = 3^2 = 9 = -2 \\ \Rightarrow\ & 8^{64} = (-2)^2 = 4 \end{aligned}$$

$$\Rightarrow\ 8^{120} = 8^{64} \cdot 8^{32} \cdot 8^{16} \cdot 8^8 = 4 \cdot (-2) \cdot 3 \cdot 5 = -8 \cdot 4 = 3 \cdot 4 = 1.$$

Wenn man weiß, dass $(\mathbb{Z}_{11} \setminus \{0\}, \odot)$ eine Gruppe ist (da 11 eine Primzahl ist), gilt nach Satz 1.3: $8^{10} = 1 \bmod 11$, also

$$8^{120} = (8^{10})^{12} = 1^{12} = 1.$$

d) Modulo 13 gilt:

$$\begin{aligned} & 7^2 = 49 = 10 \\ \Rightarrow\ & 7^4 = 10^2 = 100 = 9 = -4 \\ \Rightarrow\ & 7^8 = (-4)^2 = 16 = 3 \\ \Rightarrow\ & 7^{16} = 3^2 = 9. \end{aligned}$$

Wenn man weiß, dass $(\mathbb{Z}_{13} \setminus \{0\}, \odot)$ eine Gruppe ist (da 13 eine Primzahl ist), gilt nach Satz 1.3: $7^{12} = 1 \bmod 13$, also

$$7^{16} = 7^{12} \cdot 7^4 = 1 \cdot 7^4 = 9.$$