Rasmus Diederichsen
Lisa Goerke
Sebastian Höffner
Sven Kleine-Albers
Kristin Schmidt

# Lösungen zu Übungsblatt 6
# Kryptographische Verfahren

Besprechung 11. Dezember 2015

## Aufgabe 6.1. Exponentiation von Hand

### a)

$$
\begin{aligned}
\left[3^{1000}\right]_{100} &= \left[3^{512+256+128+64+32+8}\right]_{100} \\
&= \left[\left[\left[\left[\left[\left[3^{512}\right]_{100} \cdot 3^{256}\right]_{100} \cdot 3^{128}\right]_{100} \cdot 3^{64}\right]_{100} \cdot 3^{32}\right]_{100} \cdot 3^{8}\right]_{100} \\
&= \left[\left[\left[\left[[41 \cdot 21]_{100} \cdot 61\right]_{100} \cdot 81\right]_{100} \cdot 41\right]_{100} \cdot 61\right]_{100} \\
&= \left[\left[\left[[1 \cdot 61]_{100} \cdot 81\right]_{100} \cdot 41\right]_{100} \cdot 61\right]_{100} \\
&= \left[\left[[61 \cdot 81]_{100} \cdot 41\right]_{100} \cdot 61\right]_{100} \\
&= \left[[41 \cdot 41]_{100} \cdot 61\right]_{100} \\
&= [81 \cdot 61]_{100} \\
&= 41
\end{aligned}
$$

**Nebenrechnungen:**

$$
\begin{aligned}
\left[3^{1}\right]_{100} &= 3 \\
\left[3^{2}\right]_{100} &= 9 \\
\left[3^{4}\right]_{100} &= \left[3^{2+2}\right]_{100} = \left[\left[3^{2}\right]_{100} \cdot 3^{2}\right]_{100} = \left[9 \cdot 3^{2}\right]_{100} = 81 \\
\left[3^{8}\right]_{100} &= \left[3^{4+4}\right]_{100} = \left[81 \cdot 3^{4}\right]_{100} = [6561]_{100} = 61 \\
\left[3^{16}\right]_{100} &= \left[3^{8+8}\right]_{100} = [3721]_{100} = 21 \\
\left[3^{32}\right]_{100} &= [441]_{100} = 41 \\
\left[3^{64}\right]_{100} &= [1681]_{100} = 81 \\
\left[3^{128}\right]_{100} &= 61 \\
\left[3^{256}\right]_{100} &= 21 \\
\left[3^{512}\right]_{100} &= 41 \\
\left[3^{1024}\right]_{100} &= 81 \\
&\vdots
\end{aligned}
$$

Wir beobachten die Periode $81, 61, 21, 41, \ldots$, die wir uns zu Nutze machen können.

### b)

$$
\begin{aligned}
\left[101^{4800000002}\right]_{35} &= \left[\left[16^{6}\right]_{35} \cdot \left[11^{5}\right]_{35}\right]_{35} \\
&= \left[11^{5}\right]_{35} \\
&= 16
\end{aligned}
$$

**Nebenrechnungen:**

$$\begin{aligned}
\left[101^1\right]_{35} &= 31\\
\left[101^2\right]_{35} &= 16\\
\left[101^4\right]_{35} &= 11\\
\left[101^8\right]_{35} &= 16\\
\left[101^{16}\right]_{35} &= 11\\
&\vdots
\end{aligned}$$

Wir beobachten, dass jede zweite dieser Potenzen (also $2, 8, 32, \dots$) einen Rest von $16$ hat, alle anderen (mit Ausnahme von $1$) den Rest von $11$. Mit diesem Wissen können wir mit der Binärdarstellung und einfachem Zählen herausfinden, wie oft wir $11$ bzw. $16$ multiplizieren müssen, um auf das Ergebnis zu kommen:

$$4800000002_{10} = 100011110000110100011000000000010_2$$

Wir finden sechs Potenzen deren Rest $16$ ist und fünf Potenzen deren Rest $11$ ist. Es folgt:

$$\left[101^{4800000002}\right]_{35} = \left[\left[16^6\right]_{35} \cdot \left[11^5\right]_{35}\right]_{35}$$

Wir können nun zunächst $\left[16^6\right]_{35}$ geschickt berechnen:

$$\begin{aligned}
\left[16^6\right]_{35} &= \left[16^{2+2+2}\right]_{35}\\
&= [11 \cdot 11 \cdot 11]_{35}\\
&= 1
\end{aligned}$$

Wir stellen fest, dass wir diese Erkenntnis wiederum in unsere Gleichung einsetzen können und erhalten:

$$\begin{aligned}
\left[\left[16^6\right]_{35} \cdot \left[11^5\right]_{35}\right]_{35} &= \left[1 \cdot \left[11^5\right]_{35}\right]_{35}\\
&= \left[11^5\right]_{35}
\end{aligned}$$

Das können wir erneut geschickt berechnen:

$$\begin{aligned}
\left[11^5\right]_{35} &= \left[11^{4+1}\right]_{35}\\
&= [11 \cdot 11]_{35}\\
&= 16
\end{aligned}$$

*Nebenrechnung:*

$$\begin{aligned}
\left[11^1\right]_{35} &= 11\\
\left[11^2\right]_{35} &= 16\\
\left[11^4\right]_{35} &= 11
\end{aligned}$$

### Aufgabe 6.2. Erweiterter Euklidischer Algorithmus

**a)**

**b)**

**c)**

Wir zeigen zunächst Folgendes:

**Theorem 1.** *Falls* $a = \lfloor \frac{a}{b} \rfloor + [a]_b = qb + r$, *dann ist* $ggt(a, b) = ggt(b, r)$

*Beweis.* Sei $d = ggT(a, b)$, also gilt

$$a = dn$$
$$b = dm$$

Und daher

$$a - b = dn - dm = d(n - m) = dl$$

Also is $d$ Teiler von $a$ sowie von $a - b$. Alle gemeinsamen Teiler von $a$ und $b$ sind also Teiler von $a - b$. Deshalb gilt

$$b = a - (a - b) = dn - dl = d(n - l) = dk$$

und alle gemeinsamen Teiler von $a$ und $a - b$ sind Teiler von $b$. Die wiederholte Subtraktion von $b$ von $a$ ändert also nichts an den gemeinsamen Teilern. Es folgt $ggT(a, b) = ggT(b, a) = ggT(b, a - b) = ggT(b, a - b - b) = \ldots = ggT(b, a - qb) = ggT(b, r)$. □

Es folgt also aus der zu zeigenden Aussage

$$\begin{aligned}
ggT(b, r) = xb + yr = ggT(a, b) &= ya + xb - qyb \\
yr &= ya - yqb \\
y[a]_b &= ya - yqb \\
&= ya - y\left\lfloor \frac{a}{b} \right\rfloor b \\
&= ya - y(a - [a]_b) \\
&= ya - ya + y[a]_b \\
&= y[a]_b
\end{aligned}$$

Da aus der Aussage eine Tautologie folgt, muss sie stimmen.

### Aufgabe 6.3. Merkle-Hellmann-Verfahren

**a)**

Um $w^{-1}$ zu bestimmen, muss eEuklid mit $385$ und $17$ durchgeführt werden. Das Ergebnis ist dann $(d, x, y) = (1, -3, 68)$. Wir überprüfen, ob es sich bei $68$ tatsächlich um das multiplikative Inverse von $17$ in $\mathbb{Z}^*_{385}$ handelt.

$$[17 \cdot 68]_{385} = [1156]_{385} = 1$$

**b)**

$\mathfrak{b} = (289, 6, 12, 97, 24, 194, 48, 3)$

$$\begin{aligned}
\mathsf{Enc}_{\mathfrak{b},m}(x) &= [< \mathfrak{b}, x >]_m \\
&= [< (289, 6, 12, 97, 24, 194, 48, 3), (1, 0, 1, 1, 1, 0, 1, 1) >]_{385} \\
&= [(289, 0, 12, 97, 24, 0, 48, 3)]_{385} \\
&= (289, 0, 12, 97, 24, 0, 48, 3)
\end{aligned}$$

**c)**