S. Wewers, S. Wilke

Kryptographie, SS 06

Lösung 3

Aufgabe 1.

(a) Nach Aufgabe 1.) auf Blatt 1 ist. $\mathrm{ggT}(291, 201) = 3$. Damit existiert $\overline{201}^{-1}$ nicht in $\mathbb{Z}/291\mathbb{Z}$

(b) Ebenfall nach Aufgabe 1.) ist $3 = -29 \cdot 291 + 42 \cdot 201$, und damit folgt $1 = -29 \cdot 97 + 42 \cdot 67$. Damit ist $\overline{67}^{-1} = \overline{42} \in \mathbb{Z}/97\mathbb{Z}$.

(c) Zunächst ist $\mathrm{ggT}(7, 499) = \mathrm{ggT}(7, 499 \bmod 7) = \mathrm{ggT}(7, 2) = 1$. Damit existiert $\overline{7}^{-1} \in \mathbb{Z}/499\mathbb{Z}$. Damit ist aber $\overline{7}^{-1} \cdot \overline{42} = \overline{7}^{-1} \cdot \overline{7} \cdot \overline{6} = \overline{6} \in \mathbb{Z}/499\mathbb{Z}$. Alternativ kann man natürlich wiederum den erweiterten euklidischen Algorithmus anwenden; man erhält $1 = 214 \cdot 7 - 3 \cdot 499$. Damit ist $\overline{7}^{-1} = \overline{214}$ und somit $\overline{7}^{-1} \cdot \overline{42} = \overline{214} \cdot \overline{42} = \overline{8988} = \overline{6} \in \mathbb{Z}/499\mathbb{Z}$

Aufgabe 2. Zunächst gilt:

$$n^{13} - n = n(n^{12} - 1) = n(n-1)R_1 = (n^2 - n)R_1$$

nach Aufgabe 3.) Blatt 2. Nach dem kleinen Satz von Fermat gilt nun $n^p - n \equiv 0 \pmod p$ für alle Primzahlen p. Damit gilt insbesondere $n^{13} - n \equiv 0 \pmod 2$. Analog folgt nun:

$$\begin{aligned} n^{13} - n &= n((n^2)^6 - 1) = n(n^2 - 1)R_2 = (n^3 - n)R_2 \equiv 0 \pmod 3 \\ &= n((n^4)^3 - 1) = n(n^4 - 1)R_3 = (n^5 - n)R_3 \equiv 0 \pmod 5 \\ &= n((n^6)^2 - 1) = n(n^6 - 1)R_4 = (n^7 - n)R_4 \equiv 0 \pmod 7. \end{aligned}$$

Insgesamt gilt also $2, 3, 5, 7 \mid n^{13} - n$ und damit auch $210 = 2 \cdot 3 \cdot 5 \cdot 7 \mid n^{13} - n$.

Aufgabe 3.
Wir benutzen den Satz von Euler: Falls $\mathrm{ggT}(a, n) = 1$, so gilt $a^{\phi(n)} \equiv 1 \pmod n$. Insbesondere ist $a^k \equiv a^{k \bmod \phi(n)} \pmod n$.

(a) Gesucht: $2^{292} \bmod 100$.
Betrachte zunächst $2^{292} \bmod 25$. Es gilt: $\phi(25) = \phi(5^2) = 5 \cdot 4 = 20$. Damit ist zunächst $2^{292} \equiv 2^{12} \pmod{25}$. Weiter ist $2^{10} = 1024 \equiv -1 \pmod{25}$, und damit gilt $2^{12} \equiv -1 \cdot 2^2 \equiv -4 \pmod{25}$. Also gilt: $2^{292} \equiv 21, 46, 71$ oder $96 \pmod{100}$ Wegen $4 \mid 2^{292}$ bleibt damit nur noch $2^{292} \equiv 96 \pmod{100}$ übrig; also sind die letzten beiden Ziffern: 96.

(b) Gesucht: $7^{(7^{100000})} \bmod 1000$.
Zunächst gilt: $\phi(1000) = \phi(125) \cdot \phi(8) = (25 \cdot 4) \cdot 4 = 400$. Wegen

ggT$(7, 1000) = 1$ gilt damit: $7^{(7^{100000})} \equiv 7^{(7^{100000} \pmod{400})} \pmod{1000}$. Weiter gilt nun: $\phi(400) = \phi(16) \cdot \phi(25) = 8 \cdot 20 = 160$. Wegen ggT$(7, 400) = 1$ und $100000 = 160 \cdot 625$ gilt somit $7^{100000} \equiv 1 \pmod{400}$. Insgesamt gilt nun: $7^{(7^{100000})} \equiv 7^1 = 7 \pmod{1000}$. Also sind die letzten drei Ziffern: 007.

Aufgabe 4.

(a) Wegen ord$(a) \mid \phi(17) = 16$ kommen für ord(a) nur Zweierpotenzen; also die Zahlen $1, 2, 4, 8, 16$ in Frage.
Wir testen zunächst die Zahl 2: Es ist $2^4 \equiv 16 \equiv -1 \pmod{17}$ und damit $2^8 \equiv 1 \pmod{17}$. Damit ist 2 keine Primitivwurzel mod17.
Testen wir die Zahl 3: Es ist $3^2 = 9 \equiv -8 \pmod{17}$. Damit ist $3^4 \equiv 64 \equiv -4 \pmod{17}$. Daraus folgt wiederum $3^8 \equiv 16 \equiv -1 \pmod{17}$. Damit folgt ord$(3) = 16$, und 3 ist Primitivwurzel mod17.

(b) Wir berechnen die fehlenden Potenzen. Es ist

$$
\begin{aligned}
3^1 &\equiv 3 && \pmod{17}\\
3^2 &\equiv 9 \equiv -8 && \pmod{17}\\
3^3 &\equiv 3 \cdot 3^2 \equiv 3 \cdot (-8) \equiv -24 \equiv -7 \equiv 10 && \pmod{17}\\
3^4 &\equiv -4 \equiv 12 && \pmod{17}\\
3^5 &\equiv 3 \cdot 3^4 \equiv -4 \cdot 3 \equiv -12 \equiv 5 && \pmod{17}\\
3^6 &\equiv 3 \cdot 3^5 \equiv 5 \cdot 3 \equiv 15 \equiv -2 && \pmod{17}\\
3^7 &\equiv 3 \cdot 3^6 \equiv -2 \cdot 3 \equiv -6 \equiv 11 && \pmod{17}
\end{aligned}
$$

Damit ist $3^x \equiv 11 \pmod{17}$ für $x = 7$ erfüllt.

Aufgabe 5.

(a) Für welche $n \in \mathbb{N}$ gilt: $\phi(n) = \phi(2n)$?
Wir schreiben $n = 2^a \cdot m$ mit m ungerade. Dann ist $2n = 2^{a+1} \cdot m$, und daraus folgt $\phi(2n) = 2^a \cdot \phi(m)$. Für $a > 0$ ist $\phi(n) = 2^{a-1} \cdot \phi(m)$, also $\phi(2n) \neq \phi(n)$. Für $a = 0$ hingegen ist $\phi(n) = \phi(m) = \phi(2n)$. Also gilt $\phi(2n) = \phi(n)$ genau dann, wenn $a = 0$, m.a.W. wenn n ungerade ist.

(b) Gibt es ein $n \in \mathbb{N}$ mit $\phi(n) = 14$?
Wir schreiben $n = \prod_{p|n} p^{\alpha(p)}$. Dann ist $\phi(n) = \prod_{p|n} (p^{\alpha(p)-1} \cdot (p-1))$. Insbesondere gilt $p - 1 \mid \phi(n)$, falls $p \mid n$. Annahme: Es existiert ein $n \in \mathbb{N}$ mit $\phi(n) = 14$. Falls $p \mid n$, so gilt also: $p - 1 \mid 14 = 2 \cdot 7$. Damit folgt $p = 2$ oder $p = 3$. Dann hat also n die Form $n = 2^\alpha \cdot 3^\beta$, und damit folgt: $\phi(n) = \phi(2^\alpha) \cdot \phi(3^\beta)$. Wegen $7 \mid \phi(n)$ und $7 \nmid \phi(2^\alpha)$ folgt $7 \mid \phi(3^\beta)$; also insbesondere $\beta > 0$. Es ist aber $\phi(3^\beta) = 2 \cdot 3^{\beta-1}$, und das ist ein Widerspruch. Somit gibt es kein $n \in \mathbb{N}$ mit $\phi(n) = 14$.