

1. [1], Exercise 4.10) Berechnen Sie $\varphi(999)$.

$$\text{Lösung } \varphi(999) = 999 \cdot (1 - 1/3) \cdot (1 - 1/37) = 648.$$

2. RSA-Verschlüsselung: Der Modulus sei $N = 11 \cdot 17 = 187$. Die Botschaft x werde mit dem öffentlichen Exponenten $e = 107$ zu $y = x^e \bmod 187 = 101$ verschlüsselt und übermittelt. Wie lautet die Botschaft x in "Klartext"?

Lösung Es ist $\varphi(187) = 10 \cdot 16 = 160$ (Euler'sche φ -Funktion) und der geheime Exponent d ist das 160-modulare Inverse von e . Dieses kann man mit Hilfe des erweiterten euklidischen Algorithmus bestimmen, indem man pro forma den ggT von $e = 107$ und $\varphi(187) = 160$ berechnet und in geeigneter Form darstellt. Es ist

$$\begin{bmatrix} 107 \\ 53 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 160 \\ 107 \end{bmatrix}, \quad \begin{bmatrix} 53 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 107 \\ 53 \end{bmatrix}, \quad \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -53 \end{bmatrix} \begin{bmatrix} 53 \\ 1 \end{bmatrix}.$$

Das Produkt der drei Matrizen (Reihenfolge!) ist

$$\begin{bmatrix} 0 & 1 \\ 1 & -53 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ * & * \end{bmatrix}.$$

Aus

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} -2 & 3 \\ * & * \end{bmatrix} \begin{bmatrix} 160 \\ 107 \end{bmatrix}$$

erhält man die Beziehung $1 = (-2) \cdot 160 + 3 \cdot 107$, der man entnimmt, dass 3 das 160-modulare Inverse von 107 ist, d.h. $d = 3$.

Die Botschaft y entschlüsselt man also, indem man sie mit $d = 3$ potenziert (modulo 187). Das kann man entweder direkt rechnen (Taschenrechner) oder in $\mathbf{Z}_{11} \times \mathbf{Z}_{17}$. In $\mathbf{Z}_{11} \times \mathbf{Z}_{17}$ hat y die Darstellung $(2, -1)$. Es ist $(2, -1)^3 = (8, -1) = (2, -1) + (6, 0)$. $(1, 0) \in \mathbf{Z}_{11} \times \mathbf{Z}_{17}$ stellt die Größe $34 \in \mathbf{Z}_{187}$ dar (dies sieht man entweder "so", oder man entnimmt es der Gleichung $1 = 2 \cdot 17 + (-3) \cdot 11$, die man ebenfalls mit dem erweiterten euklidischen Algorithmus erhält). Also steht $(8, -1)$ für die Größe $(6 \cdot 34 + 101) \bmod 187 = 305 \bmod 187 = 118$. Die Klartext-Botschaft lautet somit $x = 118$.

Literatur

- [1] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics*. Addison-Wesley, second edition, 1994.