Aufgabe 8.1 (4 Punkte)

Wieviele Lösungen hat die Gleichung $x^2 - 4x + 3 = 0$ in $\mathbb{Z}^*_{2520}$.

Aufgabe 8.2 (4 Punkte)

Sei $c = 266028$ eine von uns abgefangene Nachricht, die mit dem RSA-Verfahren verschlüsselt wurde. Welche Botschaft wurde übertragen, wenn der öffentliche Schlüssel $(N, e) = (282361, 78745)$ ist.

Aufgabe 8.3 (4 Punkte)

Finde die kleinste positive ganze Zahl x, die folgende simultane Kongruenz löst:

$$\begin{aligned} 3 \cdot x &\equiv 2 \,(\mathrm{mod}\, 8) \\ 4 \cdot x &\equiv 3 \,(\mathrm{mod}\, 5) \\ x &\equiv 7 \,(\mathrm{mod}\, 9) \end{aligned}$$

Aufgabe 8.4 (4 Punkte)

Wir betrachten einen Teil des Beweises zur Sicherheit von RSA (Folien `16_RSA`, Seiten 11+12), nämlich die Reduktion der Faktorisierung von N auf das Berechnen des privaten Schlüssels d aus (N, e). Dabei betrachten wir nur den Fall 1) auf Seite 12 des Skripts:

Sei $ed - 1 = 2^r t$ für $r \geq 2$ und ungerades t. Zeige, dass bei der zufälligen Wahl eines a aus $\mathbb{Z}^*_N$, die Wahrscheinlichkeit, dass $a^{2^k t} = 1 \pmod N$ für alle $0 \leq k < r$ höchstens $\frac{1}{2}$ beträgt.

Tipp: Zeige, dass $G = \{a \in \mathbb{Z}^*_N \mid a^t = 1\}$ eine nicht triviale Untergruppe in $\mathbb{Z}^*_N$ ist und betrachte den Index $[G : \mathbb{Z}^*_N]$ von G in $\mathbb{Z}^*_N$.

Präsenzaufgabe 8.5

Finde die kleinste natürliche Zahl x, so dass gilt:

$$x \equiv 4 \pmod 7, \qquad x \equiv 2 \pmod 9 \qquad \text{und} \qquad x \equiv 3 \pmod{11}$$

Präsenzaufgabe 8.6

Peter lädt zu einer Party ein und sendet deshalb 3 mal dieselbe Botschaft an Tanja, Max und Rike. Du hast keine Botschaft bekommen, aber alle drei Ciphertexte c_1, c_2 und c_3 mitgehört. Schnell findest Du die öffentlichen Schlüssel von Tanja $(N_1, 3)$, Max $(N_2, 3)$ und Rike $(N_3, 3)$.

Kannst Du die Botschaft von Peter im Klartext ermitteln?