Aufgabe 10.1 (2 Pkt.)

Bestimmen Sie mittels Quadratisches-Sieb-Methode und Faktorbasis $\mathcal{B} := \{2, 3, 5, 7, 11, 13\}$ einen nichttrivialen Faktor von $n := 15\,770\,708\,441$. Verwenden Sie dabei die „Zufallszahlen“

$$x_1 := 8\,340\,934\,156\,, \quad x_2 := 12\,044\,942\,944 \quad \text{und} \quad x_3 := 2\,773\,700\,011\,.$$

Geben Sie auch die Faktorisierungen der $x_i^2 \bmod n$ und von x und y an.

Hinweis: Die Zahlenwerte dürfen maschinell errechnet werden.

Aufgabe 10.2 (2+1 Pkt.)

Sei n eine ungerade Zahl mit Primfaktorzerlegung $n = \prod_{i=1}^{k} p_i^{e_i}$ (alle $e_i \geq 1$.)

a) Beweisen Sie: Jeder quadratische Rest aus $\mathbb{Z}_n^*$ besitzt 2^k Quadratwurzeln.

b) Ein Paar $(a, b) \in_{\mathrm{R}} \{(\alpha, \beta) \in \mathbb{Z}_n^* \times \mathbb{Z}_n^* \mid \alpha^2 \equiv \beta^2 \pmod{n}\}$ werde zufällig gewählt. Mit welcher Wahrscheinlichkeit ist $a \not\equiv \pm b \pmod{n}$?

Aufgabe 10.3 (2 Pkt.)

Faktorisieren Sie die Zahlen 1679 und 3589 mit dem Pollard-Rho-Algorithmus. Verwenden Sie dazu $x_{i+1} = x_i^2 + 1$ und wählen Sie für x_0 einmal 5 (bei $n = 1679$) und einmal 7 (bei $n = 3589$) aus. Tragen Sie Ihre Ergebnisse in eine Tabelle folgender Form ein:

i	$x_i \bmod n$	$x_{2i} \bmod n$	$\mathrm{ggT}(x_i - x_{2i}, n)$
1	x_1	x_2	n
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Aufgabe 10.4 (3 Pkt.)

a) Berechnen Sie den Wert des Jacobi-Symbols $\left(\frac{84}{97}\right)$ mit dem Algorithmus aus der Vorlesung. Geben Sie dabei alle Jacobi-Symbole an, die bei der Vereinfachung des Ausdrucks auftreten.

b) Sei $p > 3$ eine Primzahl. Zeigen Sie:

$$\left(\frac{+3}{p}\right) = \begin{cases} +1 & \text{falls } p \equiv \pm 1 \bmod 12 \\ -1 & \text{falls } p \equiv \pm 5 \bmod 12 \end{cases} \quad \text{und} \quad \left(\frac{-3}{p}\right) = \begin{cases} +1 & \text{falls } p \equiv +1 \pmod 6 \\ -1 & \text{falls } p \equiv -1 \pmod 6 \end{cases}.$$

Aufgabe 10.5 (2 Pkt.)

Finden Sie mit Pollards $(p-1)$-Algorithmus aus der Vorlesung einen nichttrivialen Faktor von $n = 4472$, einmal mit Basiszahl $a = 2$ und einmal mit Basiszahl $a = 6$. Geben Sie in jeder Iteration die Werte von B, a und g an.

Aufgabe 10.6 (4 Pkt.)

Lösen Sie die SPOX-Aufgabe „Diskreter Logarithmus“.