5.2 Quadratwurzeln und Faktorisierung

Satz 2 (M. RABIN) *Sei $n = pq$ mit verschiedenen Primzahlen $p, q \geq 3$. Dann ist die Faktorisierung von n probabilistisch effizient auf das Problem des Quadratwurzelziehens* mod n *reduzierbar.*

Beweis. Es gibt vier Einheitswurzeln in $\mathbb{Z}/n\mathbb{Z}$, also auch zu jedem Quadrat in $\mathbb{M}_n$ vier Quadratwurzeln.

Wählt man nun $x \in M_n$ zufällig, so liefert der Quadratwurzel-Algorithmus eine Wurzel $y \in \mathbb{M}_n$ von x^2, also

$$y^2 \equiv x^2 \pmod{n}.$$

Mit Wahrscheinlichkeit $\frac{1}{2}$ ist $y \not\equiv \pm x \pmod{n}$. Da

$$n \mid (x^2 - y^2) = (x+y)(x-y), \quad n \nmid (x \pm y),$$

ist $\mathrm{ggT}(n, x+y)$ echter Teiler von n. (Alternativ: $y/x \bmod n$ ist nichttriviale Einheitswurzel.) $\diamond$

D. h., wer Quadratwurzeln mod n ziehen kann, kann auch n faktorisieren. Die Umkehrung folgt in Abschnit 5.5.