

## 5.5 Quadratwurzeln bei zusammengesetzten Moduln

Ist die Primzerlegung eines Moduls  $n$  bekannt, so lassen sich in  $\mathbb{M}_n$  effizient Quadratwurzeln ziehen; die Probleme „Faktorisierung“ und „Ziehen von Quadratwurzeln“ sind also in ihrer Komplexität äquivalent.

Zur Durchführung wird  $n$  sukzessive in teilerfremde Faktoren zerlegt (bis hinunter zu den Primpotenzen).

Sei also  $n = rs$  mit teilerfremden Faktoren  $r$  und  $s$ . Zuerst werden mit dem erweiterten Euklidischen Algorithmus Koeffizienten  $a$  und  $b$  mit  $ar + bs = 1$  bestimmt. Aus  $z$  soll die Quadratwurzel gezogen werden. Sei  $u$  die Quadratwurzel mod  $r$  und  $v$  die Quadratwurzel mod  $s$ . Dann erfüllt  $x = arv + bsu$  mod  $n$ :

$$\begin{aligned} x &\equiv bsu \equiv u \pmod{r}, & x &\equiv arv \equiv v \pmod{s}, \\ x^2 &\equiv u^2 \equiv z \pmod{r}, & x^2 &\equiv v^2 \equiv z \pmod{s}, \end{aligned}$$

insbesondere ist  $x^2 \equiv z \pmod{n}$ .

Der Aufwand für dieses Verfahren besteht aus zwei Quadratwurzeln modulo den Faktoren, einem Euklidischen Algorithmus und 4 Kongruenzmultiplikationen (+ 1 Kongruenzaddition). Er bleibt also in der Größenordnung  $O(\log(n)^3)$ .

Für BLUM-Zahlen gibt es sogar einen noch einfacheren Algorithmus, nämlich eine explizite Formel:

**Korollar 1** Sei  $n = pq$  mit Primzahlen  $p, q \equiv 3 \pmod{4}$ . Dann gilt

- (i)  $d = \frac{(p-1)(q-1)+4}{8}$  ist ganzzahlig.
- (ii) Für jedes Quadrat  $x \in \mathbb{M}_n^2$  ist  $x^d$  Quadratwurzel aus  $x$ .

*Beweis.* (i) Ist  $p = 4k + 3$ ,  $q = 4l + 3$ , so  $(p-1)(q-1) = 16kl + 8k + 8l + 4$ , also  $d = 2kl + k + l + 1$ .

(ii) Der Exponent der multiplikativen Gruppe  $\mathbb{M}_n$ ,

$$\lambda(n) = \text{kgV}(p-1, q-1) = 2 \cdot \text{kgV}(2k+1, 2l+1)$$

ist Teiler von  $2 \cdot (2k+1) \cdot (2l+1)$ , der Exponent der Quadrat-Untergruppe  $\mathbb{M}_n^2$  ist  $\frac{\lambda(n)}{2}$ , also Teiler von  $(2k+1) \cdot (2l+1) = 4kl + 2k + 2l + 1 = 2d - 1$ . Also gilt  $x^{2d} \equiv x \pmod{n}$  für alle  $x \in \mathbb{M}_n^2$ , d. h., das Quadrat von  $x^d$  ergibt  $x$ .  $\diamond$

Diese einfache Formel bewirkt, dass das Verschlüsselungsverfahren von RABIN für BLUM-Moduln besonders leicht zu handhaben ist.