## 5.3 Quadratwurzeln in endlichen Primkörpern

Oft ist das Ziehen von Quadratwurzeln trivial, wie die folgende einfache Überlegung zeigt:

**Hilfssatz 1** *Sei $G$ eine endliche Gruppe von ungerader Ordnung $m$. Dann gibt es zu jedem $a \in G$ genau ein $x \in G$ mit $x^2 = a$, nämlich $x = a^{\frac{m+1}{2}}$.*

*Beweis.* Da $a^m = 1$, ist $x^2 = a^{m+1} = a$. Insbesondere ist die Quadratabbildung $x \mapsto x^2$ surjektiv, also eine Bijektion $G \longrightarrow G$. $\diamond$

Hier soll gezeigt werden, wie man in einem endlichen Primkörper $\mathbb{F}_p$ effizient Quadratwurzeln zieht. Im Falle $p \equiv 3 \pmod 4$ ist das nach der Vorbemerkung besonders einfach: Ist $p = 4k + 3$, so hat die Gruppe $\mathbb{M}_p^2$ der Quadratreste die ungerade Ordnung $\frac{p-1}{2} = 2k + 1$. Ist also $z \in \mathbb{M}_p^2$ ein Quadratrest, so ist $x = z^{k+1} \bmod p$ die eindeutige Quadratwurzel in $\mathbb{M}_p^2$ [Lagrange 1769]. Der Aufwand für dieses Quadratwurzelziehen besteht aus höchstens $2 \cdot {}^2\log(p)$ Kongruenzmultiplikationen.

**Beispiele**

1. Für $p = 7 = 4 \cdot 1 + 3$ ist $k + 1 = 2$. Nach A.9 ist 2 Quadratrest; eine Wurzel ist $2^2 = 4$. Probe: $4^2 = 16 \equiv 2$.

2. Für $p = 23 = 4 \cdot 5 + 3$ ist $k + 1 = 6$. Nach A.9 ist 2 Quadratrest; eine Wurzel ist $2^6 = 64 \equiv 18$. Probe: $18^2 \equiv (-5)^2 = 25 \equiv 2$.

Ist $p \equiv 1 \pmod 4$, ist allerdings kein so einfaches Verfahren möglich. Es ist nämlich z. B. $-1$ ein Quadrat, aber keine Potenz von $-1$ kann gleichzeitig Quadratwurzel von $-1$ sein, da $[(-1)^m]^2 = (-1)^{2m} = 1 \neq -1$ immer gilt.

Es gibt aber u. a. ein allgemein funktionierendes Verfahren, das nach Adleman, Manders und Miller auch AMM benannt wird, im wesentlichen aber schon 1903 von Cipolla angegeben wurde. Dazu wird $p - 1$ zerlegt in $p - 1 = 2^e \cdot u$ mit ungeradem $u$. Ferner wählt man (ein- für allemal) einen beliebigen Nichtquadratrest $b \in \mathbb{F}_p^\times - \mathbb{M}_p^2$; dies ist der einzige nichtdeterministische Schritt – dazu siehe Abschnitt A.9. Insbesondere ist das Verfahren unter der erweiterten Riemannschen Vermutung deterministisch, und natürlich ebenso in den vielen Fällen, wo man einen Nichtquadratrest sowieso kennt.

Nun soll aus dem Quadratrest $z \in \mathbb{M}_p^2$ die Wurzel gezogen werden. Da $z \in \mathbb{M}_p^2$, ist $\mathrm{Ord}(z) \mid \frac{p-1}{2}$, die Zweierordnung $r = \nu_2(\mathrm{Ord}(z))$ von $\mathrm{Ord}(z)$ also $\leq e - 1$, und $r$ ist minimal mit $z^{u2^r} \equiv 1$.

Jetzt wird rekursiv eine Folge $z_1, z_2, \ldots$ gebildet:

$$z_1 = z \quad \text{mit } r_1 = \nu_2(\mathrm{Ord}(z_1)).$$

Ist bereits $z_i \in \mathbb{M}_p^2$ gewählt und $r_i$ die Zweierordnung von $\mathrm{Ord}(z_i)$, so bricht die Folge ab, wenn $r_i = 0$; sonst wird

$$z_{i+1} = z_i \cdot b^{2^{e-r_i}}$$

gesetzt. Dann ist $z_{i+1} \in \mathbb{M}_p^2$. Ferner ist

$$z_{i+1}^{u \cdot 2^{r_i - 1}} \equiv z_i^{u \cdot 2^{r_i - 1}} \cdot b^{u \cdot 2^{e-1}} \equiv 1,$$

denn der erste Faktor ist $\equiv -1$, weil $r_i$ minimal war, und der zweite $\equiv (\frac{b}{p}) = -1$, weil $u \cdot 2^{e-1} = \frac{p-1}{2}$. Also ist $r_{i+1} < r_i$. Der Abbruchpunkt $r_n = 0$ wird spätestens nach $e$ Folgegliedern erreicht, $n \leq e \leq^2 \log(p)$.

Dann wird rückwärts berechnet:

$$x_n = z_n^{\frac{u+1}{2}} \bmod p$$

mit $x_n^2 \equiv z_n^{u+1} \equiv z_n$ (denn $\mathrm{Ord}(z_n) \mid u$, da es ungerade ist). Und weiter:

$$x_i = x_{i+1} / b^{2^{e-r_i-1}} \bmod p,$$

das per Induktion

$$x_i^2 \equiv x_{i+1}^2 / b^{2^{e-r_i}} \equiv z_{i+1} / b^{2^{e-r_i}} \equiv z_i$$

erfüllt. Also ist $x = x_1$ die gesuchte Wurzel von $z$.

Abgesehen vom Aufwand, um $b$ zu finden, sind folgende Schritte nötig:

- Berechnung der Potenzen $b^2, \ldots, b^{2^{e-1}}$, und das bedeutet $(e-1)$-mal modular quadrieren.
- Berechnung der Potenzen $b^u, b^{2u}, \ldots, b^{2^{e-1}u}$, und das bedeutet höchstens $2 \cdot^2 \log(u) + e - 1$ Kongruenzmultiplikationen.
- Berechnung von $z^u$ mit höchstens $2 \cdot^2 \log(u)$ Kongruenzmultiplikationen.
- Dann wird für jedes $i = 1, \ldots, n \leq e$ berechnet:
  - $z_i$ mit einer Kongruenzmultiplikation,
  - $z_i^u$ aus $z_{i-1}^u$ mit einer Kongruenzmultiplikation,
  - $z_i^{u2^r}$ aus $z_{i-1}^{u2^r}$ mit einer Kongruenzmultiplikation,
  - und daraus $r_i$.

  Das sind höchstens $3 \cdot (e-1)$ Kongruenzmultiplikationen.
- $x_n$ als Potenz mit höchstens $2 \cdot^2 \log(u)$ Kongruenzmultiplikationen.

- $x_i$ aus $x_{i+1}$ jeweils durch eine Kongruenzdivision mit Aufwand $O(\log(p)^2)$.

Das macht zusammen einen Aufwand der Größenordnung $O(\log(p)^3)$ mit einer eher kleinen Proportionalitätskonstanten.

**Beispiel.** Sei $p = 29$ und $z = 5$. Dann ist $p-1 = 4 \cdot 7$, also $e = 2$ und $u = 7$. Nach den obigen Bemerkungen ist $b = 2$ geeigneter Nichtquadratrest. Zu berechnen sind die Potenzen

$$b^2 = 4, b^u \equiv 128 \equiv 12, b^{2u} \equiv 144 \equiv -1,$$

$$z^2 \equiv 25 \equiv -4, z^4 \equiv 16, z^6 \equiv -64 \equiv -6, z^7 \equiv -30 \equiv -1.$$

Nun ist

$$z_1 = 5, z_1^u \equiv -1, z_1^{2u} \equiv 1, r_1 = 1,$$

$$z_2 \equiv z_1 b^2 \equiv 5 \cdot 4 = 20, z_2^u \equiv z_1^u b^{2u} \equiv (-1)(-1) = 1, r_2 = 0.$$

Jetzt geht's rückwärts:

$$x_2 \equiv z_2^{\frac{u+1}{2}} = z_2^4 = (z_2^2)^2 \equiv 400^2 \equiv (-6)^2 = 36 \equiv 7,$$

$$x_1 = x_2/b \bmod p = 7/2 \bmod 29 = 18.$$

Also ist $x = 18$ die gesuchte Wurzel. Probe: $18^2 = 324 \equiv 34 \equiv 5$.

**Übungsaufgaben.** Finde je einen deterministischen Algorithmus (eine einfache Formel) zum Ziehen von Quadratwurzeln in den Körpern

- $\mathbb{F}_p$ mit $p \equiv 5 \pmod 8$,
- $\mathbb{F}_{2^m}$ mit $m \geq 2$. [Ansätze: 1. Betrachte die Ordnung des jeweiligen Körperelements in der multiplikativen Gruppe. 2. Invertiere die lineare Abbildung $x \mapsto x^2$.]
- Was wird aus dem Algorithmus für einen Körper mit Primpotenzordnung $q = p^m$?

**Alternative Algorithmen.** Fast alle bekannten effizienten Algorithmen, die den Fall $p \equiv 1 \pmod 4$ vollständig abdecken, sind probabilistisch; ihre deterministische Version ist unter der erweiterten Riemannschen Vermutung noch von polynomialem Aufwand. In dem Buch von Forster (*Algorithmische Zahlentheorie*) wird eine Variante des Cipolla/ AMM-Algorithmus beschrieben, die die quadratische Körpererweiterung $\mathbb{F}_{p^2} \supseteq \mathbb{F}_p$ benützt und konzeptionell besonders einfach ist. Im *Handbook of Applied Cryptography* (Menezes/ van Oorschot/ Vanstone) wird ein Algorithmus angegeben, der von Tonelli 1891 stammt und recht kurz zu formulieren ist, aber den Aufwand $O(\log(p)^4)$ benötigt. Eine weitere Methode ist ein Spezialfall

des Verfahrens von CANTOR/ ZASSENHAUS zur Faktorisierung von Polynomen über endlichen Körpern, siehe VON ZUR GATHEN/ GERHARD: *Modern Computer Algebra.* Ein weiteres Verfahren beruht auf der LUCAS-Folge $(a_n)$ mit $a_1 = b$, $a_2 = b^2 - 2z$, wobei $b^2 - 4z$ Nicht-Quadratrest ist; dieses Verfahren stammt von LEHMER [keine Referenz]. Der einzige bekannte deterministische Algorithmus mit polynomialem Aufwand stammt von SCHOOF, verwendet die Theorie der elliptischen Kurven und ist praktisch unterlegen – Aufwand $O(\log(p)^9)$.

Für einen Überblick siehe:

- E. BACH/ J. SHALLIT: *Algorithmic Number Theory.* MIT Press, Cambridge Mass. 1996.
- D. J. BERNSTEIN: Faster square roots in annoying finite fields. Preprint (siehe die Homepage des Autors `http://cr.yp.to/`).