5.4 Quadratwurzeln bei Primzahlpotenz-Moduln

Mit einem einfachen Verfahren (hinter dem das HENSELsche Lemma steckt) kann man von Primzahlmoduln zu Primpotenzmoduln übergehen. Sei p eine Primzahl $\neq 2$ und $e \geq 2$. Sei z ein Quadratrest $\bmod p^e$. Gesucht ist eine passende Quadratwurzel.

Natürlich ist z auch Quadratrest $\bmod p^{e-1}$. Angenommen, dafür haben wir schon eine Wurzel gefunden, also ein y mit $y^2 \equiv z \pmod{p^{e-1}}$. Sei

$$a = 1/2y \bmod p$$

und $y^2 - z = p^{e-1} \cdot u$. Dann wird

$$x = y - a \cdot (y^2 - z) \bmod p^e$$

gesetzt. Damit gilt

$$\begin{aligned} x^2 &\equiv y^2 - 2ay(y^2 - z) + a^2(y^2 - z)^2 \equiv y^2 - 2ayp^{e-1}u \\ &\equiv y^2 - p^{e-1}u = z \pmod{p^e}. \end{aligned}$$

Also ist x die gesuchte Wurzel.

Dieser Algorithmus soll hier nicht explizit aufgeschrieben, aber an zwei Beispielen verdeutlicht werden:

Beispiele

1. $n = 25$, $z = 19$. Es ist $p = 5$, $19 \bmod 5 = 4$. Also kann man $y = 2$ und $a = 1/4 \bmod 5 = 4$ nehmen. Dann ist $y^2 - z = -15$ und

   $$x = 2 + 15 \cdot 4 \bmod 25 = 62 \bmod 25 = 12.$$

   Probe: $12^2 = 144 = 125 + 19$.

2. $n = 27$, $z = 19$. Es ist $p = 3$, $19 \bmod 3 = 1$. Also kann man im ersten Schritt $y = 1$ und $a = 1/2 \bmod 3 = 2$ nehmen. Dann ist $y^2 - z = -18$ und

   $$x = 1 + 2 \cdot 18 \bmod 9 = 37 \bmod 9 = 1.$$

   Beim zweiten Schritt (von 9 nach 27) ist also wieder $y = 1$, $y^2 - z = -18$ und damit

   $$x = 37 \bmod 27 = 10.$$

   Probe: $10^2 = 100 = 81 + 19$.

Der Aufwand besteht aus zwei Teilen

1. $\bmod p$ wird eine Wurzel gezogen und einmal dividiert. (Der Quotient a muss insgesamt nur einmal bestimmt werden, da $x \equiv y \pmod p$.)

2. Bei jeder Erhöhung des Exponenten sind zwei Kongruenzmultiplikationen und zwei Subtraktionen fällig.

Der Gesamtaufwand bleibt also $O(\log(n)^3)$, wenn n der Modul ist.

Es bleibt noch der Fall zu untersuchen, dass $n = 2^e$ eine Zweierpotenz ist. Ist $e \leq 3$, so ist 1 der einzige Quadratrest, und seine Wurzel ist 1. Für größere Exponenten e wird wieder auf $e - 1$ rekurriert: Sei z eine ungerade Zahl (alle invertierbaren Elemente sind ungerade). Sei y bereits gefunden mit $y^2 \equiv z \pmod{2^{e-1}}$. Dann ist $y^2 - z = 2^{e-1} \cdot t$. Ist t gerade, so auch $y^2 \equiv z \pmod{2^e}$. Andernfalls setzt man $x = y + 2^{e-2}$. Dann ist

$$x^2 \equiv y^2 + 2^{e-1}y + 2^{2e-4} \equiv z + 2^{e-1} \cdot (t + y) \equiv z \pmod{2^e},$$

da $t + y$ gerade ist. Also ist $x = y$ oder $y + 2^{e-2}$ die gesuchte Wurzel. Der Gesamtaufwand ist hier sogar kleiner als $O(\log(n)^3)$.

Nebenbei haben wir gezeigt, dass z genau dann Quadratrest mod 2^e ist (für $e \geq 3$), wenn $z \equiv 1 \pmod{8}$.