5.4 Square Roots for Prime Power Modules

A simple procedure (implicitly using HENSEL's lifting) allows to extend the square root algorithms from prime modules to prime powers. Let p be a prime $\neq 2$, and let $e \geq 2$. Let z be a quadratic residue $\bmod p^e$. We want to find a square root of z.

Of course z is also a quadratic residue $\bmod p^{e-1}$. Assume we already have found a root for it, that is a y with $y^2 \equiv z \pmod{p^{e-1}}$. Let

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

and $y^2 - z = p^{e-1} \cdot u$. We set

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

Then we have

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

Hence x is a square root of $z \bmod p^e$.

We wont explicit this algorithm but illustrate it with two examples:

Examples

1. $n = 25$, $z = 19$. We have $p = 5$, $19 \bmod 5 = 4$. Hence we can take $y = 2$ and $a = 1/4 \bmod 5 = 4$. Then $y^2 - z = -15$ and

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

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

2. $n = 27$, $z = 19$. We have $p = 3$, $19 \bmod 3 = 1$. Hence in the first step we can take $y = 1$ and $a = 1/2 \bmod 3 = 2$. Then $y^2 - z = -18$ and

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

   For the second step (from 9 to 27) again $y = 1$, $y^2 - z = -18$, and

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

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

The costs consist of two contributions:

1. One square root $\bmod p$ and one division. (The quotient a needs to be computed only once since $x \equiv y \pmod{p}$.)

2. Each time the exponent is incremented we execute two congruence multiplications and two subtractions.

Hence the total cost is $\mathrm{O}(\log(n)^3)$ for the module n.

Finally we have to consider the case where $n = 2^e$ is a power of two.

For $e \leq 3$ the only quadratic residue is 1, its square root is 1.

For larger exponents e we have again a recurrence to $e - 1$: Let z be an odd integer (all invertible elements are odd). Assume we already found a y with $y^2 \equiv z \pmod{2^{e-1}}$. Then $y^2 - z = 2^{e-1} \cdot t$. If t is even, then $y^2 \equiv z \pmod{2^e}$. Otherwise we set $x = y + 2^{e-2}$. Then

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

since $t + y$ is even. Hence $x = y$ or $y + 2^{e-2}$ is a square root of z. Here the cost is even smaller than $\mathrm{O}(\log(n)^3)$.

By the way we have shown that z is a quadratic residue $\bmod 2^e$ (for $e \geq 3$) if and only if $z \equiv 1 \pmod 8$.