5.5 Square Roots for Composite Modules

If we know the prime decomposition of the module n, then we can efficiently compute square roots in $\mathbb{M}_n$. The two tasks “factoring” and “computing square roots” are equivalent with respect to their complexity.

For an execution of the procedure we successively decompose n into coprime factors (down to the prime powers).

So let $n = rs$ with coprime factors r and s. First we compute coefficients a and b such that $ar + bs = 1$ using the extended Euclidean algorithm.

We want to find a square root of z. Let u be a square root $\bmod r$ and v be a square root $\bmod s$. Then $x := arv + bsu \bmod n$ satisfies the congruences:

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

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

The cost for this procedure is two square roots modulo the factors, one Euclidean algorithm, and four congruence multiplications (+ 1 congruence addition). Hence it is $\mathrm{O}(\log(n)^3)$.

For Blum integers (see Appendix A.11) we even have a simpler algorithm, namely an explicit formula:

Corollary 1 *Let $n = pq$ with primes $p, q \equiv 3 \pmod{4}$. Then*

(i) $d = \frac{(p-1)(q-1)+4}{8}$ *is an integer.*

(ii) *For each quadratic residue $x \in \mathbb{M}_n^2$ the power x^d is the (unique) square root of x in $\mathbb{M}_n^2$.*

Proof. (i) If $p = 4k + 3$, $q = 4l + 3$, then $(p-1)(q-1) = 16kl + 8k + 8l + 4$, hence $d = 2kl + k + l + 1$.

(ii) The exponent of the multiplicative group $\mathbb{M}_n$,

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

is a divisor of $2 \cdot (2k+1) \cdot (2l+1)$, The exponent of the subgroup $\mathbb{M}_n^2$ of squares is $\frac{\lambda(n)}{2}$, hence a divisor of $(2k+1)\cdot(2l+1) = 4kl+2k+2l+1 = 2d-1$. Thus $x^{2d} \equiv x \pmod{n}$ for all $x \in \mathbb{M}_n^2$, thus the square of x^d is x. $\diamond$

This simple formula has the effect that the Rabin cipher is especially easy to handle for Blum integer modules.