A.11 Blum Integers

Let $n = pq$ with different primes $p, q \geq 3$. Then

$$\mathbb{M}_n \cong \mathbb{M}_p \times \mathbb{M}_q, \quad \mathbb{M}_n^2 \cong \mathbb{M}_p^2 \times \mathbb{M}_q^2,$$

$$\mathbb{M}_n/\mathbb{M}_n^2 \cong \mathbb{M}_p/\mathbb{M}_p^2 \times \mathbb{M}_q/\mathbb{M}_q^2 \cong \mathcal{Z}_2 \times \mathcal{Z}_2,$$

in particular $\#(\mathbb{M}_n/\mathbb{M}_n^2) = 4$. The subgroups $\mathbb{M}_n^2 \leq \mathbb{M}_n^+$ and $\mathbb{M}_n^+ \leq \mathbb{M}_n$ are proper and hence of index 2. The ring $\mathbb{Z}/n\mathbb{Z}$ contains exactly 4 roots of unity: $1, -1, \tau, -\tau$, where

$$\tau \equiv -1 \pmod p, \quad \tau \equiv 1 \pmod q,$$

thus $(\frac{\tau}{n}) = -1$. In other words: The kernel of the squaring homomorphism $\mathbf{q} : \mathbb{M}_n \longrightarrow \mathbb{M}_n^2$ is $K = \{\pm 1, \pm\tau\}$, isomorphic with the Klein four-group.

An integer of the form $n = pq$ with different primes $p, q \equiv 3 \pmod 4$ is called Blum **integer**.

Examples

1. 1177 in A.6.
2. If p is a special prime, then $p \equiv 3 \pmod 4$. Therefore a product of two special primes is a Blum integer. Let us call such an integer a **special** Blum **integer**.

In general, if $n = pq$ with different odd prime numbers p and q, then $\mathbb{M}_n^2 \cong \mathbb{M}_p^2 \times \mathbb{M}_q^2$ has order $\frac{p-1}{2} \cdot \frac{q-1}{2}$, and this number is odd if and only if p and q both are $\equiv 3 \pmod 4$. Hence:

Lemma 25 *A product n of two odd prime numbers is a* Blum *integer if and only if the group $\mathbb{M}_n^2$ of quadratic residues has odd order.*

For a Blum integer -1 is a quadratic non-residue in $\mathbb{M}_p$ and $\mathbb{M}_q$, hence also in $\mathbb{M}_n$. But

$$(\frac{-1}{n}) = (\frac{-1}{p})(\frac{-1}{q}) = (-1)^2 = 1,$$

thus $-1 \in \mathbb{M}_n^+$. Hence

$$(\frac{-x}{n}) = (\frac{-1}{n})(\frac{x}{n}) = (\frac{x}{n})$$

for all x. Moreover $\mathbb{M}_n^2 \cap K = \{1\}$, thus the restriction of $\mathbf{q}$ to $\mathbb{M}_n^2$ is injective, hence bijective, and $\mathbb{M}_n$ is the direct product

$$\mathbb{M}_n = K \times \mathbb{M}_n^2, \quad \mathbb{M}_n^+ = \{\pm 1\} \times \mathbb{M}_n^2.$$

Each quadratic residue $a \in \mathbb{M}_n^2$ has exactly one square root in each of the four cosets of $\mathbb{M}_n/\mathbb{M}_n^2$. If $x \in \mathbb{M}_n^2$ is one of them, then the other ones are $-x$, τx, $-\tau x$. This shows:

Proposition 24 *Let n be a* Blum *integer. Then:*

(i) *If $x^2 \equiv y^2 \pmod{n}$ for $x, y \in \mathbb{M}_n$, and $x, -x, y, -y \bmod n$ are pairwise distinct, then $(\frac{x}{n}) = -(\frac{y}{n})$.*

(ii) *The squaring homorphism $\mathbf{q}$ is an automorphism of $\mathbb{M}_n^2$.*

(iii) *Each $a \in \mathbb{M}_n^2$ has has exactly two square roots in $\mathbb{M}_n^+$. If x is one of them, then $-x \bmod n$ is the other one, and exactly one of these two is itself a quadratic residue. Moreover a has exactly two more square roots, and these are contained in $\mathbb{M}_n^-$.*

Thus from the four square roots of a quadratic residue x exactly one is itself a quadratic residue. We consider this one as something special, and denote it by $\sqrt{x} \bmod n$. The least significant bit of x—also characterized as the parity of x, or as $x \bmod 2$—is denoted by $\mathrm{lsb}(x)$.

Corollary 1 *Let $x \in \mathbb{M}_n^+$. Then x is a quadratic residue if and only if*

$$\mathrm{lsb}(x) = \mathrm{lsb}(\sqrt{x^2} \bmod n).$$

Proof. If x is a quadratic residue, then $x = \sqrt{x^2} \bmod n$. Now assume x is a quadratic non-residue, and let $y = \sqrt{x^2} \bmod n$. By (iii) we have $y = -x \bmod n = n - x$. Since n is odd, x and y have different parities. ◇

The problem of deciding quadratic residuosity $\bmod n$ remains hard. Only if the prime decomposition $n = pq$ is known there is an efficient solution:

$$x \in \mathbb{M}_n^2 \iff (\frac{x}{p}) = (\frac{x}{q}) = 1.$$

We know of no efficient procedure that works without using the prime factors. *Presumably* deciding quadratic residuosity is equivalent with factoring in the sense of complexity theory. Generally believed to be true is the

Quadratic Residuosity Assumption: Deciding quadratic residuosity for Blum integers is hard.

A mathematical sound definition of "hard" is in Section B.7.