A.5 The Jacobi Symbol

Consider the multiplicative group $\mathbb{M}_n = (\mathbb{Z}/n\mathbb{Z})^\times$ for a module $n \geq 2$, and its squaring map

$$\mathbf{q}\colon \mathbb{M}_n \longrightarrow \mathbb{M}_n, \quad x \mapsto x^2 \bmod n\,.$$

$\mathbf{q}$ is a group homomorphism. The elements in the image of $\mathbf{q}$ are the **quadratic residues** mod n. An integer x is a quadratic residue mod n if $x \bmod n$ is invertible, and there exists an integer u with $u^2 \equiv x \pmod{n}$. Thus the set of quadratic residues is the subset $\mathbb{M}_n^2$ of the residue class ring $\mathbb{Z}/n\mathbb{Z}$. (This notation is not standard just as little as $\mathbb{M}_n$. But it spares writing $((\mathbb{Z}/n\mathbb{Z})^\times)^2$ over and over again.)

Remarks and Examples

1. For $n = 2$ we have $\mathbb{M}_n^2 = \mathbb{M}_n = \{1\}$.

2. For $n \geq 3$ we have $-1 \neq 1$ and $(-1)^2 = 1$. Hence $\mathbf{q}$ is not injective and thus also not surjective. Therefore quadratic non-residues exist.

3. Let $n = p \geq 3$ be prime. Then the kernel of $\mathbf{q}$ exactly consists of the zeroes of the polynomial $X^2 - 1$ in the field $\mathbb{F}_p$, hence of $\{\pm 1\}$. We conclude that the number of quadratic residues is $\frac{p-1}{2}$.

4. More generally let $n = q = p^e$ be a power of an odd prime p. Then $\mathbb{M}_n$ is cyclic of order $\varphi(q) = q \cdot (1 - \frac{1}{p})$ by Proposition 18. Thus 1 has exactly the square roots ± 1 in $\mathbb{M}_q$, and the number of quadratic residues is $\varphi(q)/2$.

5. Let n be a product of two different odd primes p and q. By the chinese remainder theorem the natural map $\mathbb{M}_n \longrightarrow \mathbb{M}_p \times \mathbb{M}_q$ is an isomorphism. Hence $\mathbb{M}_n$ contains exactly four square roots of 1, and $\mathbb{M}_n^2 \leq \mathbb{M}_n$ is a subgroup of index 4.

6. In the general case let $n = 2^e p_1^{e_1} \cdots p_r^{e_r}$ be the prime decomposition with different odd primes $p_1, \ldots, p_r$, and $r \geq 0$, $e \geq 0$, $e_1, \ldots, e_r \geq 1$. Proposition 2 tells us the number of square roots of 1 in $\mathbb{M}_n$:

$$\begin{array}{ll} 2^r, & \text{if } e = 0 \text{ or } 1, \\ 2^{r+1}, & \text{if } e = 2, \\ 2^{r+2}, & \text{if } e \geq 3. \end{array}$$

   This number is also the order of the kernel of $\mathbf{q}$, hence the index of $\mathbb{M}_n^2$ in $\mathbb{M}_n$.

The naive algorithm, exhaustion, for determing the quadratic residuosity of a mod n tries $1^2, 2^2, 3^2, \ldots$ until it hits a. A quadratic non-residue always takes $\lfloor \frac{n}{2} \rfloor$ steps, a quadratic residue $n/4$ steps in the average. Thus the costs grow exponentially with the number $\log n$ of places.

For the case where n is *prime* we'll see better algorithms.

The phenomen that there is no efficient algorithm for *composite* integers n is the basis of many cryptographic constructions, for instance the simplest perfect random generator (BBS, see Part IV).

For a prime module p the LEGENDRE **symbol** indicates quadratic residuosity:

$$(\frac{x}{p}) = \begin{cases} 1 & \text{if } x \text{ is a quadratic residue,} \\ 0 & \text{if } p|x, \\ -1 & \text{otherwise.} \end{cases}$$

The LEGENDRE symbol defines a homomorphism

$$(\frac{\bullet}{p}) : \mathbb{M}_p \longrightarrow \mathbb{M}_p/\mathbb{M}_p^2 \cong \{\pm 1\}.$$

In the special case $p = 2$

$$(\frac{x}{2}) = \begin{cases} 1 & \text{if } x \text{ is odd,} \\ 0 & \text{if } x \text{ is even.} \end{cases}$$

Proposition 19 (EULER's criterion) *Let p be an odd prime. then*

$$x^{\frac{p-1}{2}} \equiv (\frac{x}{p}) \pmod p \quad \textit{for all } x.$$

Proof. If $p|x$ both sides equal 0. Otherwise $(x^{\frac{p-1}{2}})^2 = x^{p-1} \equiv 1$, hence $x^{\frac{p-1}{2}} \equiv \pm 1$. Let a be primitive $\bmod p$. Then both sides equal -1, hence the assertion holds for $x = a$. Since both sides represent homomorphisms $\mathbb{F}_p^\times \longrightarrow \{\pm 1\}$ the assertion is true for all powers of a, hence for all x that are no multiples of p. $\diamond$

EULER's criterion yields an efficient algorithm for deciding quadratic residuosity: We have to take $\frac{p-1}{2}$-th powers in $\mathbb{F}_p^\times$, and this costs at most $2\lfloor \log_2(\frac{p-1}{2}) \rfloor$ multiplications $\bmod p$. Taking the cost of modular multiplication into account we get an order of magnitude of $\log_2(p)^3$.

By EULER's criterion -1 is a quadratic residue if and only if $\frac{p-1}{2}$ is even, hence $p \equiv 1 \pmod 4$. The decision on 2 or 3 is significantly more difficult. However there is an even faster algorithm. It is the subject of the following Section A.6.

The LEGENDRE symbol has a natural generalization by the JACOBI symbol (that uses the same notation): For $n > 0$ with prime decomposition

$n = p_1 \cdots p_r$ (the p_i not necessarily distinct)

$$(\frac{x}{n}) := (\frac{x}{p_1}) \cdots (\frac{x}{p_r}) \quad \text{for } x \in \mathbb{M}_n.$$

In particular $(\frac{x}{n}) = 0$ if x and n are not coprime. The supplementing definitions $(\frac{x}{1}) = 1$, $(\frac{x}{n}) = (\frac{x}{-n})$ for $n < 0$, and $(\frac{x}{0}) = 0$, make the Jacobi symbol a function

$$(\frac{\bullet}{\bullet}) : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

with values in $\{0, \pm 1\}$, and multiplicative in numerator and denominator. In particular the Jacobi symbol defines a homomorphism $(\frac{\bullet}{n})$ from $\mathbb{M}_n$ to $\{\pm 1\}$. But it is *not* an indicator of quadratic residuosity. Denoting $\mathbb{M}_n^+ = \ker(\frac{\bullet}{n})$ and $\mathbb{M}_n^- = \mathbb{M}_n - \mathbb{M}_n^+$, in general $\mathbb{M}_n^2$ is a proper subgroup of $\mathbb{M}_n^+$. Its index is given by example 6 above: If the number of square roots of 1 is 2^k with $k \geq 1$, then $\mathbb{M}_n^2$ has index 2^{k-1} in $\mathbb{M}_n^+$.

In any case $(\frac{x}{n})$ depends on the residue class $x \bmod n$ only. Obviously

$$(\frac{x}{2^k}) = \begin{cases} 1, & \text{if } x \text{ is odd,} \\ 0, & \text{if } x \text{ is even.} \end{cases}$$