Quadratic Residues

Definition: Let q be a prime power. An element $a \in \mathbb{F}_q^*$ from the multiplicative group of the finite q-element field is called *quadratic residue* if there exists an element $y \in \mathbb{F}_q$ such that

$$y^2 = a.$$

If there is no such y then a is called a *quadratic non-residue*. Note that 0 is excluded from the list of quadratic residues and non-residues. The set of quadratic residues of $\mathbb{F}_q$ is denoted by $QR(q)$ and the set of quadratic non-residues by $QNR(q)$.

Theorem 1 *Let q be an odd prime power, and $a \in \mathbb{F}_q^*$ then*

$$\begin{aligned} a \in QR(q) \quad &\Leftrightarrow \quad a^{\frac{q-1}{2}} = 1 \\ a \in QNR(q) \quad &\Leftrightarrow \quad a^{\frac{q-1}{2}} = -1. \end{aligned}$$

Furthermore,

$$|QR(q)| \;=\; \frac{q-1}{2} \;=\; |QNR(q)|.$$

Proof. For the proof of Theorem 1 recall two facts from algebra:

1: A polynomial of degree d, with coefficients from a field R, can have at most d roots in R. (Proof by induction on the degree).

2: **Lagrange's Theorem:** In a finite group G, $x^{|G|} = 1$ for any $x \in G$.

On the one hand by Fact 1 the polynomial $x^{q-1} - 1 = 0$ cannot have more than $q-1$ roots in $\mathbb{F}_q$. On the other hand it does have $q-1$ roots by Lagrange's Theorem, because all the elements in $\mathbb{F}_q^*$ are roots.

Consequently, since $x^{q-1} - 1 = \left(x^{\frac{q-1}{2}} - 1\right)\left(x^{\frac{q-1}{2}} + 1\right)$ and the ring of polynomials over $\mathbb{F}_q$ has no (non-trivial) zero divisors, again Fact 1 implies that both factors $\left(x^{\frac{q-1}{2}} - 1\right)$ and $\left(x^{\frac{q-1}{2}} + 1\right)$ must have exactly $\frac{q-1}{2}$ roots.

If $a = y^2$ is a quadratic residue in $\mathbb{F}_q$ then $a^{\frac{q-1}{2}} = y^{q-1} = 1$ by Lagrange's Theorem. Hence, a is a root of $x^{\frac{q-1}{2}} - 1$ implying that $|QR(q)| \leq \frac{q-1}{2}$. On the other hand note that by Fact 1 the polynomial $x^2 - a$ has at most two roots for any quadratic residue a, hence

$$q - 1 \;=\; \left|\mathbb{F}_q^*\right| \;\leq\; \sum_{a \in QR(q)} \left|\{x \;:\; x^2 = a\}\right| \;\leq\; 2|QR(q)|.$$

Concluding, $|QR(q)| = \frac{q-1}{2}$ and thus $QR(q)$ must be equal to the set of roots of $\left(x^{\frac{q-1}{2}} - 1\right)$. Then it follows that also $|\mathrm{QNR}(q)| = \frac{q-1}{2}$, and $QNR(q)$ must be equal to the set of roots of $\left(x^{\frac{q-1}{2}} + 1\right)$. $\square$

Corollary 1 *The product of two quadratic residues or two non-residues is a quadratic residue, whereas the product of a residue and a non-residue gives a non-residue.*

Corollary 2

$$\begin{aligned} -1 \in QR(q) &\quad\Leftrightarrow\quad q \equiv 1 \pmod 4 \\ -1 \in QNR(q) &\quad\Leftrightarrow\quad q \equiv 3 \pmod 4. \end{aligned}$$

Observe that $x^2 = (-x)^2$, which, in the case of a prime field $\mathbb{F}_p$, implies that

$$QR(p) = \left\{ y^2 \ : \ 0 < y \leq \frac{p-1}{2} \right\}.$$

Remark The q-element field is in general not equal to the ring of congruence classes, i.e. calculating modulo q. Only for q being a prime this is true. To demonstrate this, we want to calculate the quadratic residue in $\mathbb{F}_{27}$. The field $\mathbb{F}_{27}$ can be seen as the ring of polynomials over $\mathbb{F}_3$ where we calculate modulo the irreducible polynom $(x^3 + 2x^2 + 2x + 2)$,

$$\mathbb{F}_{27} \cong \mathbb{F}_3[x]/(x^3 + 2x^2 + 2x + 2).$$

For example $-1 = 2$ in this field and

$$(x^2+x+1)^2 = x^4+2x^3+x^2+2x+1 = x(x^3+2x^2+2x+2)-x^2+1 = 2x^2+1.$$

We can use Maple to calculate $QR(27)$ and $QNR(27)$:

```
> with(numtheory):
> G27:= GF(3,3):
> G27[extension];
```

$$(T^3 + 2T^2 + 2T + 2) \mod 3$$

```
> elements := seq(G27[input](i), i=0..26):
> q := x -> evalb( G27[`^`](x,13) = G27[input](1) ):
> QR27 := select( q, [elements]);
```

$$\begin{aligned} QR(27) \quad := \quad & \{1, T, 2T+1, 2T+2, T^2, T^2+1, T^2+2, T^2+T+1, \\ & T^2+2T+1, T^2+2T+2, 2T^2+T, 2T^2+2T, 2T^2+2T+2\}. \end{aligned}$$

```
> QNR27 := select( not q, [elements]);
```

$$\begin{aligned} QNR(27) \quad := \quad & \{2, T+1, T+2, 2T, T^2+T, T^2+T+2, T^2+2T, 2T^2, \\ & 2T^2+1, 2T^2+2, 2T^2+T+1, 2T^2+T+2, 2T^2+2T+2\}. \end{aligned}$$