Sign in finite fields

Abraham Westerbaan*[1] and Bas Westerbaan†[2]

[1]Radboud Universiteit Nijmegen
[2]University College London & Cloudflare

August 28, 2020

In cryptography it is often required to make a choice of square root. Often in a finite field $\mathbb{F}_p$, with p and odd prime, one chooses the root whose least positive integer representative is odd. Such an element is called *positive*, so that one can utter the familiar phrase "the positive square root". Following the terminology, one defines a *sign* on the finite field:

$$\operatorname{sign}\colon \mathbb{F}_p \to \{-1,0,1\} \qquad \operatorname{sign}(n) = \begin{cases} 1 & n \text{ is odd} \\ 0 & n = 0 \\ -1 & n \text{ is even} \end{cases} \qquad \text{where } n \leq p.$$

This map has few properties.

1. $\operatorname{sign}(-x) = -\operatorname{sign}(x)$.
2. If $\operatorname{sign}(x) = 0$, then $x = 0$.
3. $\operatorname{sign}(Tx) = \operatorname{sign}(x)$ for any isomorphism T.

The existence of such a sign map is equivalent to being able to make a choice of square root independent of the construction of $\mathbb{F}_p$. Indeed given such a sign map one simply chooses the root with sign 1. Conversely, suppose we can make a choice of root independent of the construction of $\mathbb{F}_p$, then we define

$$\operatorname{sign}(x) = \begin{cases} 1 & x \neq 0 \text{ and } \sqrt{x^2} = x \\ 0 & x = 0 \\ -1 & \text{otherwise.} \end{cases}$$

This sign satisfies the three axioms above. In this paper we will study when such a sign exists for a finite field $\mathbb{F}_{p^k}$ with odd $p \neq 1$ and $k \neq 0$. We will show it exists if and only if k is odd.

*bram@westerbaan.name
†bas@westerbaan.name

Assume k is even. Reasoning towards contradiction, assume a sign map with the listed properties exists. Note that any non-zero $x \in \mathbb{F}_p \subseteq \mathbb{F}_{p^k}$ (i.e. $x^p = x$) has a root in $\mathbb{F}_{p^k}$. Indeed:

$$x^{\frac{p^k-1}{2}} \;=\; \left(x^{\frac{p-1}{2}}\right)^{1+p+\ldots+p^{k-1}} \;\overset{\circledast}{=}\; \left(x^{\frac{p-1}{2}}\right)^{k} \;=\; 1.$$

(Equality $\circledast$ holds because $x^{\frac{p-1}{2}} \in \{-1,1\}$ and so $(x^{\frac{p-1}{2}})^a$ only depends on the parity of a.) Pick any $x \in \mathbb{F}_p$ that has no square root in $\mathbb{F}_p$ (which exists as $p \geq 3$.) Thus $x^{\frac{p-1}{2}} = -1$. We just saw that x does have a square root α in $\mathbb{F}_{p^k}$, i.e. $\alpha^2 = x$. Then $\alpha^p = \alpha(\alpha^{\frac{p-1}{2}})^2 = \alpha x^{\frac{p-1}{2}} - \alpha$. Recall that the Frobenius map $\varphi(x) \equiv x^p$ is an automorphism of $\mathbb{F}_{p^k}$. Combined with the previous we see

$$\operatorname{sign}(\alpha) \;=\; \operatorname{sign}(\alpha^p) \;=\; \operatorname{sign}(-\alpha) \;=\; -\operatorname{sign}(\alpha).$$

Thus $\operatorname{sign}(\alpha) = 0$, whence $\alpha = 0$, quod non. We have now shown that no such sign can exist for even k.

Now assume k is odd. We will construct a sign map. We must choose $\operatorname{sign}(0) = 0$. We will proceed in steps. Pick any element x for which sign is not yet defined. We choose $\operatorname{sign}(x) = 1$. We are then also forced to define $\operatorname{sign}(-x) = -\operatorname{sign}(x)$. As our characteristic p is odd, we know $x \neq -x$ and so this does not directly lead a contradiction. For any automoprhism T we are forced to define $\operatorname{sign}(T(x)) = \operatorname{sign}(x)$ and $\operatorname{sign}(-T(x)) = -\operatorname{sign}(x)$. To show this can be done consistently, assume reasoning towards contradiction that it cannot be done consistently. Then there must be automorphisms T and S such that $Tx = -Sx$ for some $x \in \mathbb{F}_{p^k}$. As the only automorphisms of $\mathbb{F}_{p^k}$ are the powers of the Frobenius map, i.e. $\varphi, \varphi^2, \ldots, \varphi^k = \mathrm{id}$, we see that then there are n and m with $\varphi^n(x) = -\varphi^m(x)$. Thus $-x = \varphi^\ell(x) = x^{p^\ell}$ for some ℓ.

Note that we have $(x^2)^{p^\ell} = (-x)^2 = x^2$. Recall $\{y;\ y^{p^\ell} = y\}$ is a subfield (in fact it's the fixed field of $\langle\varphi^\ell\rangle$.) It is non-trivial because it contains x^2. Thus $p^\ell - 1 \mid p^k - 1$. As $\gcd(p^\ell - 1, p^k - 1) = p^{\gcd(\ell,k)} - 1$ [Lin], we must have $\ell \mid k$. In particular ℓ is odd.

We had $x^{p^\ell} = -x$ and so $x^{p^{\ell a}} = (-1)^a x$ for any a and in particular $x = x^{p^k} = x^{p^{\ell \frac{k}{\ell}}} = -x$. Thus $x = 0$, quod non. Contradiction.

References

[Lin] Juan Liner. Prove that $\gcd(a^n - 1, a^m - 1) = a^{\gcd(n,m)} - 1$. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/7473 (version: 2015-07-05).