Generalizing Wilson's and Legendre-symbol thm to finite fields: NumThy

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
1 March, 2023 (at *12:15*)

Overview. We extend some theorems about the finite fields.

Standing notation. Use $\mathsf{F} = \mathsf{F}_{\mathbf{q}} := \mathbb{GF}(\mathbf{q})$ for the finite field of cardinality $\mathbf{q} = p^L$, where p is prime and $L \in \mathbb{Z}_+$. So $\mathsf{F}_p = \mathbb{Z}_p$. Rather than $\mathbf{q}$, use $\boxed{\mathcal{F} := |\mathsf{F}|}$ and, extending our Euler-phi-fnc notation, define the units-group

$$\Phi_{\mathsf{F}} \;:=\; \mathsf{F} \smallsetminus \{0\} \quad \textit{and} \quad \varphi_{\mathsf{F}} \;:=\; |\Phi_{\mathsf{F}}| \;=\; \mathcal{F} - 1\,.$$

More generally, consider a commutative ring Γ: We will *sometimes* use $0,1$ for the zero and one of Γ, to emphasize that they are elements of the ring. Use Φ_Γ for the units-group,

$$\{\alpha \in \Gamma \mid \exists \beta \in \Gamma \quad \text{s.t} \quad \alpha\beta = 1\}\,.$$

Say "F *is odd*" to mean $|\mathsf{F}|$ is odd, i.e the characteristic of the field, $\text{Char}(\mathsf{F}) \overset{\text{note}}{=\!=} p$, is odd. Finally, when F is odd, define [H for Half]

$$H_{\mathsf{F}} \;:=\; \tfrac{1}{2}\cdot|\Phi_{\mathsf{F}}| \;=\; \frac{\mathcal{F}-1}{2}\,.$$

Legendre symbol. A ***quadratic-residue***, an F-QR, is an $\alpha \in \Phi_{\mathsf{F}}$ for which $\exists \sigma \in \mathsf{F}$ such that $\sigma^2 = \alpha$. [Necessarily, $\sigma \in \Phi_{\mathsf{F}}$.]

A ***non-quadratic–residue***, an F-NQR, is a unit α for which *no* sqroot exists.

Define the ***Legendre-symbol*** $\left(\frac{\cdot}{\mathsf{F}}\right)\!:\mathsf{F}\to\{-1,0,+1\}$ by $\left(\frac{0}{\mathsf{F}}\right) := 0$ and, for α a unit: $\left(\frac{\alpha}{\mathsf{F}}\right) := +1$ if $\alpha \in \text{QR}$, else $\left(\frac{\alpha}{\mathsf{F}}\right) := -1$ if $\alpha \in \text{NQR}$. □

1: Gen Wilson's Thm. *Below, F is a finite-field, and Γ is a commutative ring with finite units-group.*

a: *Let $S := \{\sigma \in \Gamma \mid \sigma^2 = 1\}$, the sqroots of 1. Then $\prod(\Phi_\Gamma) = \prod(S)$.*

b: *For $p = 2$: Product $\prod(\Phi_{\mathsf{F}}) = 1 \overset{\text{note}}{=\!=} -1$, in F.*

c: *For p an odd prime: Product $\prod(\Phi_{\mathsf{F}}) = -1$.* ◊

Pf of (a). Define $h\!:\!\Phi_\Gamma\circlearrowleft$ by $h(x) := 1/x$. Since h is an involution, orbits have size 2 or 1 [are h-fixed-points]. The elements of a size-2 orbit multiply to 1, so we can discard them. ♦

Pf of (b,c). Polynomial $x^2 - 1$ factors over F as $[x-1][x+1]$, and this factorization is unique, since F is a field. Hence the only h-fixed-pts are ± 1.

When $p = 2$, then $-1{=}1$, whence $\prod(\Phi_{\mathsf{F}}) = 1$. For p oddprime, $\prod(\Phi_{\mathsf{F}}) = \prod(\{-1, 1\}) = -1$. ♦

2: Legendre-Symbol Thm (LSThm). *Every unit in $\mathbb{GF}(2^L)$ is a QR.*

Fix an odd(-card.) field F. Then for all $x,\alpha,\beta \in \mathsf{F}$:

i: $\left(\frac{x}{\mathsf{F}}\right) = x^{H_{\mathsf{F}}}$.

ii: $\left(\frac{\alpha\cdot\beta}{\mathsf{F}}\right) = \left(\frac{\alpha}{\mathsf{F}}\right)\left(\frac{\beta}{\mathsf{F}}\right)$. *Also,* $\left(\frac{-1}{\mathsf{F}}\right) = \langle\mathcal{F}\rangle_4$,
where $\langle\cdot\rangle_4$ is the symmetric mod-4 residue. ◊

Proof. The units group of $\mathsf{F} := \mathbb{GF}(2^L)$ has odd order $D := 2^L - 1$. Recall that the mult-group of a field is cyclic, so squaring on Φ_{F} is the doubling-map on an odd-cycle, which is surjective.

Establishing (i). Fix an odd F, set $\Phi := \Phi_{\mathsf{F}}$ and $H := \frac{1}{2}[\,|\mathsf{F}| - 1]$ Certainly $\left(\frac{0}{\mathsf{F}}\right) = 0 = 0^H$.

Fix a unit α and define $g\!:\!\Phi\circlearrowleft$ by $g(x) := \alpha/x$, which is an involution. The g-fixed-pts are the sqroots of α.

CASE: $\alpha \in \text{NQR}$ Thus g pairs all elements of Φ. Hence

$$\alpha^H \;=\; \prod(\Phi) \overset{\text{Wilson's}}{=\!=} -1 \overset{\text{note}}{=\!=} \left(\frac{\alpha}{\mathsf{F}}\right).$$

CASE: $\alpha \in \text{QR}$ Take $\sigma \in \mathsf{F}$ so that $\sigma^2 = \alpha$. Note $\pm\sigma$ are distinct [F is odd], so they are the *only* [since F is a field] sqroots of α. Thus $\alpha^{H-1} = \prod(\Phi \smallsetminus \{\pm\sigma\})$. Hence

$$-1 \overset{\text{Wilson's}}{=\!=} \prod(\Phi) \;=\; \alpha^{H-1}\cdot -\sigma\cdot\sigma \;=\; -1\cdot\alpha^H\,.$$

So $\alpha^H = 1 \overset{\text{note}}{=\!=} \left(\frac{\alpha}{\mathsf{F}}\right)$.

Finally, both (ii) and (iii) follow from (i). ♦

Relations among QRs. We start by summing Legendre-symbols along a quadratic polynomial.

3: Quad-Legendre-sum Thm (G. Andrews, P.130, Thm 10-3). *On an odd* F, *let* $g(x) := [x-U][x-V]$, *where* $U,V \in \mathsf{F}$. *Define the sum*

$$\mathcal{S} := \sum_{x\in\mathsf{F}} \left(\frac{g(x)}{\mathsf{F}}\right).$$

If $U = V$ *then* $\mathcal{S} = \mathcal{F} - 1$. *If* $U \neq V$ *then* $\mathcal{S} = -1$. ♢

Proof. Set $y := x - U$ and $D := V - U \in \mathsf{F}$. This CoV makes $\mathcal{S} = \sum_y (\frac{y\cdot[y-D]}{\mathsf{F}}) = \sum_{y\neq 0} (\frac{y\cdot[y-D]}{\mathsf{F}})$, since $(\frac{0}{\mathsf{F}}) = 0$. Use $\widetilde{y}$ for the reciprocal of y. Then

$$\left(\frac{y\cdot[y-D]}{\mathsf{F}}\right) = \left(\frac{\widetilde{y}^2}{\mathsf{F}}\right)\cdot\left(\frac{y\cdot[y-D]}{\mathsf{F}}\right) = \left(\frac{1-D\widetilde{y}}{\mathsf{F}}\right).$$

Setting $z := \widetilde{y}$, then, $\mathcal{S} = \sum_{z\neq 0} (\frac{1-Dz}{\mathsf{F}}) = \left[\sum_z (\frac{1-Dz}{\mathsf{F}})\right] - 1$, since $(\frac{1}{\mathsf{F}}) = 1$.

CASE: $U = V$ So $D = 0$, hence $\mathcal{S} = \mathcal{F} - 1$.

CASE: $U \neq V$ Now $D \neq 0$. As z ranges over F, so does Dz, hence so does $1 - Dz$. Our F is odd, so $\sum_w (\frac{w}{\mathsf{F}}) = 0$. Thus $\mathcal{S} = 0 - 1 = -1$. ♦

4a: Lemma. *Fix an odd* F *and a* $D \in \mathsf{F}$. *Define*

$$\mathcal{S}_D := \sum_x \left(\frac{x^2 - D}{\mathsf{F}}\right).$$

When $D \neq 0$ *then* $\mathcal{S}_D = -1$. *Trivially,* $\mathcal{S}_0 = \mathcal{F} - 1$. ♢

Pf. Fix $D \neq 0$ and define

$$\mathcal{Q} := \sum_{w\in\mathrm{QR}} \left(\frac{1-w}{\mathsf{F}}\right) \quad \text{and} \quad \mathcal{N} := \sum_{z\in\mathrm{NQR}} \left(\frac{1-z}{\mathsf{F}}\right).$$

For each $x \in \Phi$, let $\widetilde{x}$ denote its reciprocal.

Note $\mathcal{S}_D - (\frac{-D}{\mathsf{F}})$ equals

$$\sum_{x\neq 0} \left(\frac{x^2-D}{\mathsf{F}}\right) = \sum_{x\neq 0} \left(\frac{1-D\widetilde{x}^2}{\mathsf{F}}\right) = \sum_{y\neq 0} \left(\frac{1-Dy^2}{\mathsf{F}}\right).$$

CASE: $D \in \mathrm{QR}$ Then $(\frac{-D}{\mathsf{F}}) = (\frac{-1}{\mathsf{F}}) = \langle\mathcal{F}\rangle_4$. As y varies, product Dy^2 hits each QR twice. Consequently, $\mathcal{S}_D - \langle\mathcal{F}\rangle_4 = 2\mathcal{Q}$. We see all QRs D yield the same $\mathcal{S}_D$. Calling the common value $\mathcal{S}_{\mathrm{QR}}$, we have

$$\mathcal{S}_{\mathrm{QR}} - \langle\mathcal{F}\rangle_4 = 2\mathcal{Q}.$$

CASE: $D \in \mathrm{NQR}$ Now $(\frac{-D}{\mathsf{F}}) = -\langle\mathcal{F}\rangle_4$. As y varies, product Dy^2 visits each NQR twice. Calling the common value $\mathcal{S}_{\mathrm{NQR}}$, we have that

$$\mathcal{S}_{\mathrm{NQR}} + \langle\mathcal{F}\rangle_4 = 2\mathcal{N}.$$

Adding, gives that

4b: $$\mathcal{S}_{\mathrm{QR}} + \mathcal{S}_{\mathrm{NQR}} = 2\sum_{x\neq 0} \left(\frac{1-x}{\mathsf{F}}\right).$$

But $(\frac{1}{\mathsf{F}}) + \sum_{x\neq 0} (\frac{1-x}{\mathsf{F}}) = \sum_x (\frac{1-x}{\mathsf{F}}) = 0$. Thus

4c: $$\mathcal{S}_{\mathrm{QR}} + \mathcal{S}_{\mathrm{NQR}} = -2.$$

Last step. Over F, note $x^2 - 1 = [x-1][x+1]$, and $-1 \neq 1$, since F is odd. So Quad-Legendre-sum Thm (3) informs us that $-1 = \mathcal{S}_1 = \mathcal{S}_{\mathrm{QR}}$. Now (4c) assures that $\mathcal{S}_{\mathrm{NQR}} = -1$. ♦

4d: Corollary. *Using the* $\mathcal{Q}$ *and* $\mathcal{N}$ *from above,*

$$\sum_{w\in\mathrm{QR}} (\tfrac{1-w}{\mathsf{F}}) = \tfrac{1}{2}[-\langle\mathcal{F}\rangle_4 - 1], \quad \sum_{z\in\mathrm{NQR}} (\tfrac{1-z}{\mathsf{F}}) = \tfrac{1}{2}[+\langle\mathcal{F}\rangle_4 - 1] \text{♢}$$

Definition. Recall that the ***discriminant*** of polynomial $g(x) := Ax^2 + Bx + C$ with $A \neq 0$, is $\mathrm{Discr}(g) := B^2 - 4AC$. □

4e: General Quad-LS Thm. *Fix an odd* F *and consider polynomial*

$$g(x) := x^2 + Bx + C, \text{ with } B,C \in \mathsf{F},$$

$$\text{and sum } \mathcal{S}_g := \sum_{x\in\mathsf{F}} \left(\frac{g(x)}{\mathsf{F}}\right).$$

In the algebraic closure $\overline{\mathsf{F}}$, *factor* $g(x)$ *as*

$$g(x) = [x-U][x-V], \text{ with } U,V \in \overline{\mathsf{F}}.$$

Then

$$4e'\text{:}\quad \mathcal{S}_g \;=\; \begin{Bmatrix} \mathcal{F}-1 & ;\text{if } U=V,\ \text{i.e Discr}(g)=0 \\ -1 & ;\text{if } U\neq V,\ \text{i.e Discr}(g)\neq 0 \end{Bmatrix}.$$

So a general $g(x) := Ax^2+Bx+C$ [*where* $A,B,C\in\mathsf{F}$ *with* $A\neq 0$] *thus has*

$$4e''\text{:}\qquad \mathcal{S}_g \;=\; \begin{Bmatrix} [\mathcal{F}-1]\cdot(\frac{A}{\mathsf{F}}) & ;\text{if Discr}(g)=0 \\ -(\frac{A}{\mathsf{F}}) & ;\text{if Discr}(g)\neq 0 \end{Bmatrix}. \quad \Diamond$$

Pf of $(4e')$. Since F is odd, value $\frac{B}{2}$ is well-defined, and $D := [\frac{B}{2}]^2 - C \in \mathsf{F}$. Complete the square to write

$$g(y) \;:=\; [y+\tfrac{B}{2}]^2 \;-\; D\,.$$

Define $h(x) := g(x-\frac{B}{2}) \overset{\text{note}}{=\!=} x^2 - D$.

Our h is a translate of g, so $\mathcal{S}_g = \mathcal{S}_h$. And g has a double-root [in $\overline{\mathsf{F}}$] IFF h does IFF $D=0$. [Thus any $\overline{\mathsf{F}}$-double-root of g already lies in F.] The improvement is that (4a) applies to h. Happily, it yields $(4e')$.

Finally, note $4D = B^2 - 4C = \text{Discr}(g)$. ♦

Remark. George Andrews' text, in Thm 10-1 on P.128, states the following theorem with $\mathsf{F}=\mathbb{Z}_p$ and $\Gamma=1$. His proof works in the following slightly more general context. □

5: Gap-QR Thm. *Fix an odd* F, *and a non-zero "gap"* $\Gamma\in\mathsf{F}$. *Define the set*

$$\mathcal{C} \;:=\; \Big\{ x\in\mathsf{F} \;\Big|\; \textit{Both } x, x-\Gamma \in \text{QR} \Big\}.$$

Let $N := |\mathcal{C}|$. *Then*

$$5\text{a:}\qquad N \;=\; \tfrac{1}{4}\Big[\mathcal{F} - 3 - (\tfrac{\Gamma}{\mathsf{F}}) - (\tfrac{-\Gamma}{\mathsf{F}})\Big].$$

Write $\mathcal{F}$ *as* $4T-1$ *or* $4T+1$ *as* $\mathcal{F}$ *is* 4Neg *or* 4Pos. *Then we can restate* (5a) *as*

$$5\text{b:}\quad \textit{When } \mathcal{F} \textit{ is 4Neg:}\quad N \;=\; T-1\,.$$

$$5\text{c:}\quad \textit{When } \mathcal{F} \textit{ is 4Pos:}\quad N \;=\; T - \tfrac{1}{2}[1+(\tfrac{\Gamma}{\mathsf{F}})]\,. \quad \Diamond$$

Pf. Note $0,\Gamma\notin\mathcal{C}$. Define $\boxed{\mathcal{J} := \mathsf{F}\smallsetminus\{0,\Gamma\}}$. Then

$$4N \;=\; \sum_{x\in\mathcal{J}} \Big[1+\Big(\frac{x}{\mathsf{F}}\Big)\Big]\cdot\Big[1+\Big(\frac{x-\Gamma}{\mathsf{F}}\Big)\Big],$$

since, for each $x\in\mathcal{J}$, both $(\frac{x}{\mathsf{F}})$ and $(\frac{x-\Gamma}{\mathsf{F}})$ lie in $\{\pm1\}$.

As $|\mathcal{J}| = \mathcal{F}-2$, we get that $4N$ equals

$$*\text{:}\quad [\mathcal{F}-2] + \underbrace{\sum_{x\in\mathcal{J}}(\tfrac{x}{\mathsf{F}})}_{U} + \underbrace{\sum_{x\in\mathcal{J}}(\tfrac{x-\Gamma}{\mathsf{F}})}_{V} + \underbrace{\sum_{x\in\mathcal{J}}(\tfrac{x}{\mathsf{F}})(\tfrac{x-\Gamma}{\mathsf{F}})}_{\mathcal{S}}.$$

Evidently $(\frac{\Gamma}{\mathsf{F}}) + U = \sum_{x\neq 0}(\frac{x}{\mathsf{F}}) = 0$, since F is odd. Consequently $U = -(\frac{\Gamma}{\mathsf{F}})$.

Similarly, $(\frac{-\Gamma}{\mathsf{F}}) + V = \sum_{x\neq 0}(\frac{x}{\mathsf{F}}) = 0$; so $V = -(\frac{-\Gamma}{\mathsf{F}})$.

Computing $\mathcal{S}$. Let $g(x) := x\cdot[x-\Gamma]$. Then $\mathcal{S}$ equals $\sum_x (\frac{g(x)}{\mathsf{F}})$. Since g has distinct roots, both in F, the Quad-Legendre-sum Thm (3) says that $\mathcal{S} = -1$.

Plugging the values for $U, V, \mathcal{S}$ into $(*)$ will produce the claimed (5a). ♦

Filename: `Problems/NumberTheory/legendre-sym.finite-field.latex`
As of: *Tuesday 03Jun2014.* Typeset: *1Mar2023 at 12:15.*