Gauss's Quadratic Reciprocity Theorem : NumThy

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
25 July, 2016 (at *20:31*)

1: *Nomenclature.* For odd D, use H_D to mean $\frac{D-1}{2}$. (The H is to suggest "Half".)

In the sequel, p is an odd prime and $S \perp p$ is the "stridelength"; we will walk around the circumference=p circle using strides of length S.

Use $H := H_p$ and $\langle x\rangle := \langle x\rangle_p$ for the *symmetric* residue of integer x modulo p; so $\langle x\rangle$ is in $[-H\,..\,H]$. Let $\equiv$ mean $\equiv_p$.

Let $\mathcal{G}=\mathcal{G}_p(S)$ be the set of indices $\ell \in [1\,..\,H]$ such that $\langle \ell\cdot S\rangle_p$ is neGative. Letting $\mathcal{P}$ be the indices with $\langle \ell\cdot S\rangle$ Positive, we have that (disjointly)

$$\mathcal{G} \sqcup \mathcal{P} \;=\; [1\,..\,H]\,.$$

Finally, use $\mathcal{N} = \mathcal{N}_p(S)$ for the number of "negative" indices; $\mathcal{N} := {}^{\#}\mathcal{G}$. □

2: Prop'n. *Fix an $S \perp p$, with notation from (1). Then the mapping (absolute-value of symm-residue)*

$$\ell \;\mapsto\; \big|\langle \ell\cdot S\rangle\big|\,,$$

is a ***permutation*** *of $[1\,..\,H]$. We say that the mapping $\ell \mapsto \langle \ell\cdot S\rangle$ is a "permutation up to sign" of $[1\,..\,H]$.* ◊

Proof. Given indices $1 \leqslant \ell \leqslant k \leqslant H$, we want that either equality $\mp\langle \ell\cdot S\rangle = \langle k\cdot S\rangle$ forces $\ell = k$.

For either choice of sign in $\mp$, note that

$$\begin{aligned} \mp\langle \ell\cdot S\rangle = \langle k\cdot S\rangle \qquad &\text{IFF} \qquad 0 \equiv [k\pm\ell]\cdot S \\ &\text{IFF} \qquad 0 \equiv k\pm\ell\,, \end{aligned}$$

since $S \perp p$. Thus

$$0 \;\leqslant\; k\pm\ell \;\leqslant\; 2H \;<\; p\,.$$

Together with $k\pm\ell \equiv 0$, this forces $k\pm\ell$ to actually *be* zero. Thus the "±" is a minus sign, and $k = \ell$. ♦

3: Gauss Lemma. *Fix an odd prime p and integer $S \perp p$. Then the Legendre symbol $\left(\frac{S}{p}\right)$ satisfies*

$$\left(\tfrac{S}{p}\right) \;=\; [-1]^{\mathcal{N}}\,.$$ ◊

Proof of Gauss Lemma. Necessarily

$$4\text{:}\quad \prod_{\ell=1}^{H} \langle \ell\cdot S\rangle \;\equiv\; \prod_{\ell=1}^{H} \ell\cdot S \;=\; H!\cdot S^H \;\equiv\; H!\cdot\left(\frac{S}{p}\right),$$

with the last step following from LSThm. Observe that $\langle \ell\cdot S\rangle$ equals $\pm\big|\langle \ell S\rangle\big|$ as ℓ is-not/is in $\mathcal{G}$. Prop'n 2, consequently, tells us that LhS(4) can be written as $H!$ times $[-1]^{\mathcal{N}}$. Thus RhS(4) equals

$$H!\cdot\left(\tfrac{S}{p}\right) \;\equiv\; H!\cdot[-1]^{\mathcal{N}}\,.$$

The $H!$, being co-prime to p, cancels mod-p to hand us congruence $\left(\frac{S}{p}\right) \equiv [-1]^{\mathcal{N}}$. ♦

An important application is the following.

5: Two-is-QR Lemma. *Consider an oddprime p. Then 2 is a p-QR IFF $p \equiv_8 \pm 1$.* ◊

Abbrev. An odd integer D is ***8Near*** if $D \equiv_8 \pm 1$; it is ***8Far*** if $D \equiv_8 \pm 3$. [The names come from being, mod 8, near/far from zero.] □

Proof. Call p "good" if 2 is a p-QR. As usual, let $H := \frac{p-1}{2}$. It is easy to check that

$$\begin{aligned} \dagger\text{:} \qquad &\text{Even } H \iff p \equiv_8 \{+1,-3\}\,; \\ \ddagger\text{:} \qquad &\text{Odd } H \iff p \equiv_8 \{-1,+3\}\,. \end{aligned}$$

Evidently, $\mathcal{G}=\mathcal{G}_p(2)$ is the set

$$\left\{\lceil\tfrac{H+1}{2}\rceil, \ldots, H-1, H\right\}.$$

In counting this set, $\mathcal{N} := {}^{\#}\mathcal{G}$, we have two cases.

CASE: H is even Here, $\mathcal{N} = [H - \frac{H+2}{2}] + 1 = \frac{H}{2}$.

CASE: H is odd So $\mathcal{N} = [H - \frac{H+1}{2}] + 1 = \frac{H+1}{2}$.

The Gauss lemma directs us to examine $\mathcal{N}$ mod-2.

Case: H is even. Courtesy (†) we can write p as $8L + \{1,-3\}$, with $L\in\mathbb{Z}$. Thus

$$H \;=\; \frac{8L + \{1,-3\} - 1}{2} \;=\; 4L + \{0,-2\}\,.$$

So $\mathcal{N} = \frac{H}{2} = 2L + \{0,-1\}$. Consequently,

$$p \text{ good} \iff \mathcal{N} \equiv_2 0 \iff H \equiv_4 0 \iff p \equiv_8 1\,.$$

Case: H is odd. We can write $p = 8L + \{-1, +3\}$. Thus

$$H+1 \;=\; \frac{8L + \{-1,+3\} - 1}{2} + 1 \;=\; 4L + \{0, 2\}\,.$$

So $\mathcal{N} = \frac{H+1}{2} = 2L + \{0, 1\}$. Consequently,

$$p \text{ good} \iff \mathcal{N} \equiv_2 0 \iff H+1 \equiv_4 0 \iff p \equiv_8 -1\,.$$

This gives the theorem. ♦

The Wrapping function. Count "full ***Wraps***",

$$\mathcal{W} = \mathcal{W}_p(S) \;:=\; \sum_{\ell=1}^{H_p} \left\lfloor \frac{\ell \cdot S}{p} \right\rfloor,$$

when walking around the circle with stridelength S. (Here, $\lfloor\cdot\rfloor$ is the floor function.)

6: Eisenstein Lemma. *Fix $S \perp p$ from (1), with S odd. Then $\mathcal{N}$ and $\mathcal{W}$ are either both even or both odd. I.e.*

$$\mathcal{N}_p(S) \;\equiv_2\; \mathcal{W}_p(S)\,.$$ ◊

Proof of Eisenstein Lemma. Let $r_\ell := \langle \ell \cdot S \rangle_p$, Then

$$\ell \cdot S \;=\; p \cdot \left\lfloor \frac{\ell \cdot S}{p} \right\rfloor + \begin{Bmatrix} r_\ell & \text{if } \ell \in \mathcal{P} \\ p + r_\ell & \text{if } \ell \in \mathcal{G} \end{Bmatrix}.$$

Summing this over ℓ produces

$$7\text{:}\quad S \cdot \sum_{\ell=1}^{H} \ell \;=\; p\cdot\mathcal{W} + \left[\sum_{\ell\in\mathcal{P}} r_\ell\right] + p\cdot\mathcal{N} + \left[\sum_{\ell\in\mathcal{G}} r_\ell\right].$$

On $[1\,..\,H]$, recall that $\ell \mapsto r_\ell$ is a permutation up to sign. Thus

$$7'\text{:}\qquad \sum_{\ell=1}^{H} \ell \;=\; \left[\sum_{\ell\in\mathcal{P}} r_\ell\right] - \left[\sum_{\ell\in\mathcal{G}} r_\ell\right].$$

Subtracting equations, $(7) - (7')$, yields that

$$8\text{:}\quad [S-1] \cdot \sum_{\ell=1}^{H} \ell \;=\; p\mathcal{W} + p\mathcal{N} + 2 \cdot \sum_{\ell\in\mathcal{G}} r_\ell\,.$$

But S is odd, so $S - 1 \equiv_2 0$. Reducing each side mod 2, then, gives

$$\begin{aligned} 8'\text{:}\qquad 0 \;&\equiv_2\; p\cdot[\mathcal{W}+\mathcal{N}] + 0 \\ &\equiv_2\; \mathcal{W}+\mathcal{N}\,, \quad \text{since } p \text{ is odd.} \end{aligned}$$

Thus $\mathcal{W} \equiv_2 \mathcal{N}$, as desired. ♦

9: The Quadratic Reciprocity Theorem. *For odd-primes p and q:*

$$9'\text{:}\qquad \left(\frac{q}{p}\right) \;=\; \left(\frac{p}{q}\right) \cdot \big[-1\big]^{H_p \cdot H_q}\,.$$

When $p \neq q$ then we can write in a visually more symmetric way as

$$9''\text{:}\qquad \left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) \;=\; \big[-1\big]^{H_p \cdot H_q}\,.$$

Equivalently, $\left(\frac{q}{p}\right)$ equals $\left(\frac{p}{q}\right)$ unless both p and q are 4NEG primes; in that case, the Legendre symbols are negatives of each other. ◊

Partial Proof of (9″). Eisenstein uses a geometric argument –essentially decomposing a rectangle into two triangles– to show that

$$10\text{:}\qquad \mathcal{W}_p(q) + \mathcal{W}_q(p) \;=\; H_p \cdot H_q\,.$$

Then the Eisenstein Lemma shows that LhS(10) has the same parity as $\mathcal{N}_p(q) + \mathcal{N}_q(p)$, i,e,

$$10'\text{:}\qquad \mathcal{N}_p(q) + \mathcal{N}_q(p) \;\equiv_2\; H_p \cdot H_q\,.$$

Applying the Gauss Lemma now establishes (9″). ♦

Legendre/Jacobi Symbol

Consider a posint N and an integer $k \perp N$. This k is an N-***QR***, an N–quadratic-residue, if *there exists* an integer x with $x^2 \equiv_N k$; otherwise, this k is an N-***nonQR***. In contrast, if $k \not\perp N$, then k is *neither* a QR nor a nonQR.

For p prime, the ***Legendre Symbol***

$$\left(\frac{k}{p}\right) \;:=\; \begin{Bmatrix} 0 & \text{if } k \bullet\!\!| \; p \\ +1 & \text{if } k \text{ is a } p\text{-QR} \\ -1 & \text{if } k \text{ is a } p\text{-nonQR} \end{Bmatrix}.$$

I pronounce $\left(\frac{k}{p}\right)$ as "k legendre p". Below, I use $\langle\cdot\rangle_N$ for the **symmetric** residue mod N.

11: Legendre-Symbol Thm (LSThm). *For all odd-primes p and all integers K, k_ℓ, k', we have:*

A: If $k \perp p$: Our k is a p-QR IFF $\left(\frac{k}{p}\right) = 1$. [By defn.]

B: $$\left(\frac{K}{p}\right) \;=\; \left\langle K^{\frac{p-1}{2}} \right\rangle_p \,.$$

Furthermore

i: LS is "top multiplicative":

$$\left(\frac{k_1 \cdot k_2 \cdot \ldots \cdot k_L}{p}\right) \;=\; \left(\frac{k_1}{p}\right) \cdot \left(\frac{k_2}{p}\right) \cdot \ldots \cdot \left(\frac{k_L}{p}\right) .$$

ii: If $k' \equiv_p k$ then $\left(\frac{k'}{p}\right) = \left(\frac{k}{p}\right)$. ◊

Pf of (B). Use the involution $x \mapsto \frac{K}{x}$ on $\Phi(p)$. Etc.. ♦

Pf of (i). Note RhS(B) is [totally] multiplicative in K. Hence LhS(B) is multiplicative in K. ♦

Defn of Jacobi Symbol. Factoring a posodd N into primes, $N = p_1 \cdot p_2 \cdots p_L$, define the ***Jacobi Symbol*** by

$$\left(\frac{k}{N}\right) \;:=\; \left(\frac{k}{p_1}\right) \cdot \left(\frac{k}{p_2}\right) \cdots \left(\frac{k}{p_L}\right) ,$$

where k is an arbitary integer. □

12: *Commentary.* Properties (14ii,iii,iv), below, will give a lightning-bolt (ie, Euclidean) algorithm for rapidly computing Jacobi-Symbols; the QRecip property of JS is the primary reason for generalizing LS. *However, something is lost* in the process:

For example, $\left(\frac{2}{9}\right) = 1$, yet certainly 2 is **not** a 9-QR, since 2 is not a 3-QR.

Also, $2^{H_9} = 2^4 \equiv_9 -2$. So the symm-residue $\langle 2^{H_9} \rangle_9$ **doesn't equal** ± 1, let alone answer whether 2 is a 9-QR. Similarly, $[-1]^{H_9} = 1$. So the value **is** in $\{\pm 1\}$, but the answer is *wrong*: Negative-one is a 9-nonQR, since -1 is a 3-nonQR. □

13: Prop'n. *For odd integers d and e:*

$$H_d + H_e \;\equiv_2\; H_{d\cdot e} \,.$$ ◊

Proof. Write $d = 1 + 2A$ and $e = 1 + 2B$. The product de equals $4AB + 2A + 2B + 1$. Thus

$$H_{d\cdot e} \;=\; 2AB + A + B \;\equiv_2\; A + B \;\overset{\text{note}}{=\!=}\; H_d + H_e \,.$$ ♦

14: Jacobi-Symbol Thm (JSThm). *For all posodd N, D, d_j, and all integers K, k_ℓ, k':*

A: For each $k \perp N$: k is an N-QR IFF

Every prime $p \bullet\!\!| N$ has $\left(\frac{k}{p}\right) = 1$.

Moreover

i: JS is "multiplicative, top and bottom":

$$\left(\frac{k_1 \cdot k_2 \cdot \ldots \cdot k_L}{N}\right) \;=\; \left(\frac{k_1}{N}\right) \cdot \left(\frac{k_2}{N}\right) \cdot \ldots \cdot \left(\frac{k_L}{N}\right) \quad \textit{and}$$

$$\left(\frac{K}{d_1 \cdot d_2 \cdot \ldots \cdot d_J}\right) \;=\; \left(\frac{K}{d_1}\right) \cdot \left(\frac{K}{d_2}\right) \cdot \ldots \cdot \left(\frac{K}{d_J}\right) .$$

ii: If $k' \equiv_N k$ then $\left(\frac{k'}{N}\right) = \left(\frac{k}{N}\right)$.

iii: These Jacobi-symbols satisfy:

$$\left(\frac{2}{N}\right) \;=\; \left\{ \begin{matrix} +1 & \text{if } N \equiv_8 \pm 1 \\ -1 & \text{if } N \equiv_8 \pm 3 \end{matrix} \right\} .$$

$$\left(\frac{-1}{N}\right) \;=\; \left\{ \begin{matrix} +1 & \text{if } N \equiv_4 +1 \\ -1 & \text{if } N \equiv_4 -1 \end{matrix} \right\} .$$

iv: QReciprocity: For n and d posodd,

$$\left(\frac{d}{n}\right) \;=\; \left(\frac{n}{d}\right) \cdot [-1]^{H_d \cdot H_n} \,.$$ ◊

Pf of (14A). Fix a prime $p \bullet\!\!| N$. Take r, a mod-p sqroot of k. Let $\mathbf{E} \in \mathbb{Z}_+$ be largest st. $p^{\mathbf{E}} \bullet\!\!| N$. Use Hensel's lemma to lift r to s_p, a mod-$p^{\mathbf{E}}$ sqroot of k. [Details: Our r is a mod-p root of $f(x) := x^2 - k$. Now $f'(r) \overset{\text{note}}{=\!=} 2r$ is not divisible by p, since p is odd. Thus Hensel's says this root can be lifted to a mod p^2 root, which can be lifted to a mod p^3 root, ..., indefinitely.[♡1]]

For each $p \bullet\!\!| N$, let s_p be a mod-p sqroot of k. Use CRThm[♡2] to suture together the $\{s_p \mid p \bullet\!\!| N\}$ values into a mod-N sqroot of k. ♦

[♡1] Fix $V \in [0\,..\,p)$ with $V \equiv_p f'(r)$. For a posint ℓ, suppose r_ℓ is mod-p^ℓ sqroot of k. Compute the integer $m_\ell := -f(r_\ell)/p^\ell$. Now doing division mod p, compute $t_\ell \in [0\,..\,p)$ st. $t_\ell \cdot V \equiv_p m_\ell$. Then $r_\ell + [t_\ell \cdot p^\ell]$ is mod-$p^{\ell+1}$ sqroot of k.

[♡2] The Chinese Remainder Theorem.

Pf (14iii). Let $\langle\cdot\rangle$ and $\equiv$ mean symm-residue mod 8.

Our Two-is-QR Lemma implies that $\left(\frac{2}{N}\right) = -1$ IFF N has *oddly many* 8Far primes in its factorization.

OTOHand, $\langle N\rangle$ is the product of $\langle p\rangle$ over these primes. And for each two values in $\{\pm 3\}$, the product is congruent to ± 1. So $\langle N\rangle = \pm 3$ IFF N has *oddly* many 8Far primes in its factorization. ♦

Pf (14iv). If $d \not\perp n$ then both $\left(\frac{d}{n}\right)$ and $\left(\frac{n}{d}\right)$ are zero. So establishing

$$\dagger: \qquad \left(\tfrac{d}{n}\right)\cdot\left(\tfrac{n}{d}\right) \stackrel{?}{=} [-1]^{H_d\cdot H_n}$$

will suffice, since WLOG $d \perp n$.

Lets prove the following.

‡: *Suppose each of d and e satisfies (†) w.r.t n. Then their product $d\cdot e$ satisfies (†) w.r.t n.*

Applying (†) twice, and mult. top and bottom,

$$\begin{aligned}\left(\frac{de}{n}\right)\cdot\left(\frac{n}{de}\right) &= \left(\frac{d}{n}\right)\left(\frac{e}{n}\right)\cdot\left(\frac{n}{d}\right)\left(\frac{n}{e}\right)\\ &= \left(\frac{d}{n}\right)\left(\frac{n}{d}\right)\cdot\left(\frac{e}{n}\right)\left(\frac{n}{e}\right)\\ &= [-1]^{H_d\cdot H_n}\cdot[-1]^{H_e\cdot H_n}.\end{aligned}$$

The combined exponent is $H_dH_n + H_eH_n$. ie.,

$$\left(\tfrac{de}{n}\right)\cdot\left(\tfrac{n}{de}\right) = [-1]^{[H_d+H_e]\cdot H_n}.$$

And Prop'n 13 says that the RhS equals $[-1]^{H_{de}\cdot H_n}$.

Inducting twice. W.r.t. a posodd N, say that posodd d is "N-good" if

$$£: \qquad \left(\tfrac{d}{N}\right) = \left(\tfrac{N}{d}\right)\cdot[-1]^{H_d\cdot H_N}.$$

Having established (‡), we have this:

¥: *For each posodd N, the set of N-good numbers is sealed (closed) under multiplication.*

Fixing a prime N, the QReciprocity Thm, in form (9′), tells us that every prime, d, is N-good. By (¥), then: *Every posodd d is N-good.*

But (£) is symmetric in N & d. So we can restate our accomplishment as: *W.r.t. each posodd d, every prime N is d-good.* Applying (¥) again, now says that every posodd N is d-good. ♦

1st Application of LST+QRecip. Fix an $N \in \mathbb{Z}$. We seek a characterization of those odd-primes $p \perp N$, for which $N \in \mathrm{QR}_p$. Say k is ***5Near*** if $k \equiv_5 \pm 1$, and k is ***5Far*** if $k \equiv_5 \pm 2$.

15: Thm. *Prime $p \neq 5$ has $\mathrm{QR}_p \ni 5$ IFF p is 5Near.* ◊

Proof. Since 5 is 4Pos, we have $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$

Unfinished: as of 25Jul2016 ♦

2nd Application of LST+QRecip. We will show:

16a: *For each $n \geqslant 2$, integer $[n^3-1]$ has a* 3Pos *prime factor.*

Note, $n^3 - 1 = [n-1][n^2+n+1]$ where We will prove this stronger statement:

16b: Thm. *Let $T_n := n^2+n+1$, and define*

$$\mathcal{C}_n := \left\{ p \bullet\!\!| \; T_n \;\middle|\; p \text{ is prime, and } p \notin \{2,3\} \right\}.$$

Every $\mathcal{C}_n$-prime is 3Pos. *And for $n \geqslant 2$, collection $\mathcal{C}_n$ is not empty* ◊

Pf of 3Posness. ISTShow that $p \in$ 3Pos, where p is an arbitrary non-2,3 prime p that divides

$$*: \qquad F_n := 4T_n \stackrel{\text{note}}{=\!=} [2n+1]^2 + 3.$$

Now $F_n \equiv_p 0$, so $(*)$ says $[-3]$ is a mod-p square. By hyp, $-3 \perp p$, so $-3 \in \mathrm{QR}_p$, i.e

$$\begin{aligned}1 = \left(\tfrac{-3}{p}\right) &\stackrel{\text{LST}}{=\!=} \left(\tfrac{-1}{p}\right)\cdot\left(\tfrac{3}{p}\right)\\ &\stackrel{\text{LST+QRecip}}{=\!=\!=} [-1]^{\frac{p-1}{2}}\cdot\left[[-1]^{\frac{p-1}{2}}\left(\tfrac{p}{3}\right)\right] = \left(\tfrac{p}{3}\right).\end{aligned}$$

But the *only* 3-QR is 1. So p is 3Pos. ♦

Pf $\mathcal{C}_n \neq \varnothing$. Fix $n \geqslant 2$. FTSOC suppose $\mathcal{C}_n$ is empty. Since T_n is odd, this implies that $T_n = 3^k$, for some $k \geqslant 2$; this last, since $T_n > T_1 = 3^1$. So $\boxed{F_n = 4\cdot 3^k}$.

Since $F_n \equiv_3 0$, our $(*)$ says that $[2n+1]^2 \not\bullet 3$. Courtesy FTA, $[2n+1] \not\bullet 3$. Thus, $[2n+1]^2 \equiv_9 0$.

Recall that $k \geqslant 2$, whence $F_n \equiv_9 0$. So $(*)$ implies that $0 \equiv_9 3$, which is false. Hence $\mathcal{C}_n$ is non-void. ♦

E11: For what *negative* integers n do we have (16a)? Or have (16b)?

Filename: `Problems/NumberTheory/quad-reciprocity.latex`
As of: *Sunday 01Jun2014.* Typeset: *25Jul2016 at 20:31.*