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/
27 July, 2018 (at 21:40)

1: Nomenclature. For odd \( D \), use \( H_D \) to mean \( \frac{D-1}{2} \).
\( (\text{The } H \text{ is to suggest “Half”}) \)
In the sequel, \( p \) is odd prime and \( S \perp p \) is the “stride-length”; 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)
\[
\mathcal{G} \cup \mathcal{P} = [1..H]. \quad (\text{The “Time” set.})
\]
Finally, use \( N := N_p(S) \) for the number of “negative” indices; \( N := \# \mathcal{G} \).
\[ \square \]

2: Prop’n. Fix an \( S \perp p \), with notation from (1). Then the mapping \( \langle \text{absolute-value of symm-residue} \rangle \)
\[
\ell \mapsto |\langle \ell \cdot S \rangle|,
\]
is a permutation of \([1..H] \). Mapping \( \ell \mapsto \langle \ell \cdot S \rangle \) is a “permutation up to sign” of \([1..H] \).
\[ \diamond \]

Proof. Given indices \( 1 \leq k \leq \ell \leq H \), we want that either equality \( \mp \langle k \cdot S \rangle = \langle \ell \cdot S \rangle \) forces \( k = \ell \).
For either choice of sign in \( \mp \), note that
\[
\mp \langle k \cdot S \rangle = \langle \ell \cdot S \rangle \iff 0 \equiv [\ell \pm k] \cdot S \iff 0 \equiv \ell \pm k,
\]
since \( S \perp p \). Thus
\[
0 \leq \ell \pm k \leq 2H < p.
\]
Together with \( \ell \pm k \equiv 0 \), this forces \( \ell \pm k \) to actually be zero. Thus the “\( \pm \)” is a minus sign, and \( \ell = k \).
\[ \diamond \]

3: Gauss Lemma. Fix an odd prime \( p \) and integer \( S \perp p \). Then the Legendre symbol \( \langle S \rangle_p \) satisfies
\[
\langle S \rangle_p = [-1]^N_p.
\]
\[ \diamond \]

\( \text{Pf of Gauss Lemma.} \) Let \( N := N_p(S) \). Necessarily
\[
*: \prod_{\ell=1}^{H} \langle \ell \cdot S \rangle \equiv \prod_{\ell=1}^{H} \ell \cdot S = H! \cdot S^H \equiv H! \cdot \left( \frac{S}{p} \right),
\]
with the last step following from LSThm. Observe that \( \langle \ell \cdot S \rangle \) equals \( \pm \langle \ell(S) \rangle \) as \( \ell \) is not/is in \( \mathcal{G} \).
Prop’n 2, consequently, tells us that LhS(\( * \)) can be written as \( H! \) times \([-1]^N \). Thus RhS(\( * \)) equals
\[
H! \cdot \left( \frac{S}{p} \right) \equiv H! \cdot [-1]^N.
\]
The \( H! \), being co-prime to \( p \), cancels mod-\( p \) to hand us congruence \( \left( \frac{S}{p} \right) \equiv [-1]^N \).
\[ \diamond \]

An important application is the following.

4: Two-is-QR Lemma. Consider an odd prime \( p \). Then \( 2 \) is a \( p \)-QR IFF \( p \equiv \pm 1 \).
\[ \diamond \]

Abbrev. An odd integer \( D \) is \textbf{8Near} if \( D \equiv \pm 1 \); it is \textbf{8Far} if \( D \equiv \pm 3 \). [The names come from being, mod 8, near/far from zero.]
\[ \square \]

Proof. Call \( p \) “good” if \( 2 \) is a \( p \)-QR. As usual, let \( H := \frac{p-1}{2} \). It is easy to check that
\[
\uparrow: \quad \text{Even } H \iff p \equiv \pm \{+1,-3\}; \quad \downarrow: \quad \text{Odd } H \iff p \equiv \pm \{-1,+3\}.
\]
Let \( \mathcal{G} := \mathcal{G}_p(2) \). Computing \( N := |\mathcal{G}| \) has two cases:
\[
|\text{Case: } H \text{ is even} | \quad \text{Here, } N = [H - H^2 + 1] + 1 = \frac{H}{2}, \quad \text{since } \mathcal{G} = \{H/2, H/2, \ldots, H\}.
\]
\[
|\text{Case: } H \text{ is odd} | \quad \text{So } N = [H - H^2 + 1] + 1 = \frac{H+1}{2}, \quad \text{since } \mathcal{G} = \{H/-2, H/2, \ldots, H\}.
\]
The Gauss lemma directs us to examine \( N \) mod-2.

\textbf{CASE: } H \text{ is even.} Courtesy (\( \uparrow \)) we can write \( p \) as
\[
8L + \{1,-3\}, \quad \text{with } L \in \mathbb{Z}. \quad \text{Thus}
\]
\[
H = \frac{8L + \{1,-3\} - 1}{2} = 4L + \{0,-2\}.
\]
So \( N = \frac{H}{2} = 2L + \{0,-1\} \). Consequently,
\[
p \text{ good } \iff N \equiv 2 \iff H \equiv 0 \iff p \equiv 1.
\]
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 \( N = \frac{H + 1}{2} = 2L + \{0, 1\} \). Consequently,
\[
p \text{ good } \iff N \equiv 2 \iff H + 1 \equiv 4 \iff p \equiv 2 - 1.
\]
This gives the lemma.

The Wrapping function. Count “full Wraps”,
\[
W = W_p(S) := \sum_{\ell=1}^{H} \left\lfloor \frac{\ell \cdot S}{p} \right\rfloor,
\]
when walking around the circle with stridelength \( S \).
(Here, \( \lfloor \cdot \rfloor \) is the floor function.)

5: Eisenstein Lemma. Fix \( S \perp p \) from (1), with \( S \text{ odd} \). Then \( N \) and \( W \) are either both even or both odd. I.e.
\[
N_p(S) \equiv 2 \iff W_p(S).
\]

Proof of Eisenstein Lemma. Let \( r_\ell := \langle \ell \cdot S \rangle_p \). Then
\[
\ell \cdot S = p \cdot \left\lfloor \frac{\ell \cdot S}{p} \right\rfloor + \begin{cases} r_\ell & \text{if } \ell \in \mathcal{P} \\ p + r_\ell & \text{if } \ell \in \mathcal{G} \end{cases}.
\]
Summing this over \( \ell \) produces
\[
S \cdot \sum_{\ell=1}^{H} \ell = \sum_{\ell \in \mathcal{P}} r_\ell + p \cdot N + \sum_{\ell \in \mathcal{G}} r_\ell.
\]
On \([1..H]\), recall that \( \ell \mapsto r_\ell \) is a permutation up to sign. Thus
\[
6': \sum_{\ell=1}^{H} \ell = \sum_{\ell \in \mathcal{P}} r_\ell - \sum_{\ell \in \mathcal{G}} r_\ell.
\]
Subtracting equations, (6) – (6'), yields that
\[
7': (S - 1) \sum_{\ell=1}^{H} \ell = p \cdot W + p \cdot N + 2 \cdot \sum_{\ell \in \mathcal{G}} r_\ell.
\]
But \( S \) is odd, so \( S - 1 \equiv 0 \). Reducing each side mod 2, then, gives
\[
7': 0 \equiv 2 \cdot p \cdot \lfloor W + N \rfloor + 0
\]
\[
\equiv 2 \cdot W + N, \quad \text{since } p \text{ is odd}.
\]
Thus \( W \equiv 2 \cdot N \), as desired.

Filename: Problems/NumberTheory/quad-reciprocity.latex
Fig. 1: Here, $p=17$ and $q=13$. Note: The diagonal of $(0, H_p) \times (0, H_q)$ has no lattice-points, since $p \perp q$.

Triangle $B$ contains $W_p(q)$ many lattice-pts because, traveling vertically from point $(k, 0)$, one passes through $\lfloor k \cdot \frac{q}{p} \rfloor$ many lattice-pts until reaching the diagonal line. Similarly, triangle $A$ has $W_q(p)$ lattice-points. Hence $W_p(q) + W_q(p) = H_p \cdot H_q$.

**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 $x^2 \equiv_k N$; 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**

$$\left( \frac{k}{p} \right) := \begin{cases} 0 & \text{if } k \mid p \\ +1 & \text{if } k \text{ is a } p\text{-QR} \\ -1 & \text{if } k \text{ is a } p\text{-nonQR} \end{cases}. $$

I pronounce $(\frac{k}{p})$ as “$k$ legendre $p$”. Below, I use $(\cdot)_N$ for the **symmetric** residue mod $N$.

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

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

**B:** $\left( \frac{K}{p} \right) = \left( \frac{p-1}{2} \right)^{\frac{p-1}{2}}.$

Furthermore

**i:** $LS$ is “top multiplicative”:

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

**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 arbitrary integer. ☐

11: Commentary. Properties (13ii,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, \( \left( \frac{2}{3} \right) = 1 \), yet certainly 2 is not a 9-QR, since 2 is not a 3-QR.

Also, \( 2^{H_0} = 4 \equiv_3 -2 \). So the symm-residue \( \langle 2^{H_0}_0 \rangle \) doesn’t equal \( \pm 1 \), let alone answer whether 2 is a 9-QR. Similarly, \( [-1]^{H_0} = 1 \). So the value \( \mathbf{is} \) in \( \{ \pm 1 \} \), but the answer \( \mathbf{is} \) wrong: Negative-one is a 9-QR, since \(-1\) is a 3-nonQR.

12: Prop’n. For odd integers \( d \) and \( e \):
\[
H_d + H_e \equiv_2 H_{d,e}. \tag*{◊}
\]

Proof. Write \( d = 1 + 2A \) and \( e = 1 + 2B \). The product \( de \) equals \( 4AB + 2A + 2B + 1 \). Thus
\[
H_{d,e} = 2AB + A + B \equiv_2 A + B \ \text{note} \ H_d + H_e. \tag*{♣}
\]

13: Jacobi-Symbol Thm (JSThm). For all posodd \( N, D, d, j \), and all integers \( K, K_j, K' \):

A: For each \( k \perp N: \ k \) is an \( N \)-QR IFF
\[
\text{Every prime} \ p \nmid N \ \text{has} \ \left( \frac{k}{p} \right) = 1.
\]
Moreover

\[ i: \ \text{JS is “multiplicative, top and bottom”}: \]
\[
\left( \frac{k_1 \cdots k_j}{N} \right) = \left( \frac{k_1}{N} \right) \cdot \cdots \cdot \left( \frac{k_j}{N} \right) \quad \text{and} \quad \left( \frac{K}{d_1 \cdots d_j} \right) = \left( \frac{K}{d_1} \right) \cdot \cdots \cdot \left( \frac{K}{d_j} \right).
\]

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

iii: These Jacobi-symbols satisfy:
\[
\left( \frac{2}{N} \right) = \begin{cases} 
+1 & \text{if } N \equiv_8 \pm 1 \\
-1 & \text{if } N \equiv_8 \pm 3 
\end{cases}.
\]
\[
\left( \frac{-1}{N} \right) = \begin{cases} 
+1 & \text{if } N \equiv_4 1 \\
-1 & \text{if } N \equiv_4 -1 
\end{cases}.
\]

iv: QReciprocity: For \( n \) and \( d \) posodd,
\[
\left( \frac{d}{n} \right) = \left( \frac{n}{d} \right) (-1)^{H_d \cdot H_n}. \tag*{◊}
\]

Pf of (13A). Fix a prime \( p \nmid N \). Take \( r \), a mod-\( p \) sqroot of \( k \). Let \( E \in \mathbb{Z}_+ \) be largest st. \( p^E \nmid N \). Use Hensel’s lemma to lift \( r \) to \( s_p \), a mod-\( p^E \) sqroot of \( k \). [Details: Our \( r \) is a mod-\( p \) root of \( f(x) := x^2 - k \). Now \( f'(r) \) 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.] ☞

For each \( p \nmid N \), let \( s_p \) be a mod-\( p \) sqroot of \( k \). Use CRThm ☞ to suture together the \( \{ s_p \mid p \nmid N \} \) values into a mod-\( N \) sqroot of \( k \).

Pf (13iii). Let \( \langle \cdot \rangle \) and \( \equiv \) mean symm-residue mod 8.

Our Two-is-QR Lemma implies that \( \langle \frac{2}{N} \rangle = -1 \) 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 \( \pm 1 \). So \( \langle N \rangle = \pm 1 \) IFF \( N \) has oddly many 8Far primes in its factorization. ☞

Pf (13iv). If \( d \not\parallel n \) then both \( \left( \frac{d}{n} \right) \) and \( \left( \frac{n}{d} \right) \) are zero. So establishing
\[
\hat{\dagger}: \quad \left( \frac{d}{n} \right) \cdot \left( \frac{n}{d} \right) \equiv \ Advertisement will suffice, since WLOG \( d \perp n \).

Lets prove the following.
\[
\hat{\dagger}: \quad \text{Suppose each of} \ d \ e \ \text{satisfies} \ (\hat{\dagger}) \ \text{w.r.t} \ n. \quad \text{Then their product} \ d \cdot e \ \text{satisfies} \ (\hat{\dagger}) \ \text{w.r.t} \ n.
\]

\footnote{Fix \( V \in [0..p) \) with \( V \equiv f'(r) \). For a posint \( \ell \), suppose \( r_\ell \) is mod-\( p^\ell \) 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 \( k \).}

\footnote{The Chinese Remainder Theorem.}
Applying (†) twice, and mult. top and bottom,
\[
\left( \frac{de}{n} \right) \cdot \left( \frac{n}{de} \right) = \left( \frac{d}{n} \right) \left( \frac{e}{n} \right) \cdot \left( \frac{n}{d} \right) \left( \frac{n}{e} \right) = \left( \frac{d}{n} \right) \left( \frac{n}{d} \right) \cdot \left( \frac{e}{n} \right) \left( \frac{n}{e} \right) = \left[ -1 \right]^{H_d H_n} \cdot \left[ -1 \right]^{H_e H_n}.
\]
The combined exponent is \( H_d H_n + H_e H_n \), i.e.,
\[
\left( \frac{de}{n} \right) \cdot \left( \frac{n}{de} \right) = \left[ -1 \right]^{H_d H_n + H_e H_n}.
\]

And Prop’n 12 says that the RhS equals \( -1 \)^{\(d_e H_n \).}

**Inducting twice.** W.r.t. a posodd \( N \), say that posodd \( d \) is “\( N \)-good” if
\[
\begin{align*}
\left( \frac{d}{N} \right) &= \left( \frac{N}{d} \right) \cdot \left[ -1 \right]^{H_d H_N}.
\end{align*}
\]

Having established (†), we have this:

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

Fixing a prime \( N \), the QReciprocity Thm, in form \((8')\), tells us that every prime, \( d \), is \( N \)-good. By (3), then: **Every posodd \( d \) is \( N \)-good.**

But (1) 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 (3) 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 oddprimes \( p \perp N \), for which \( N \in \text{QR}_p \). Say \( k \) is 5Near if \( k \equiv_5 \pm 1 \), and \( k \) is 5Far if \( k \equiv_5 \pm 2 \).

14: Thm. **Prime \( p \neq 5 \) has \( \text{QR}_p \equiv 5 \) IFF \( p \) is 5Near.**

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

Unfinished: as of 27Jul2018

2nd Application of LST+QRecip. We will show:
15a: For each \( n \geq 2 \), 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:

15b: Thm. Let \( T_n := n^2 + n + 1 \), and define
\[
\mathcal{E}_n := \left\{ p \in T_n \mid p \text{ is prime, and } p \notin \{2, 3\} \right\}.
\]

Every \( \mathcal{E}_n \)-prime is 3Pos. And for each \( n \geq 2 \), collection \( \mathcal{E}_n \) is not empty.

**Pf of 3Posness.** LSTShow that \( p \in \text{3Pos} \), where \( p \) is an arbitrary non-2,3 prime \( p \) that divides \( *: F_n := 4T_n \not\sim [2n + 1]^2 + 3 \).

Now \( F_n \equiv_p 0 \), so (*) says \(-3\) is a mod-\(p\) square. By hyp, \(-3 \not\equiv_p \), so \(-3 \in \text{QR}_p \), i.e.
\[
1 = \left( \frac{-3}{p} \right) \left( \frac{-1}{p} \right) = \left[ -1 \right]^{\frac{p - 1}{2}} \cdot \left( \frac{-1}{p} \right) = \left( \frac{-3}{3} \right) = \left( \frac{1}{3} \right).
\]

But the only 3-QR is 1. So \( p \) is 3Pos.

**Pf \( \mathcal{E}_n \neq \emptyset \).** Fix \( n \geq 2 \). FTSOC suppose \( \mathcal{E}_n \) is empty. Since \( T_n \) is odd, this implies that \( T_n = 3^k \), some \( k \geq 2 \); this last, since \( T_n > T_1 = 3 \). So \( \left\{ F_n = 4 \cdot 3^k \right\} \).

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

Recall that \( k \geq 2 \), whence \( F_n \not\sim 0 \). So (*) implies that \( 0 \not\sim 3 \), which is false. Hence \( \mathcal{E}_n \) is non-void.

E11: For what negative integers \( n \) do we have (15a)? Or have (15b)?