Acta Universitatis Apulensis No. 28/2011
ISSN: 1582-5329 pp. 333-339

# PERMUTATIONS OF RATIONAL RESIDUES

Mark Budden, Sean Eastman, Scott King, and Alexander Moisant

Abstract. In 1872, Zolotarev gave a new proof of the law of quadratic reciprocity by equating the value of the Legendre symbol $\left(\frac{a}{p}\right)$ with the signature of the permutation

$$i \pmod p \mapsto ia \pmod p$$

on $(\mathbb{Z}/p\mathbb{Z})^\times$. In this paper, we show how Zolotarev's approach may be extended to proving higher powered rational reciprocity laws.

2000 *Mathematics Subject Classification*: Primary 11A15, 11R18; Secondary 11R32.

## 1. Introduction

Recent estimates (eg., see [6]) claim that there are about 224 different proofs of the law of quadratic reciprocity. One of the gems on the list includes a proof that follows from Zolotarev's 1872 observation that the permutation

$$i \pmod p \mapsto ia \pmod p$$

on the nonzero congruence class representatives of $\mathbb{Z}/p\mathbb{Z}$ is even if and only if $a$ is a quadratic residue modulo $p$. Duke and Hopkins [3] recently revived Zolotarev's work, extending it to define a quadratic symbol for all finite groups and proving a corresponding quadratic reciprocity law.

In this paper, we extend Zolotarev's equivalent description of the Legendre symbol to $2^t$th rational residues modulo a prime $p \equiv 1 \pmod{2^t}$. Our extension is not new as it is a special case of Theorem 6 of Lehmer's paper [4]. However, the proof we give is self-contained and does not make use of Lehmer's generalization of Gauss' Lemma (Theorem 3 of [4]). Using this extension, we then provide a new proof of the recent $2n$th reciprocity law proved by Budden, Collins, Lea, and Savioli [1], in the special case where $n$ is a power of 2. Many of the known rational reciprocity laws follow from this result by choosing appropriate primitive elements for the subfields of $\mathbb{Q}(\zeta_p)$.

## 2. Rational Residues Modulo $p$

In this section, we prove an analogue of Zolotarev's description of the Legendre symbol for the $2^t$th rational residue symbol. First, we establish the main definitions and notations. Letting $p$ be an odd prime, we will be working in the finite field $\mathbb{Z}/p\mathbb{Z}$, and by abuse of notation, we will frequently write the least residue $a$ in place of the left coset $a+p\mathbb{Z}$. The notation $\left(\frac{\cdot}{\cdot}\right)$ will be used to denote the Legendre symbol. We can generalize the Legendre symbol to higher power residues in two ways: the power residue symbol and the rational residue symbol.

To define the power residue symbol, let $k$ be an algebraic number field and $n \geq 1$ an integer. If $\mathfrak{p}$ is an ideal in the ring of integers $\mathcal{O}_k$ that is relatively prime to $n$, then for every $\alpha \in \mathcal{O}_k - \mathfrak{p}$, define the $n$th power residue symbol by

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n \equiv \alpha^{(N\mathfrak{p}-1)/n} \pmod{\mathfrak{p}}.$$

We will only define the rational residue symbol in the case of even powers. If we assume that $p \equiv 1 \pmod{2n}$, $a \in \mathbb{Z}$ is relatively prime to $p$, and

$$a^{(p-1)/n} \equiv 1 \pmod{p},$$

then the $2n$th rational residue symbol is given by

$$\left(\frac{a}{p}\right)_{2n} \equiv a^{(p-1)/2n} \pmod{p}.$$

This symbol agrees with the power residue symbol $\left(\frac{a}{\mathfrak{p}}\right)_{2n}$, where $\mathfrak{p}$ is any prime ideal above $p\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q}(\zeta_{2n})} = \mathbb{Z}[\zeta_{2n}]$. We denote the subgroup of $2n$th rational residues in $(\mathbb{Z}/p\mathbb{Z})^\times$ by $(\mathbb{Z}/p\mathbb{Z})^{\times 2n}$. The following theorem describes the relationship between the $2^t$th rational residue symbol and the corresponding permutation on $(\mathbb{Z}/p\mathbb{Z})^\times$.

**Theorem 1.** *Let $p \equiv 1 \pmod{2^t}$ be a prime for $t \geq 1$ and assume that $\left(\frac{a}{p}\right)_{2^{t-1}} = 1$ for $a \in \mathbb{Z}$ relatively prime to $p$. Then*

$$\left(\frac{a}{p}\right)_{2^t} = 1 \quad \Longleftrightarrow \quad \phi_a|_{(\mathbb{Z}/p\mathbb{Z})^{\times 2^{t-1}}} \text{ is even,}$$

*where $\phi_a$ is the permutation on $(\mathbb{Z}/p\mathbb{Z})^\times$ given by*

$$i \pmod{p} \mapsto ia \pmod{p}.$$

*Proof.* In the case $t = 1$, we set $\left(\frac{a}{p}\right)_1 = 1$ by convention (since every element in $(\mathbb{Z}/p\mathbb{Z})^\times$ is a first power). Then Zolotarev [7] proved

$$\left(\frac{a}{p}\right) = 1 \quad \Longleftrightarrow \quad \phi_a \text{ is even.}$$

We proceed by induction on $t$. Suppose the theorem holds for the $(t-1)$th case and that $\left(\frac{a}{p}\right)_{2^{t-1}} = 1$. Let $f$ denote the order of $a$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ and write $g = \frac{p-1}{f}$. If $\mathfrak{p}$ is any prime ideal above $p\mathbb{Z}$ in $\mathcal{O}_{\mathbb{Q}(\zeta_{2^{t-1}})}$, then the sets

$$B_i := \left\{ b \in (\mathbb{Z}/p\mathbb{Z})^\times \;\middle|\; \left(\frac{b}{\mathfrak{p}}\right)_{2^{t-1}} = \zeta_{2^{t-1}}^i \right\}$$

each have cardinality $\frac{p-1}{2^{t-1}}$ and

$$\left(\frac{\phi_a(b)}{\mathfrak{p}}\right)_{2^{t-1}} = \left(\frac{ba}{\mathfrak{p}}\right)_{2^{t-1}} = \left(\frac{b}{\mathfrak{p}}\right)_{2^{t-1}} \left(\frac{a}{\mathfrak{p}}\right)_{2^{t-1}} = \left(\frac{b}{\mathfrak{p}}\right)_{2^{t-1}}$$

implies that $\phi_a$ preserves the $2^{t-1}$th rational residue classes modulo $p$. We also note that

$$\phi_a^f(b) \equiv ba^f \equiv b \pmod{p},$$

with $f$ minimal, shows that $\phi_a$ is a product of $g$ cycles of length $f$ and that $\phi_a$ affects each $B_i$ in exactly the same way. It follows that

$$\begin{aligned} \left(\frac{a}{p}\right)_{2^t} \equiv a^{(p-1)/2^t} \equiv 1 \pmod{p} \quad &\Longleftrightarrow \quad f \text{ divides } \frac{p-1}{2^t} = \frac{fg}{2^t} \\ &\Longleftrightarrow \quad g \equiv 0 \pmod{2^t} \\ &\Longleftrightarrow \quad \phi_a|_{(\mathbb{Z}/p\mathbb{Z})^{\times 2^{t-1}}} \text{ is even,} \end{aligned}$$

completing the proof of Theorem 1. $\square$

## 3. Reciprocity Laws

Utilizing our new description of the rational residue symbol, we provide a new proof of the $2n$th reciprocity law of Budden, Collins, Lea, and Savioli [1] in the special case where $n$ is a power of 2. From this result, all of the known rational quartic reciprocity laws follow (cf. [5]) by choosing appropriate primitive elements for $K_4$, the unique quartic subfield of $\mathbb{Q}(\zeta_p)$ (assuming $p \equiv 1 \pmod 4$). When $p \equiv 1 \pmod{2^t}$, the $2^t$th generalization of Scholz's Reciprocity Law proved in [2] also follows from the following theorem by choosing an appropriate primitive element for $K_{2^t}$, the unique subfield of $\mathbb{Q}(\zeta_p)$ of dimension $2^t$ over $\mathbb{Q}$.

Our setup is similar to that of Duke and Hopkins [3] and may shed some light on the potential formulation of a rational $2^t$th reciprocity law in any finite group. The additive group $\mathbb{Z}/p\mathbb{Z}$ is abelian, and thus has $p$ irreducible characters

$$\chi_i : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{C}^\times$$

given by $\chi_i(a) = \zeta_p^{ia}$, for $0 \leq i < p$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is given by

$$\left\{\sigma_k : \mathbb{Q}(\zeta_p) \longrightarrow \mathbb{Q}(\zeta_p) \mid \sigma_k(\zeta_p) = \zeta_p^k\right\} \cong (\mathbb{Z}/p\mathbb{Z})^\times .$$

Assuming that $p \equiv 1 \pmod{2^t}$, the fundamental theorem of Galois theory implies that

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_{2^t}) \cong (\mathbb{Z}/p\mathbb{Z})^{\times 2^t} .$$

The action of any automorphism $\sigma_k$ may be identified with the permutation $\phi_k$ via

$$\sigma_k(\chi_i(a)) = \sigma_k(\zeta_p^{ia}) = \zeta_p^{iak} = \chi_i(\phi_k(a)).$$

**Theorem 2.** *Let $p \equiv q \equiv 1 \pmod{2^t}$ be distinct primes such that*

$$\left(\frac{p}{q}\right)_{2^{t-1}} = \left(\frac{q}{p}\right)_{2^{t-1}} = 1.$$

*If $\beta \in \mathcal{O}_{K_{2^{t-1}}}$ such that $K_{2^t} = \mathbb{Q}(\sqrt{\beta})$, then*

$$\left(\frac{q}{p}\right)_{2^t} = \left(\frac{\beta}{\mathfrak{q}}\right)_2 ,$$

*where $\mathfrak{q}$ is any prime ideal above $q\mathbb{Z}$ in $\mathcal{O}_{K_{2^{t-1}}}$.*

*Proof.* Let $a_1, a_2, \ldots, a_k$ denote the $2^{t-1}$th residues of $p$, with $k = \frac{p-1}{2^{t-1}}$, and consider the matrix

$$R = \begin{pmatrix} \chi_1(a_1) & \cdots & \chi_1(a_k) \\ \vdots & \ddots & \vdots \\ \chi_k(a_1) & \cdots & \chi_k(a_k) \end{pmatrix}.$$

For any $a \in (\mathbb{Z}/p\mathbb{Z})^{\times 2^{t-1}}$, the automorphism $\sigma_a$ maps $\chi_i(a_j) \mapsto \chi_i(\phi_a(a_j))$ and hence, permutes the columns of $R$. From Theorem 1 and the basic properties of determinants, it follows that

$$\sigma_a(det(R)) = \left(\frac{a}{p}\right)_{2^t} det(R).$$

When the automorphism $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/K_{2^{t-1}})$ is restricted to $K_{2^t}$, it agrees with either the identity or conjugation $\sqrt{\beta} \mapsto -\sqrt{\beta}$, depending on whether or not $a$ is a $2^t$th residue of $p$. Hence, it follows that

$$\sigma_a\left(\sqrt{\beta}\ det(R)\right) = \sqrt{\beta}\ det(R), \tag{1}$$

so that $\sqrt{\beta}\ det(R) \in K_{2^{t-1}}$. Now suppose that $\mathfrak{q}$ is any prime ideal above $q\mathbb{Z}$ in $K_{2^{t-1}}$ and consider the congruence

$$\begin{aligned} \sigma_q\left(\sqrt{\beta}\ det(R)\right) &\equiv \left(\sqrt{\beta}\right)^q \left(\frac{q}{p}\right)_{2^t} det(R) \pmod{\mathfrak{q}} \\ &\equiv \beta^{(q-1)/2}\left(\frac{q}{p}\right)_{2^t} \sqrt{\beta}\ det(R) \pmod{\mathfrak{q}} \\ &\equiv \left(\frac{\beta}{\mathfrak{q}}\right)_2 \left(\frac{q}{p}\right)_{2^t} \sqrt{\beta}\ det(R) \pmod{\mathfrak{q}}. \end{aligned} \tag{2}$$

Comparing (1) and (2) when $a = q$, we obtain

$$\sqrt{\beta}\ det(R) \equiv \left(\frac{\beta}{\mathfrak{q}}\right)_2 \left(\frac{q}{p}\right)_{2^t} \sqrt{\beta}\ det(R) \pmod{\mathfrak{q}}. \tag{3}$$

Since the matrix $R$ is of Vandermonde-type, its determinant is given by

$$\begin{aligned} det(R) &= \prod_{1\le m\le k} \zeta_p^{a_m} \cdot \prod_{1\le i<j\le k} (\zeta_p^{a_j} - \zeta_p^{a_i}) \\ &= \prod_{1\le m\le k} \zeta_p^{a_m} \cdot \prod_{1\le i<j\le k} \zeta_p^{a_j}(1 - \zeta_p^{a_i - a_j}), \end{aligned}$$

which is a product of units and factors that divide $p$ in $\mathbb{Q}(\zeta_p)$. Also, the principal ideal generated by $\beta$ in $\mathcal{O}_{K_2^{t-1}}$ becomes a square when lifted to $K_{2^t}$, so $\beta$ must be relatively prime to $q$. Thus, $\sqrt{\beta}\ det(R)$ is not in the ideal $\mathfrak{q}$ and can be canceled from both sides of the congruence (3). Since the residue symbols in (3) only take on the values $\pm 1$, we may drop the congruence to obtain the desired result. $\square$

Note that Theorem 2 is independent of the choice of prime ideal $\mathfrak{q}$. Since we assume $\left(\frac{p}{q}\right)_{2^{t-1}} = 1$, $q\mathbb{Z}$ splits completely in $K_{2^{t-1}}$ giving the isomorphism

$$\mathcal{O}_{K_{2^{t-1}}}/\mathfrak{q} \cong \mathbb{Z}/q\mathbb{Z}.$$

Thus, we can identify $\left(\frac{\beta}{\mathfrak{q}}\right)_2$ with a Legendre symbol $\left(\frac{b}{q}\right)$ via

$$b \equiv \beta \pmod{\mathfrak{q}},$$

with $b \in (\mathbb{Z}/p\mathbb{Z})^{\times}$.

Our approach to proving this theorem using a partial character table (matrix) is similar to the method employed by Duke and Hopkins [3] in the proof of their quadratic reciprocity law in finite groups. This demonstrates the potential for extending their results to $2^t$th rational residues.

## References

[1] M. Budden, A. Collins, K. Lea, and S. Savioli, *Rational Residuacity of Primes,* Involve, 3, (2010), 249-257.

[2] M. Budden, R.J Eisenmenger, and J. Kish, *A Generalization of Scholz's Reciprocity Law,* J. Théor. Nombres Bordeaux, 19, (2007), 583-594.

[3] W. Duke and K. Hopkins, *Quadratic Reciprocity in a Finite Group,* Amer. Math. Monthly, 112, (2005), 251-256.

[4] E. Lehmer, *Generalizations of Gauss' Lemma,* Number Theory and Algebra, Academic Press, New York, (1977), 187-194.

[5] F. Lemmermeyer, *Rational Quartic Reciprocity,* Acta Arith., 67, (1994), 387-390.

[6] F. Lemmermeyer, *Reciprocity Laws,* Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[7] G. Zolotarev, *Nouvelle démonstration de la loi de réciprocité de Legendre,* Nouvelle Ann. Math., 11, No. 2, (1872), 354-362.

Mark Budden
Mathematics and Computer Science Department
Western Carolina University
Cullowhee, NC 28723
email:*mrbudden@email.wcu.edu*

Sean Eastman
Department of Mathematics

Armstrong Atlantic State University
11935 Abercorn St.
Savannah, GA 31419
email:*Sean.Eastman@armstrong.edu*

Scott King
4345 Driggers Road
Waycross, GA 31503
email:*scottjacksonking@gmail.com*

Alexander Moisant
Department of Mathematics
Armstrong Atlantic State University
11935 Abercorn St.
Savannah, GA 31419
email:*am1677@students.armstrong.edu*