

# involve

a journal of mathematics

## Rational residuacity of primes

Mark Budden, Alex Collins, Kristin Ellis Lea and Stephen Savioli

 mathematical sciences publishers

# Rational residuacity of primes

Mark Budden, Alex Collins, Kristin Ellis Lea and Stephen Savioli

(Communicated by Filip Saidak)

The most natural extensions to the law of quadratic reciprocity are the rational reciprocity laws, described using the rational residue symbol. In this article, we provide a reciprocity law from which many of the known rational reciprocity laws may be recovered by picking appropriate primitive elements for subfields of  $\mathbb{Q}(\zeta_p)$ . As an example, a new generalization of Burde's law is provided.

## 1. Introduction

The law of quadratic reciprocity has played a central role in the development of number theory since Gauss published its first proof in 1801 (see [Lemmermeyer 2000] for the history of this important result). To state the law, assume that  $a \in \mathbb{Z}$  is not divisible by an odd prime  $p$  and define the Legendre symbol by

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } x^2 \equiv a \pmod{p} \text{ is solvable,} \\ -1 & \text{if not.} \end{cases}$$

Then if  $p$  and  $q$  are distinct odd primes, we have

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

The remainder of the 1800s and early 1900s saw many generalizations of this result to higher powers, culminating in class field theory, in which generalized reciprocity laws were established. Making such generalizations requires one to leave the realm of the integers, introducing rings of integers in algebraic number fields and primes within these rings. Hence, the study of reciprocity laws can serve as a great topic for students interested in learning about field extensions and Galois theory.

While class field theory has succeeded in capturing the true essence of the higher reciprocity laws, the extensions to the law of quadratic reciprocity that are the most accessible to students are the rational reciprocity laws. Such laws make use of the

---

*MSC2000:* primary 11A15; secondary 11R32, 11R18.

*Keywords:* reciprocity laws, ramification of prime ideals, cyclotomic fields.

Supported in part by an internal grant from Armstrong Atlantic State University and a CURM mini-grant funded through NSF grant DMS-0636648.

rational residue symbol, which only takes on the integer values  $\pm 1$  and is defined on rational primes. The simplicity of the rational residue symbol is much more tangible to students than the power residue symbol, making such laws an excellent starting point for students in algebraic number theory. Like the law of quadratic reciprocity, the statements are often elementary, but the proofs elucidate the utility of Galois theory and the ramification theory of prime ideals in algebraic number fields.

We begin with a description of the quadratic residue symbol and the rational residue symbol. Let  $K$  be an algebraic number field and  $N$  the norm map of  $K$  over  $\mathbb{Q}$ . Let  $\mathfrak{p}$  be a prime ideal such that  $\mathfrak{p} \nmid 2\mathbb{O}_K$ , where  $\mathbb{O}_K$  is the ring of integers in  $K$ . For every  $\alpha \in \mathbb{O}_K - \mathfrak{p}$ , define the quadratic residue symbol  $\left(\frac{\alpha}{\mathfrak{p}}\right)$  by

$$\left(\frac{\alpha}{\mathfrak{p}}\right) \equiv \alpha^{(N(\mathfrak{p})-1)/2} \pmod{\mathfrak{p}}.$$

In the case where  $K = \mathbb{Q}$ , our definition agrees with the Legendre symbol on the generator of the prime ideal  $\mathfrak{p} = p\mathbb{Z}$ .

Now let  $a \in \mathbb{Z}$  and  $p$  be an odd prime satisfying  $(a, p) = 1$  such that

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

Then the  $2n$ -th rational residue symbol  $(a/p)_{2n}$  is defined by

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

It is easily verified that this symbol only takes on the integer unit values  $\pm 1$ . It should also be noted that it agrees with the  $2n$ -th power residue symbol  $(a/\mathfrak{p})_{\mathbb{Q}(\zeta_{2n})}$ , where  $\mathfrak{p}$  is any prime ideal above  $p$  in  $\mathbb{Q}(\zeta_{2n})$  and  $\zeta_{2n}$  is the primitive  $2n$ -th root of unity  $e^{\pi i/n}$ .

An indispensable object used in the proofs of most reciprocity laws is the Galois group

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}),$$

defined to be the group of all automorphisms  $\mathbb{Q}(\zeta_p) \rightarrow \mathbb{Q}(\zeta_p)$  that fix  $\mathbb{Q}$  pointwise (here,  $\zeta_p$  is the primitive  $p$ -th root of unity  $e^{2\pi i/p}$ ). By the fundamental theorem of Galois theory (see [Gallian 2010, Chapter 32], for instance), there is a one-to-one correspondence between the intermediate subfields of the extension  $\mathbb{Q}(\zeta_p)/\mathbb{Q}$  and the subgroups of  $\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ . It is well known that

$$\text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$$

is a cyclic group of order  $p-1$ . So, whenever  $p \equiv 1 \pmod{m}$ , there exists a unique subfield  $K_m$  of  $\mathbb{Q}(\zeta_p)$  that satisfies  $[K_m : \mathbb{Q}] = m$ .

Lemmermeyer [1994] showed that when  $p \equiv 1 \pmod{4}$ , specific choices of  $A, B \in \mathbb{Z}$  so that  $K_4 = \mathbb{Q}(\sqrt{A + B\sqrt{p}})$  result in the rational quartic reciprocity laws of Scholz [1934], Lehmer [1958; 1978], and Burde [1969]. His work simplified the all-encompassing rational quartic reciprocity law of Williams et al. [1985] as well as its simplification by Evans [1989]. The reader unfamiliar with these laws may consult Lehmer’s survey article [Lehmer 1978] and [Lemmermeyer 2000] for the relevant background.

When extending the known rational quartic reciprocity laws, it is natural to look for analogues that involve the  $2^t$ -th rational residue symbols  $(p/q)_{2^t}$  and  $(q/p)_{2^t}$  when  $p \equiv q \equiv 1 \pmod{2^t}$  are distinct primes. Such a generalization of Burde’s law was proved by Evans [1981], and Budden et al. [2007] recently proved such a generalization of Scholz’s law. In Section 2, we follow the approach of [Budden et al. 2007] to prove a  $2n$ -th reciprocity law (Theorem 1), from which many of the known rational reciprocity laws can be recovered. The approach is similar to that of [Lemmermeyer 1994] in that it compares the factorization of the prime ideal  $q\mathbb{Z}$  in  $\mathbb{Q}(\zeta_p)$  to its factorization in  $K_{2n}$ . Additionally, the all-encompassing rational quartic law in this last reference may be viewed as a special case of the quartic version of the  $2n$ -th law presented here. Hence, all of the known rational quartic reciprocity laws may be recovered from Theorem 1.

Finally, as an application of Theorem 1, we give in Section 3 a  $2^t$ -th generalization of Burde’s law (Theorem 3), that differs from the known generalizations. In particular, our result is different from Williams’ octic version of Burde’s law [Williams 1976] when  $t = 3$  (also proved independently by Wu [1975]), Leonard and Williams’ sixteenth version of Burde’s law when  $t = 4$  [Leonard and Williams 1977], and Evans’  $2^t$ -th generalization of Burde’s law [Evans 1981]. Interesting results follow from comparing the variations.

### 2. A $2n$ -th rational reciprocity law

Now assume that  $p \equiv q \equiv 1 \pmod{2n}$  are distinct primes with  $n \geq 1$  such that

$$\left(\frac{p}{q}\right)_n = \left(\frac{q}{p}\right)_n = 1.$$

Then the ideal  $q\mathbb{O}_{K_n}$  factors into prime ideals as

$$q\mathbb{O}_{K_n} = \lambda_1 \lambda_2 \cdots \lambda_n,$$

with all of the  $\lambda_i$  distinct. We obtain the following reciprocity law.

**Theorem 1.** *Let  $p \equiv q \equiv 1 \pmod{2n}$  be distinct primes with  $n \geq 1$  and assume*

$$\left(\frac{p}{q}\right)_n = \left(\frac{q}{p}\right)_n = 1.$$

If  $\beta \in \mathbb{O}_{K_n}$  is such that  $K_{2n} = K_n(\sqrt{\beta})$ , then  $\left(\frac{q}{p}\right)_{2n} = \left(\frac{\beta}{\lambda}\right)$ , where  $\lambda$  is any prime ideal above  $q$  in  $\mathbb{O}_{K_n}$ .

*Proof.* The cyclotomic polynomial  $\Phi_p(x) = \prod_{k=1}^{p-1} (x - \zeta_p^k)$  splits over  $K_n$ , and we let  $\varphi_p(x)$  be the irreducible factor

$$\varphi_p(x) = \prod_{\substack{1 \leq r \leq p-1 \\ (r/p)_n=1}} (x - \zeta_p^r).$$

Since  $\Phi_p(x) \in \mathbb{Z}[\zeta_p][x]$ , it follows that  $\varphi_p(x) \in \mathbb{O}_{K_n}$ . Furthermore, it has degree  $(p-1)/n$  and splits further over  $K_{2n}$  into  $\varphi_p(x) = \psi_p(x) \cdot \tilde{\psi}_p(x)$ , where

$$\psi_p(x) = \prod_{\substack{1 \leq r \leq p-1 \\ (r/p)_{2n}=1}} (x - \zeta_p^r) \quad \text{and} \quad \tilde{\psi}_p(x) = \prod_{\substack{1 \leq t \leq p-1 \\ (t/p)_{2n}=-1 \\ (t/p)_n=1}} (x - \zeta_p^t).$$

Define the polynomial  $\vartheta(x) = \psi_p(x) - \tilde{\psi}_p(x) \in \mathbb{O}_{K_{2n}}[x]$  and consider the automorphism  $\sigma_q \in \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ , defined by  $\sigma_q(\zeta_p) = \zeta_p^q$ . Since the group  $(\mathbb{Z}/p\mathbb{Z})^\times$  is cyclic, it has unique cyclic subgroups of orders dividing  $p-1$ , implying that

$$\text{Gal}(\mathbb{Q}(\zeta_p)/K_n) \cong (\mathbb{Z}/p\mathbb{Z})^{\times n} \quad \text{and} \quad \text{Gal}(\mathbb{Q}(\zeta_p)/K_{2n}) \cong (\mathbb{Z}/p\mathbb{Z})^{\times 2n}.$$

Under the assumption  $(q/p)_n = 1$ , the automorphism  $\sigma_q$  is contained in the Galois group  $\text{Gal}(\mathbb{Q}(\zeta_p)/K_n)$ . Its restriction to  $K_{2n}$  must agree with either the identity automorphism  $I \in \text{Gal}(K_{2n}/K_n)$ , or the nontrivial automorphism  $\alpha(\sqrt{\beta}) = -\sqrt{\beta}$ . It follows that

$$\sigma_q|_{K_{2n}} = I \iff (q/p)_{2n} = 1.$$

Since

$$\alpha(\sqrt{\beta} \vartheta(x)) = \sqrt{\beta} \vartheta(x)$$

and the coefficients in  $\vartheta(x)$  come from  $\mathbb{O}_{K_{2n}}$ , every coefficient must be an element in  $\mathbb{O}_{K_n}$  multiplied by  $\sqrt{\beta}$  so that we can write

$$\vartheta(x) = \sqrt{\beta} \phi(x), \quad \text{for some } \phi(x) \in \mathbb{O}_{K_n}[x].$$

We have also assumed that  $(p/q)_n = 1$ , so that the ideal  $q\mathbb{O}_{K_n}$  splits completely in  $\mathbb{O}_{K_n}$  (i.e.,  $q\mathbb{O}_{K_n} = \lambda_1 \lambda_2 \cdots \lambda_n$ , a product of distinct prime ideals). If  $\lambda$  is any such prime ideal in  $\mathbb{O}_{K_n}$ , then  $\mathbb{O}_{K_n}/\lambda \cong \mathbb{Z}/q\mathbb{Z}$ . We have the congruence

$$(\vartheta(x))^q = (\psi_p(x) - \tilde{\psi}_p(x))^q \equiv \left(\frac{q}{p}\right)_{2n} (\psi_p(x^q) - \tilde{\psi}_p(x^q)) \pmod{\lambda}.$$

On the other hand, we also have

$$\begin{aligned} (\vartheta(x))^q &= (\sqrt{\beta} \phi(x))^q \equiv \beta^{(q-1)/2} \sqrt{\beta} \phi(x^q) \pmod{\lambda} \\ &\equiv \left(\frac{\beta}{\lambda}\right) (\psi_p(x^q) - \tilde{\psi}_p(x^q)) \pmod{\lambda}. \end{aligned}$$

We will obtain the desired result from the congruence

$$\left(\frac{q}{p}\right)_{2n} (\psi_p(x^q) - \tilde{\psi}_p(x^q)) \equiv \left(\frac{\beta}{\lambda}\right) (\psi_p(x^q) - \tilde{\psi}_p(x^q)) \pmod{\lambda}$$

once we show that  $\psi_p(X) \not\equiv \tilde{\psi}_p(X) \pmod{\lambda}$ ; note that if  $\psi_p(X) \equiv \tilde{\psi}_p(X) \pmod{\lambda}$ , then  $\varphi_p(X) \equiv \psi(X)^2 \pmod{\lambda}$ . Applying Kummer’s theorem [Janusz 1996, Theorem 7.4], the polynomial  $\Phi_p(X)$  factors in exactly the same way in

$$(\mathbb{Z}/q\mathbb{Z})[X] \cong (\mathbb{O}_{K_n}/\lambda)[X],$$

as  $q\mathbb{Z}[\zeta_p]$  factors in  $\mathbb{Z}[\zeta_p]$ . However, the distinctness of the primes  $p$  and  $q$  implies that  $q\mathbb{Z}[\zeta_p]$  does not ramify, giving a contradiction. Thus, we conclude that

$$\left(\frac{q}{p}\right)_{2n} \equiv \left(\frac{\beta}{\lambda}\right) \pmod{\lambda},$$

which reduces to an equality since the residue symbols only take on the values  $\pm 1$ . □

While this reciprocity law may not appear to be rational, given the existence of the quadratic residue symbol, it can be identified with a Legendre symbol. Namely, the element  $\beta$  is a coset representative in

$$\mathbb{O}_{K_n}/\lambda \cong \mathbb{Z}/q\mathbb{Z},$$

and since  $0, 1, \dots, q-1$  represent distinct cosets in  $\mathbb{O}_{K_n}/\lambda$ , we have  $\beta \equiv a \pmod{\lambda}$  for some unique element  $a \in \{1, 2, \dots, q-1\}$ . Thus, we have

$$\left(\frac{\beta}{\lambda}\right) = \left(\frac{a}{\lambda}\right),$$

and since [Theorem 1](#) is independent of the choice of prime  $\lambda$  above  $q$ , we may write

$$\left(\frac{\beta}{\lambda}\right) = \left(\frac{a}{q}\right).$$

In this capacity, [Theorem 1](#) may be viewed as a rational reciprocity law.

We chose the polynomial-based proof given for [Theorem 1](#) because it highlights the significance of Kummer’s theorem, relating the factoring of minimal polynomials in function fields to that of prime ideals in number fields. We note that [Theorem 1](#) can also be proved in an analogous way to Lemmermeyer’s proof of the all-encompassing rational quartic reciprocity law in [[Lemmermeyer 1994](#)].

### 3. Generalizing Burde’s law

Since [Theorem 1](#) is a generalization of the all-encompassing rational quartic reciprocity law in [[Lemmermeyer 1994](#)], the rational quartic laws of Scholz [[1934](#)], Lehmer [[1958](#); [1978](#)] and Burde [[1969](#)] all follow by picking appropriate primitive elements for  $K_4$ . In this section, we show that [Theorem 1](#) implies a generalization of Burde’s law that differs from the known generalizations. Before giving the general case, we recall Lemmermeyer’s proof [[2000](#)] of Burde’s law for motivation.

Assume that  $p \equiv q \equiv 1 \pmod{4}$  are distinct primes, so we can write  $p = a^2 + b^2$  and  $q = A^2 + B^2$  with  $2 \nmid aA$ . We also assume that  $(p/q) = 1$ . A few simple consequences of these conditions that can be checked directly are

$$\left(\frac{A}{q}\right) = 1 \quad \text{and} \quad \left(\frac{2B}{q}\right) = 1.$$

Lemmermeyer argued that  $K_4 = \mathbb{Q}(\sqrt{\beta_4})$ , where

$$\beta_4 = pq + (b(A^2 - B^2) + 2aAB)\sqrt{p}.$$

Then we see that

$$\begin{aligned} \left(\frac{\beta_4}{q}\right) &\equiv \beta_4^{(q-1)/2} \equiv (b(A^2 - B^2) + 2aAB)^{(q-1)/2} p^{(q-1)/4} \pmod{q} \\ &\equiv (-2bB^2 + 2aAB)^{(q-1)/2} \left(\frac{p}{q}\right)_4 \pmod{q} \\ &\equiv (-2B(bB - aA))^{(q-1)/2} \left(\frac{p}{q}\right)_4 \pmod{q} \\ &\equiv \left(\frac{-2B}{q}\right) \left(\frac{bB - aA}{q}\right) \left(\frac{p}{q}\right)_4 \pmod{q} \\ &\equiv \left(\frac{bB - aA}{q}\right) \left(\frac{p}{q}\right)_4 \pmod{q}. \end{aligned}$$

Thus, from [Theorem 1](#), we obtain Burde’s law:

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{bB - aA}{q}\right).$$

Note that Burde’s law is independent of the choices of signs of  $a, b, A$ , and  $B$ .

We now describe a primitive element for  $K_{2^t}$ , when  $t \geq 2$ , analogous to  $\sqrt{\beta_4}$  used above for  $K_4$ .

**Theorem 2.** *Let  $p \equiv q \equiv 1 \pmod{2^t}$  be distinct primes with  $t \geq 2$  such that  $p = a^2 + b^2$  and  $q = A^2 + B^2$  with  $2 \nmid aA$ . If  $\beta_4 = pq + (b(A^2 - B^2) + 2aAB)\sqrt{p}$ , then a primitive element for  $K_{2^t}$  can be defined recursively for  $t > 2$  by*

$$\beta_{2^t} = (q\sqrt{p} + (b(A^2 - B^2) + 2aAB))\sqrt{\beta_{2^{t-1}}},$$

with  $K_{2^t} = \mathbb{Q}(\sqrt{\beta_{2^t}})$ .

*Proof.* Our proof proceeds by using (weak) induction on  $t \geq 2$  following Lemmermeyer’s approach [Lemmermeyer 1994] in the quartic case (and as our starting point when  $t = 2$ ). Assume that the theorem holds for the  $2^{t-1}$  case with  $K_{2^{t-1}} = \mathbb{Q}(\sqrt{\beta_{2^{t-1}}})$  and let

$$\alpha_{2^t} = q\sqrt{p}\sqrt{\beta_{2^{t-1}}}, \quad \gamma = (b(A^2 - B^2) + 2aAB), \quad \delta = (a(A^2 - B^2) - 2bAB).$$

It is easily checked that  $\alpha_{2^t}$ ,  $\gamma$ , and  $\delta$  are pairwise relatively prime and that

$$\alpha_{2^t}^2 = \beta_{2^{t-1}}(\gamma^2 + \delta^2).$$

From the identity

$$2(\alpha_{2^t} + \gamma\sqrt{\beta_{2^{t-1}}})(\alpha_{2^t} + \delta\sqrt{\beta_{2^{t-1}}}) = (\alpha_{2^t} + \gamma\sqrt{\beta_{2^{t-1}}} + \delta\sqrt{\beta_{2^{t-1}}})^2,$$

we see that

$$K_{2^t} := \mathbb{Q}\left(\sqrt{\alpha_{2^t} + \gamma\sqrt{\beta_{2^{t-1}}}}\right) = \mathbb{Q}\left(\sqrt{2(\alpha + \delta\sqrt{\beta_{2^{t-1}}})}\right).$$

Thus, the only primes that can possibly ramify in  $K_{2^t}/K_{2^{t-1}}$  are 2 and any common divisors of

$$\alpha_{2^t}^2 - \beta_{2^{t-1}}\gamma^2 = \beta_{2^{t-1}}\delta^2 \quad \text{and} \quad \alpha_{2^t}^2 - \beta_{2^{t-1}}\delta^2 = \beta_{2^{t-1}}\gamma^2.$$

Since  $\delta$  and  $\gamma$  are relatively prime, the only odd primes that can ramify are divisors of  $\beta_{2^{t-1}}$ . However, any such prime would have to have ramified in  $\mathbb{Q}(\sqrt{\beta_{2^{t-1}}})$  and by our inductive hypothesis, only  $p$  ramified there. Thus,  $p$  is the only odd prime that ramifies in  $K_{2^t}/K_{2^{t-1}}$ .

Finally, we must argue that 2 does not ramify. Lemmermeyer [1994] showed the case  $t = 2$ , that is,  $\beta_4 \equiv 1 \pmod{4}$ . As our inductive hypothesis, we assume that  $\beta_{2^{t-1}} \equiv 1 \pmod{4}$ . Then the congruences

$$\sqrt{\beta_{2^{t-1}}} \equiv \pm 1 \pmod{4}, \quad \sqrt{p} \equiv \pm 1 \pmod{4}, \quad q \equiv 1 \pmod{4}$$

and the fact that  $\gamma$  is even show that  $\beta_{2^t} \equiv \sqrt{\beta_{2^{t-1}}}(q\sqrt{p} + \gamma) \equiv \pm 1 \pmod{4}$ . By Stickelberger’s discriminant relation [Ribenoim 2001, Section 6.3], the discriminant of an algebraic number field is  $0, 1 \pmod{4}$ . Thus,  $\beta_{2^t} \equiv 1 \pmod{4}$  and we conclude that 2 does not ramify in  $K_{2^t}/K_{2^{t-1}}$ . Since  $p$  is the only prime that ramifies in the abelian Galois extension  $K_{2^t}/\mathbb{Q}$ ,  $K_{2^t}$  is the unique subfield of  $\mathbb{Q}(\zeta_p)$  of degree  $2^t$  over  $\mathbb{Q}$  by the theorem of Kronecker and Weber [Ribenoim 2001, Section 15.1]. □

Using the reciprocity law given in Theorem 1 with the choice of primitive element for  $K_{2^t}$  given in Theorem 2, we obtain the following  $2^t$ -th generalization of Burde’s law, which is also independent of the choices of signs of  $a$ ,  $b$ ,  $A$ , and  $B$ .



**Theorem 3.** Let  $p \equiv q \equiv 1 \pmod{2^t}$  be distinct primes with  $t \geq 2$  such that

$$p = a^2 + b^2 \quad \text{and} \quad q = A^2 + B^2,$$

with  $2 \nmid aA$ . If

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

then

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

*Proof.* Once again, we use an inductive argument with Lemmermeyer's proof of Burde's law as a starting point. With regard to [Theorem 1](#), assuming that [Theorem 3](#) is true for the  $t - 1$  case is equivalent to assuming that

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

Letting  $\left(\frac{p}{q}\right)_{2^{t-1}} = \left(\frac{q}{p}\right)_{2^{t-1}} = 1$ , we then obtain, for  $t > 2$ ,

$$\begin{aligned} \left(\frac{q}{p}\right)_{2^t} &= \left(\frac{\beta_{2^t}}{q}\right) \equiv \beta_{2^t}^{(q-1)/2} \equiv \beta_{2^{t-1}}^{(q-1)/4} (b(A^2 - B^2) + 2aAB)^{(q-1)/2} \pmod{q} \\ &\equiv \left(\frac{2B(bB - aA)}{q}\right)_{2^{t-1}} \left(\frac{p}{q}\right)_{2^t} \left(\frac{2B(bB - aA)}{q}\right) \pmod{q} \\ &\equiv \left(\frac{2B(bB - aA)}{q}\right)_{2^{t-1}} \left(\frac{p}{q}\right)_{2^t} \pmod{q}. \end{aligned}$$

Since all of the rational residue symbols take on only the values  $\pm 1$ , we may drop the congruence and conclude the statement of [Theorem 3](#).  $\square$

Perhaps the other known generalizations of Burde's law also follow as consequences of [Theorem 1](#). At this time, we have not been able to find suitable primitive elements to prove such implications.

## References

- [Budden et al. 2007] M. Budden, J. Eisenmenger, and J. Kish, "A generalization of Scholz's reciprocity law", *J. Théor. Nombres Bordeaux* **19**:3 (2007), 583–594. [MR 2009b:11004](#)
- [Burde 1969] K. Burde, "Ein rationales biquadratisches Reziprozitätsgesetz", *J. Reine Angew. Math.* **235** (1969), 175–184. [MR 39 #2694](#)
- [Evans 1981] R. J. Evans, "Rational reciprocity laws", *Acta Arith.* **39**:3 (1981), 281–294. [MR 83h:10006](#) [MR 83h:10006](#) [Zbl 0472.10006](#)
- [Evans 1989] R. Evans, "Residuacity of primes", *Rocky Mountain J. Math.* **19**:4 (1989), 1069–1081. [MR 90m:11008](#) [Zbl 0699.10012](#)
- [Gallian 2010] J. Gallian, *Contemporary Abstract Algebra*, 7th ed., Brooks Cole, Belmont, CA, 2010.

- [Janusz 1996] G. J. Janusz, *Algebraic number fields*, 2nd ed., Graduate Studies in Mathematics 7, American Mathematical Society, Providence, RI, 1996. [MR 96j:11137](#) [Zbl 0854.11001](#)
- [Lehmer 1958] E. Lehmer, “Criteria for cubic and quartic residuacity”, *Mathematika* **5** (1958), 20–29. [MR 20 #1668](#) [Zbl 0102.28002](#)
- [Lehmer 1978] E. Lehmer, “Rational reciprocity laws”, *Amer. Math. Monthly* **85**:6 (1978), 467–472. [MR 58 #16482](#) [Zbl 0383.10003](#)
- [Lemmermeyer 1994] F. Lemmermeyer, “Rational quartic reciprocity”, *Acta Arith.* **67**:4 (1994), 387–390. [MR 95m:11010](#) [Zbl 0833.11049](#)
- [Lemmermeyer 2000] F. Lemmermeyer, *Reciprocity laws: From Euler to Eisenstein*, Springer, Berlin, 2000. [MR 2001i:11009](#) [Zbl 0949.11002](#)
- [Leonard and Williams 1977] P. A. Leonard and K. S. Williams, “A rational sixteenth power reciprocity law”, *Acta Arith.* **33**:4 (1977), 365–377. [MR 57 #219](#) [Zbl 0363.10003](#)
- [Ribenoim 2001] P. Ribenoim, *Classical theory of algebraic numbers*, Universitext, Springer, New York, 2001. [MR 2002e:11001](#) [Zbl 1082.11065](#)
- [Scholz 1934] A. Scholz, “Über die Lösbarkeit der Gleichung  $t^2 - Du^2 = -4$ ”, *Math. Z.* **39** (1934), 95–111.
- [Williams 1976] K. S. Williams, “A rational octic reciprocity law”, *Pacific J. Math.* **63**:2 (1976), 563–570. [MR 54 #2568](#) [Zbl 0311.10004](#)
- [Williams et al. 1985] K. S. Williams, K. Hardy, and C. Friesen, “On the evaluation of the Legendre symbol  $((A + B\sqrt{m})/p)$ ”, *Acta Arith.* **45**:3 (1985), 255–272. [MR 87b:11006](#) [Zbl 0524.10002](#)
- [Wu 1975] P. Wu, “A rational reciprocity law”, Ph.D. thesis, University of Southern California, Los Angeles, 1975.

Received: 2009-04-27      Accepted: 2010-09-20

[mrbudden@email.wcu.edu](mailto:mrbudden@email.wcu.edu)

*Department of Mathematics and Computer Science,  
Western Carolina University, Cullowhee, NC 28723,  
United States*

[ac0428@students.armstrong.edu](mailto:ac0428@students.armstrong.edu)

*Department of Mathematics,  
Armstrong Atlantic State University, 11935 Abercorn St.,  
Savannah, GA 31419, United States*

[ke3203@students.armstrong.edu](mailto:ke3203@students.armstrong.edu)

*Department of Mathematics,  
Armstrong Atlantic State University, 11935 Abercorn St.,  
Savannah, GA 31419, United States*

[ss7965@students.armstrong.edu](mailto:ss7965@students.armstrong.edu)

*Department of Mathematics,  
Armstrong Atlantic State University, 11935 Abercorn St.,  
Savannah, GA 31419, United States*

## EDITORS

### MANAGING EDITOR

Kenneth S. Berenhaut, Wake Forest University, USA, [berenhks@wfu.edu](mailto:berenhks@wfu.edu)

### BOARD OF EDITORS

John V. Baxley	Wake Forest University, NC, USA <a href="mailto:baxley@wfu.edu">baxley@wfu.edu</a>	Chi-Kwong Li	College of William and Mary, USA <a href="mailto:ckli@math.wm.edu">ckli@math.wm.edu</a>
Arthur T. Benjamin	Harvey Mudd College, USA <a href="mailto:benjamin@hmc.edu">benjamin@hmc.edu</a>	Robert B. Lund	Clemson University, USA <a href="mailto:lund@clemson.edu">lund@clemson.edu</a>
Martin Bohner	Missouri U of Science and Technology, USA <a href="mailto:bohner@mst.edu">bohner@mst.edu</a>	Gaven J. Martin	Massey University, New Zealand <a href="mailto:g.j.martin@massey.ac.nz">g.j.martin@massey.ac.nz</a>
Nigel Boston	University of Wisconsin, USA <a href="mailto:boston@math.wisc.edu">boston@math.wisc.edu</a>	Mary Meyer	Colorado State University, USA <a href="mailto:meyer@stat.colostate.edu">meyer@stat.colostate.edu</a>
Amarjit S. Budhiraja	U of North Carolina, Chapel Hill, USA <a href="mailto:budhiraj@email.unc.edu">budhiraj@email.unc.edu</a>	Emil Minchev	Ruse, Bulgaria <a href="mailto:eminchev@hotmail.com">eminchev@hotmail.com</a>
Pietro Cerone	Victoria University, Australia <a href="mailto:pietro.cerone@vu.edu.au">pietro.cerone@vu.edu.au</a>	Frank Morgan	Williams College, USA <a href="mailto:frank.morgan@williams.edu">frank.morgan@williams.edu</a>
Scott Chapman	Sam Houston State University, USA <a href="mailto:scott.chapman@shsu.edu">scott.chapman@shsu.edu</a>	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran <a href="mailto:moslehian@ferdowsi.um.ac.ir">moslehian@ferdowsi.um.ac.ir</a>
Jem N. Corcoran	University of Colorado, USA <a href="mailto:corcoran@colorado.edu">corcoran@colorado.edu</a>	Zuhair Nashed	University of Central Florida, USA <a href="mailto:znashed@mail.ucf.edu">znashed@mail.ucf.edu</a>
Michael Dorff	Brigham Young University, USA <a href="mailto:mdorff@math.byu.edu">mdorff@math.byu.edu</a>	Ken Ono	University of Wisconsin, USA <a href="mailto:ono@math.wisc.edu">ono@math.wisc.edu</a>
Sever S. Dragomir	Victoria University, Australia <a href="mailto:sever@matilda.vu.edu.au">sever@matilda.vu.edu.au</a>	Joseph O'Rourke	Smith College, USA <a href="mailto:orourke@cs.smith.edu">orourke@cs.smith.edu</a>
Behrouz Emamizadeh	The Petroleum Institute, UAE <a href="mailto:bemamizadeh@pi.ac.ae">bemamizadeh@pi.ac.ae</a>	Yuval Peres	Microsoft Research, USA <a href="mailto:peres@microsoft.com">peres@microsoft.com</a>
Errin W. Fulp	Wake Forest University, USA <a href="mailto:fulp@wfu.edu">fulp@wfu.edu</a>	Y.-F. S. Pétermann	Université de Genève, Switzerland <a href="mailto:petermann@math.unige.ch">petermann@math.unige.ch</a>
Andrew Granville	Université Montréal, Canada <a href="mailto:andrew@dms.umontreal.ca">andrew@dms.umontreal.ca</a>	Robert J. Plemmons	Wake Forest University, USA <a href="mailto:plemmons@wfu.edu">plemmons@wfu.edu</a>
Jerrold Griggs	University of South Carolina, USA <a href="mailto:griggs@math.sc.edu">griggs@math.sc.edu</a>	Carl B. Pomerance	Dartmouth College, USA <a href="mailto:carl.pomerance@dartmouth.edu">carl.pomerance@dartmouth.edu</a>
Ron Gould	Emory University, USA <a href="mailto:rg@mathcs.emory.edu">rg@mathcs.emory.edu</a>	Bjorn Poonen	UC Berkeley, USA <a href="mailto:poonen@math.berkeley.edu">poonen@math.berkeley.edu</a>
Sat Gupta	U of North Carolina, Greensboro, USA <a href="mailto:sgupta@uncg.edu">sgupta@uncg.edu</a>	James Propp	U Mass Lowell, USA <a href="mailto:jpropp@cs.uml.edu">jpropp@cs.uml.edu</a>
Jim Haglund	University of Pennsylvania, USA <a href="mailto:jhaglund@math.upenn.edu">jhaglund@math.upenn.edu</a>	József H. Przytycki	George Washington University, USA <a href="mailto:przytyck@gwu.edu">przytyck@gwu.edu</a>
Johnny Henderson	Baylor University, USA <a href="mailto:johnny_henderson@baylor.edu">johnny_henderson@baylor.edu</a>	Richard Rebarber	University of Nebraska, USA <a href="mailto:rrebarbe@math.unl.edu">rrebarbe@math.unl.edu</a>
Natalia Hritonenko	Prairie View A&M University, USA <a href="mailto:nahritonenko@pvamu.edu">nahritonenko@pvamu.edu</a>	Robert W. Robinson	University of Georgia, USA <a href="mailto:rwr@cs.uga.edu">rwr@cs.uga.edu</a>
Charles R. Johnson	College of William and Mary, USA <a href="mailto:crjohnso@math.wm.edu">crjohnso@math.wm.edu</a>	Filip Saidak	U of North Carolina, Greensboro, USA <a href="mailto:f.saidak@uncg.edu">f.saidak@uncg.edu</a>
Karen Kafadar	University of Colorado, USA <a href="mailto:karen.kafadar@cudenver.edu">karen.kafadar@cudenver.edu</a>	Andrew J. Sterge	Honorary Editor <a href="mailto:andy@ajsterge.com">andy@ajsterge.com</a>
K. B. Kulasekera	Clemson University, USA <a href="mailto:kk@ces.clemson.edu">kk@ces.clemson.edu</a>	Ann Trenk	Wellesley College, USA <a href="mailto:atrenk@wellesley.edu">atrenk@wellesley.edu</a>
Gerry Ladas	University of Rhode Island, USA <a href="mailto:gladas@math.uri.edu">gladas@math.uri.edu</a>	Ravi Vakil	Stanford University, USA <a href="mailto:vakil@math.stanford.edu">vakil@math.stanford.edu</a>
David Larson	Texas A&M University, USA <a href="mailto:larson@math.tamu.edu">larson@math.tamu.edu</a>	Ram U. Verma	University of Toledo, USA <a href="mailto:verma99@msn.com">verma99@msn.com</a>
Suzanne Lenhart	University of Tennessee, USA <a href="mailto:lenhart@math.utk.edu">lenhart@math.utk.edu</a>	John C. Wierman	Johns Hopkins University, USA <a href="mailto:wierman@jhu.edu">wierman@jhu.edu</a>

## PRODUCTION

Silvio Levy, Scientific Editor

Sheila Newbery, Senior Production Editor

Cover design: ©2008 Alex Scorpan

See inside back cover or <http://pjm.math.berkeley.edu/involve> for submission instructions.

The subscription price for 2010 is US \$100/year for the electronic version, and \$120/year (+\$20 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY  
 **mathematical sciences publishers**  
<http://www.mathscipub.org>

A NON-PROFIT CORPORATION

Typeset in L<sup>A</sup>T<sub>E</sub>X

Copyright ©2010 by Mathematical Sciences Publishers

# involve

2010

vol. 3

no. 3

Gracefulness of families of spiders	241
PATRICK BAHLS, SARA LAKE AND ANDREW WERTHEIM	
Rational residuacity of primes	249
MARK BUDDEN, ALEX COLLINS, KRISTIN ELLIS LEA AND STEPHEN SAVIOLI	
Coexistence of stable ECM solutions in the Lang–Kobayashi system	259
ERICKA MOCHAN, C. DAVIS BUENGER AND TAMAS WIANDT	
A complex finite calculus	273
JOSEPH SEABORN AND PHILIP MUMMERT	
$\zeta(n)$ via hyperbolic functions	289
JOSEPH D’AVANZO AND NIKOLAI A. KRYLOV	
Infinite family of elliptic curves of rank at least 4	297
BARTOSZ NASKRĘCKI	
Curvature measures for nonlinear regression models using continuous designs with applications to optimal experimental design	317
TIMOTHY O’BRIEN, SOMSRI JAMROENPINYO AND CHINNAPHONG BUMRUNGSUP	
Numerical semigroups from open intervals	333
VADIM PONOMARENKO AND RYAN ROSENBAUM	
Distinct solution to a linear congruence	341
DONALD ADAMS AND VADIM PONOMARENKO	
A note on nonresidually solvable hyperlinear one-relator groups	345
JON P. BANNON AND NICOLAS NOBLETT	