International Journal of Number Theory
Vol. 11, No. 8 (2015) 2487–2503

DOI: 10.1142/S1793042115501158

World Scientific
www.worldscientific.com

Quartic residuacity and the quadratic character of certain quadratic irrationalities

Ronald J. Evans

Department of Mathematics
University of California San Diego
La Jolla, CA 92093, USA
revans@ucsd.edu

Kenneth S. Williams

School of Mathematics and Statistics
Carleton University
Ottawa, ON, Canada K1S 5B6
kwilliam@connect.carleton.ca

Received 6 February 2014
Accepted 5 February 2015
Published 4 August 2015

We prove a general theorem that evaluates the Legendre symbol $(\frac{A+B\sqrt{m}}{p})$ under certain conditions on the integers A, B, m and the prime p. The evaluation is in terms of parameters appearing in a binary quadratic form representing p. The theorem has applications to quartic residuacity.

Keywords: Quadratic character; quartic residuacity; irrationalities; fundamental unit; discriminant; binary quadratic forms; Gauss's theory of genera.

Mathematics Subject Classification 2010: 11A15, 11E25

1. Introduction

Various Legendre symbols of the form $(\frac{A+B\sqrt{m}}{p})$ have been evaluated in the literature; see for example [6, 9, 11, 13, 17–20, 22]. For a survey on the determination of such symbols, see [10]. The main result of our paper is a general theorem that evaluates a large class of Legendre symbols $(\frac{A+B\sqrt{m}}{p})$ in terms of parameters occurring in binary quadratic forms representing the prime p. Our theorem is very different from those in the papers cited above.

In this section, we state our theorem and give an application to quartic residuacity. In Sec. 2, we prove the theorem. Then in Sec. 3, we present interesting examples as corollaries. Special cases of some of our corollaries embrace results in the literature that were obtained by different methods. Corollaries 11–14 provide

infinite classes of examples of our theorem, as well as infinite classes of quartic residuacity criteria.

Our theorem makes use of the Kronecker symbol

$$K(x,y) := \left(\frac{x}{y}\right),$$

as defined in [3, p. 28] for arbitrary integers x, y. Recall that the Kronecker symbol coincides with the Jacobi symbol whenever the latter is defined. For $(x,y)=1$, the generalized quadratic reciprocity law

$$\left(\frac{x}{y}\right) = \left(\frac{yK(-1,y)}{x}\right) \tag{1.1}$$

holds if and only if x and y are not both negative [3, p. 44]. We will need the following periodicity property for the "numerator":

$$\left(\frac{x+yz}{z}\right) = \left(\frac{x}{z}\right) w_z(x,y), \quad \text{when } z>0 \text{ and } (x,z)=1, \tag{1.2}$$

where

$$w_z(x,y) = \begin{cases} -1 & \text{if } 2\|z, 4\nmid y, \quad \text{and} \quad 4\nmid (x+yz/2), \\ 1 & \text{otherwise.} \end{cases} \tag{1.3}$$

This is easily proved by factoring the "denominator" z into a power of two times an odd integer. A useful formula for $w_z(x,y)$ is given by

$$w_z(x,y) = (-1)^{y(2x+yz)/4}, \quad \text{when } 2\|z. \tag{1.4}$$

Theorem. *Let $\delta \in \{\pm 1, \pm 2\}$ and let a,b,c,d,r,s and t be nonzero integers such that*

$$acr^2 - bds^2 = \delta t^2 \tag{1.5}$$

and

$$a>0, \quad d>0, \quad r>0, \quad s>0, \quad (a,s)=(d,r)=(r,s)=1. \tag{1.6}$$

Let p be an odd prime such that

$$\left(\frac{ac\delta}{p}\right) = \left(\frac{bd\delta}{p}\right) = 1, \quad p\nmid t, \tag{1.7}$$

so that $\sqrt{abcd}$ can be taken as an integer whose square equals $abcd$ modulo p. Suppose that

$$p = cde^2 - abf^2, \tag{1.8}$$

where e and f are integers such that

$$e>0, \quad f>0. \tag{1.9}$$

Define A and B by

$$A := rce + sbf, \quad B := sde + raf. \tag{1.10}$$

Then

$$\left(\frac{rac + s\sqrt{abcd}}{p}\right) = \left(\frac{cK(-1,p)}{f}\right)\left(\frac{\delta K(-1,adp)}{B}\right)\left(\frac{rK(-1,af)}{d}\right)\left(\frac{se}{a}\right) \times \left(\frac{c}{p}\right) w_f(cde^2, -abf) w_B(adA^2, -bcB) w_a(sde, rf) w_d(raf, se), \tag{1.11}$$

independent of the choice of square root of $abcd$ modulo p.

While the right side of (1.11) does not look particularly simple, many choices of the parameters yield elegant evaluations. This is illustrated in Sec. 3.

By (1.5) and (1.7), we have

$$\left(\frac{rac + s\sqrt{abcd}}{p}\right)\left(\frac{rac - s\sqrt{abcd}}{p}\right) = \left(\frac{r^2a^2c^2 - s^2abcd}{p}\right) = \left(\frac{ac\delta}{p}\right) = 1,$$

so that

$$\left(\frac{rac + s\sqrt{abcd}}{p}\right) = \left(\frac{rac - s\sqrt{abcd}}{p}\right). \tag{1.12}$$

Thus the Legendre symbol on the left side of (1.11) is independent of the choice of the integer $\sqrt{abcd}$ modulo p.

Suppose for the moment that $p \equiv 1 \pmod 4$. Define $\sigma := \operatorname{sgn} bc$. Then by (1.5),

$$\left(\frac{\sqrt{abcd}}{p}\right) = \left(\frac{rac - \sigma s\sqrt{abcd}}{p}\right)\left(\frac{sbd\sigma + r\sqrt{abcd}}{p}\right)\left(\frac{\delta}{p}\right). \tag{1.13}$$

The first symbol on the right side of (1.13) can be evaluated using (1.11), in view of (1.12). If in addition to the hypotheses of the theorem, we have

$$(b, r) = (c, s) = 1, \tag{1.14}$$

then the second symbol on the right side of (1.13) can also be evaluated using (1.11), as follows: in (1.11), replace a by $|b|$; b by $a \operatorname{sgn} b$; c by $d \operatorname{sgn} c$; d by $|c|$; r by s; s by r; and δ by $-\delta\sigma$. As a result, when (1.14) holds and $p \equiv 1 \pmod 4$, our theorem can be applied to evaluate the right side of (1.13), thus providing general criteria for the quartic residuacity of integers having the form $abcd$ modulo p. Examples of quartic residuacity criteria are given throughout Sec. 3.

If in addition to the hypotheses of the theorem, we have

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

then $\sqrt{ab}$ and $\sqrt{cd}$ may be taken as integers whose squares respectively equal ab and cd modulo p. In that case, from (1.11) and the identities

$$\left(\frac{ra\sqrt{cd}+sd\sqrt{ab}}{p}\right)=\left(\frac{c}{p}\right)\left(\frac{\sqrt{cd}}{p}\right)\left(\frac{rac+s\sqrt{abcd}}{p}\right), \tag{1.15}$$

$$\left(\frac{rc\sqrt{ab}+sb\sqrt{cd}}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{\sqrt{ab}}{p}\right)\left(\frac{rac+s\sqrt{abcd}}{p}\right), \tag{1.16}$$

we can give evaluations of the symbols on the left sides of (1.15) and (1.16), independent of the choice of square roots of ab and cd modulo p.

2. Proof of Theorem

From (1.7) and (1.8), we have

$$(abf, cde) = (p, e) = (p, f) = (p, abcd) = 1. \tag{2.1}$$

From (1.5), (1.8) and (1.10), we deduce

$$\delta pt^2 = adA^2 - bcB^2. \tag{2.2}$$

Note that by (1.6), (1.9) and (1.10),

$$B > 0. \tag{2.3}$$

Since $p \neq 2$, $\delta \in \{\pm 1, \pm 2\}$, and $p \nmid abcdt$, it follows from (2.2) that

$$(p, A) = (p, B) = 1. \tag{2.4}$$

Next we show that

$$g := (A, B) = 1. \tag{2.5}$$

From (1.10), we have the two congruences

$$rce \equiv -sbf \pmod{g}, \quad sde \equiv -raf \pmod{g}. \tag{2.6}$$

Multiplying them together, we obtain $rs(cde^2 - abf^2) \equiv 0 \pmod{g}$ so that by (1.8), $rsp \equiv 0 \pmod{g}$. Since $(g, p) = 1$ by (2.4), it follows that $g \mid rs$. By (2.6), $g \mid bfs^2$ and $g \mid des^2$, so that by (1.8), $g \mid ps^2$. Thus $g \mid s^2$. Also by (2.6), $g \mid cer^2$ and $g \mid afr^2$, so that by (1.8), $g \mid pr^2$. Thus $g \mid r^2$. Since $(r^2, s^2) = 1$ by (1.6), we have $g = 1$. This completes the proof of (2.5).

Now we show that

$$h := (B, t) = 1. \tag{2.7}$$

By (2.2), we have $h \mid adA^2$. Since (h, a) divides both B and a, it follows from (1.10) that $(h, a) \mid sde$. Thus, by (1.8), $(h, a) \mid sp$. But $p \nmid a$ so $(h, a) \mid s$. Since $(a, s) = 1$ by (1.6), we have $(h, a) = 1$. Hence $h \mid dA^2$, so that $h \mid d(A^2, B)$. But $(A, B) = 1$ by (2.5), so we have $h \mid d$. As $h \mid B$ and $h \mid d$, we have from (1.10) that $h \mid raf$. Since

$(d,r)=1$ by (1.6) and $h \mid d$, we have $(h,r)=1$. Thus $h \mid af$. It follows that $h \mid (d, af)$, so that $h=1$ by (2.1). This proves (2.7).

From (1.8), we have

$$\pm f\sqrt{abcd} \equiv cde \pmod{p}. \tag{2.8}$$

By (1.12), (2.1) and (2.8), it follows that

$$\left(\frac{rac+s\sqrt{abcd}}{p}\right) = \left(\frac{f}{p}\right)\left(\frac{\pm sf\sqrt{abcd}+racf}{p}\right) = \left(\frac{c}{p}\right)\left(\frac{f}{p}\right)\left(\frac{B}{p}\right). \tag{2.9}$$

We proceed to evaluate $(\frac{f}{p})$ and $(\frac{B}{p})$. By (1.1) and (1.8),

$$\left(\frac{f}{p}\right) = \left(\frac{pK(-1,p)}{f}\right) = \left(\frac{K(-1,p)}{f}\right)\left(\frac{cde^2-abf^2}{f}\right),$$

so that by application of (1.2) to the rightmost symbol, we obtain

$$\left(\frac{f}{p}\right) = \left(\frac{cdK(-1,p)}{f}\right) w_f(cde^2, -abf). \tag{2.10}$$

By (1.1), (2.2) and (2.7),

$$\left(\frac{B}{p}\right) = \left(\frac{pK(-1,p)}{B}\right) = \left(\frac{\delta K(-1,p)}{B}\right)\left(\frac{adA^2-bcB^2}{B}\right),$$

so that by application of (1.2) to the rightmost symbol, we obtain

$$\left(\frac{B}{p}\right) = \left(\frac{a}{B}\right)\left(\frac{d}{B}\right)\left(\frac{\delta K(-1,p)}{B}\right) w_B(adA^2, -bcB). \tag{2.11}$$

Arguing in the same fashion, we obtain

$$\left(\frac{a}{B}\right) = \left(\frac{K(-1,a)}{B}\right)\left(\frac{sde}{a}\right) w_a(sde, rf) \tag{2.12}$$

and

$$\left(\frac{d}{B}\right) = \left(\frac{K(-1,d)}{B}\right)\left(\frac{raf}{d}\right) w_d(raf, se). \tag{2.13}$$

By (1.1),

$$\left(\frac{a}{d}\right)\left(\frac{d}{a}\right)\left(\frac{f}{d}\right)\left(\frac{d}{f}\right) = \left(\frac{K(-1,af)}{d}\right). \tag{2.14}$$

The desired result (1.11) now follows by combining (2.9)–(2.14). □

3. Special Cases of Theorem

The first ten corollaries below involve discriminants Δ of binary quadratic forms for which there is one form class per form genus. For those without ready access to Pari or Sage, this can be checked for $|\Delta| \leq 200$ with the tables in [16, pp. 383–386]. Those tables also indicate the form classes. More extensive tables of form class numbers (with $-1500 \leq \Delta \leq 1600$) may be found in [7, pp. 194–203], and the formula in [13, Theorem 2.1] gives the sizes of corresponding groups of genera. For example, when $\Delta = 240$ as in Corollary 9, the form class number is 4 and there are four genera. The significance of "one class per genus" is that, by Gauss's theory of genera [5, p. 221; 16, p. 186; 7, p. 147] the congruence conditions for p in our corollaries determine the binary quadratic form class representing p.

There are infinitely many examples with one class per genus that we could choose from, because there exist infinite sets of positive discriminants with one class per genus. Explicit examples of such sets are given in [4, Sec. 4]. It is conjectured that there exist infinitely many positive *fundamental* discriminants with one class per genus. (Of course this would be proved if one could prove the existence of infinitely many real quadratic fields with class number 1.) The situation is different for negative discriminants. Flath [7, p. 198] lists 101 negative discriminants with one class per genus, and it is conjectured that this list is complete.

For any nonzero integer y modulo p, we write $\sqrt{y}$ to denote either of the two square roots of y modulo p. As in [2, p. 251], when u is a square modulo a prime $p \equiv 1 \pmod 4$ with $(u, p) = 1$, we define

$$\left(\frac{u}{p}\right)_4 = \begin{cases} 1 & \text{if } u \text{ is a quartic residue modulo } p, \\ -1 & \text{otherwise.} \end{cases}$$

If m is a positive squarefree integer, we write ϵ_m for the fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{m})$.

Our first corollary is essentially equivalent to the classical result in algebraic number theory that an odd prime p splits completely in $\mathbb{Q}(\sqrt{2+\sqrt{2}}) = \mathbb{Q}(\cos(2\pi/16))$ if and only if $p \equiv \pm 1 \pmod{16}$ [14, p. 247]. Corollary 13 will significantly extend Corollary 1.

Corollary 1. *Let p be a prime with $p \equiv 1$ or $7 \pmod 8$ so that 2 is a square modulo p. Then*

$$\left(\frac{2+\sqrt{2}}{p}\right) = \begin{cases} (-1)^{(p-1)/8} & \text{if } p \equiv 1 \pmod 8, \\ (-1)^{(p+1)/8} & \text{if } p \equiv 7 \pmod 8, \end{cases} \tag{3.1}$$

and

$$\left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{\epsilon_2}{p}\right) = \begin{cases} (-1)^{(p-1)/8}\left(\dfrac{2}{p}\right)_4 & \text{if } p \equiv 1 \pmod 8, \\ (-1)^{(p+1)/8}\left(\dfrac{\sqrt{2}}{p}\right) & \text{if } p \equiv 7 \pmod 8. \end{cases} \tag{3.2}$$

In the last equality it is understood that the choice of $\sqrt{2}$ *modulo* p *on the left side is the same as that on the right side.*

Proof. In (1.5), choose $a = 2$ and let each of the seven other parameters equal 1. Let p be a prime such that $(\frac{2}{p}) = 1$, so that $p \equiv 1$ or 7 (mod 8) and (1.7) holds. From the table in [16] for discriminant 8, there are positive integers e and f such that

$$p = e^2 - 2f^2,$$

i.e. (1.8) holds. Clearly e and $B = e + 2f$ are odd, and

$$\begin{cases} f \equiv 0 \pmod 2 & \text{if } p \equiv 1 \pmod 8, \\ f \equiv 1 \pmod 2 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

First suppose that $p \equiv 1$ (mod 8), so that f is even. The theorem gives

$$\left(\frac{2+\sqrt{2}}{p}\right) = \left(\frac{e}{2}\right) w_2(e,f) = \left(\frac{2}{e}\right)(-1)^{f/2}.$$

Since

$$\left(\frac{2}{e}\right)(-1)^{f/2} = (-1)^{(4f+e^2-1)/8} = (-1)^{(4f+2f^2+p-1)/8} = (-1)^{(p-1)/8},$$

we obtain (3.1) when $p \equiv 1$ (mod 8).

Now suppose that $p \equiv 7$ (mod 8), so that f is odd. In view of (1.4), the theorem gives

$$\left(\frac{2+\sqrt{2}}{p}\right) = \left(\frac{-1}{fB}\right)\left(\frac{e}{2}\right) w_2(e,f) = \left(\frac{-1}{fB}\right)\left(\frac{2}{e}\right)(-1)^{(e+f)/2} = \left(\frac{2}{e}\right).$$

Since

$$\left(\frac{2}{e}\right) = (-1)^{(e^2-1)/8} = (-1)^{(p+2f^2-1)/8} = (-1)^{(p+1)/8},$$

we obtain (3.1) when $p \equiv 7$ (mod 8).

Finally, (3.2) follows by multiplying both sides of (3.1) by $(\frac{\sqrt{2}}{p})$, since $(\frac{2}{p})_4 = (\frac{\sqrt{2}}{p})$ when $p \equiv 1$ (mod 8). □

We remark that when p is a prime with $p \equiv 1$ (mod 8), it is a result going back to Gauss and Dirichlet that

$$\left(\frac{2}{p}\right)_4 = (-1)^{\frac{p-1}{8}+D},$$

where $p = C^2 + 8D^2$; see for example [10, Proposition 5.4, p. 156; 2, p. 226]. Then from (3.2) we deduce

$$\left(\frac{\epsilon_2}{p}\right) = (-1)^D,$$

which is a result of Barrucand and Cohn [1, 21].

There are two genera of classes of forms of discriminant 24. The principal genus contains the class of the form $x^2 - 6y^2$ and the nonprincipal genus contains the class of the form $-x^2 + 6y^2$. The next two corollaries involve the representations of primes p by each of these two forms $x^2 - 6y^2$ and $-(x^2 - 6y^2)$.

Corollary 2. *Let p be a prime congruent to 1 or 19 modulo 24, so that 6 is a square modulo p. Then there are positive integers e and f satisfying*

$$p = e^2 - 6f^2 \tag{3.3}$$

such that

$$\left(\frac{2+\sqrt{6}}{p}\right) = \begin{cases} (-1)^{(p-1)/8}\left(\dfrac{-1}{e}\right) & \text{if } p \equiv 1 \pmod{24}, \\ (-1)^{(p-3)/8}\left(\dfrac{-1}{e}\right) & \text{if } p \equiv 19 \pmod{24}, \end{cases} \tag{3.4}$$

and

$$\left(\frac{3+\sqrt{6}}{p}\right) = \begin{cases} (-1)^{(p-1)/8}\left(\dfrac{-1}{e}\right)\left(\dfrac{6}{p}\right)_4 & \text{if } p \equiv 1 \pmod{24}, \\ (-1)^{(p+5)/8}\left(\dfrac{-1}{e}\right)\left(\dfrac{\sqrt{6}}{p}\right) & \text{if } p \equiv 19 \pmod{24}. \end{cases} \tag{3.5}$$

Proof. Choose

$$a = 2, \quad b = 3, \quad c = d = r = s = t = 1, \quad \delta = -1.$$

Then (3.3) holds, in view of the table in [16] for discriminant 24. From (3.3), we see that e and $B = e + 2f$ are both odd, and

$$\begin{cases} f \equiv 0 \pmod 2 & \text{if } p \equiv 1 \pmod{24}, \\ f \equiv 1 \pmod 2 & \text{if } p \equiv 19 \pmod{24}. \end{cases}$$

If $p \equiv 1 \pmod{24}$, so that f is even, then

$$w_2(e, f) = (-1)^{f/2},$$

so that the theorem gives

$$\left(\frac{2+\sqrt{6}}{p}\right) = \left(\frac{-1}{B}\right)\left(\frac{e}{2}\right) w_2(e, f) = (-1)^{f/2}\left(\frac{-2}{e}\right). \tag{3.6}$$

If $p \equiv 19 \pmod{24}$, so that f is odd, then

$$w_2(e, f) = (-1)^{(e+f)/2},$$

so that the theorem gives

$$\left(\frac{2+\sqrt{6}}{p}\right) = \left(\frac{-1}{f}\right)\left(\frac{e}{2}\right) w_2(e, f) = (-1)^{(e+2f-1)/2}\left(\frac{2}{e}\right). \tag{3.7}$$

Suppose first that $p \equiv 1 \pmod{24}$. By (3.3),

$$\left(\frac{2}{e}\right) = (-1)^{(6f^2+p-1)/8} = (-1)^{f/2}(-1)^{(p-1)/8},$$

so that by (3.6),

$$\left(\frac{2+\sqrt{6}}{p}\right) = (-1)^{(p-1)/8}\left(\frac{-1}{e}\right).$$

This proves (3.4) in the case $p \equiv 1 \pmod{24}$. The case $p \equiv 19 \pmod{24}$ of (3.4) follows from (3.7) in a similar manner. Finally, (3.5) follows by multiplying (3.4) by $(\frac{\sqrt{6}}{p})$. □

Consider the special case of Corollary 2 where $p \equiv 1 \pmod{24}$. We have

$$\left(\frac{2+\sqrt{6}}{p}\right) = \left(\frac{(2+\sqrt{6})^2}{p}\right)_4 = \left(\frac{2(5+2\sqrt{6})}{p}\right)_4 = \left(\frac{2}{p}\right)_4\left(\frac{\epsilon_6}{p}\right)_4.$$

Hence, by (3.4),

$$\left(\frac{\epsilon_6}{p}\right)_4 = (-1)^{(p-1)/8}\left(\frac{-1}{e}\right)\left(\frac{2}{p}\right)_4, \quad \text{when } p \equiv 1 \pmod{24},$$

which is equivalent to a result of Leonard and Williams [11, p. 103]. See (3.13) for another formula for the left side of (3.5) when $p \equiv 1 \pmod{24}$.

Corollary 3. *Let $p \neq 5$ be a prime congruent to 5 modulo 24, so that 6 is a square modulo p. Then there are positive integers e and f (with e odd and f odd) satisfying*

$$-p = e^2 - 6f^2 \tag{3.8}$$

such that

$$\left(\frac{12+7\sqrt{6}}{p}\right) = \left(\frac{-1}{f}\right)\left(\frac{6}{e}\right). \tag{3.9}$$

Proof. Choose

$$a = 6, \quad b = c = -1, \quad d = 1, \quad r = 2, \quad s = 7, \quad t = 5, \quad \delta = 1.$$

Then (3.8) holds, in view of the table in [16] for discriminant 24. From (3.8) and the congruence $p \equiv 5 \pmod{8}$, we see that e, f and $B = 7e + 12f$ are odd. Since $w_6(7e, 2f) = -1$, the theorem gives

$$\left(\frac{12+7\sqrt{6}}{p}\right) = \left(\frac{-1}{fB}\right)\left(\frac{e}{6}\right)w_6(7e,2f) = -\left(\frac{-1}{efB}\right)\left(\frac{6}{e}\right). \tag{3.10}$$

We have

$$\left(\frac{-1}{B}\right) = \left(\frac{-1}{7e+12f}\right) = -\left(\frac{-1}{e}\right), \tag{3.11}$$

so we see that (3.9) follows from (3.10) and (3.11). □

It follows from Corollary 3 that

$$\left(\frac{6}{p}\right)_4 = \left(\frac{-1}{f}\right)\left(\frac{6}{e}\right),$$

since

$$\left(\frac{7+2\sqrt{6}}{p}\right) = \left(\frac{(1+\sqrt{6})^2}{p}\right) = 1.$$

Corollary 4. *Let p be a prime congruent to 1 or 23 modulo 24, so that 6 is a square modulo p. Then for each $\epsilon = \pm 1$, there are positive integers e and f satisfying*

$$p = \epsilon(e^2 - 24f^2) \tag{3.12}$$

and

$$\left(\frac{3+\sqrt{6}}{p}\right) = (-1)^f \left(\frac{3}{e}\right). \tag{3.13}$$

Proof. Choose

$$a = 6, \quad b = 4\epsilon, \quad c = \epsilon, \quad d = r = s = t = 1, \quad \delta = 2\epsilon.$$

Then (3.12) holds, in view of the table in [16] for discriminant 96. From (3.12), we see that e and $B = e + 6f$ are odd, and $p \equiv \epsilon \pmod 8$. The theorem gives

$$\left(\frac{6\epsilon + 2\sqrt{6}}{p}\right) = \left(\frac{\epsilon}{p}\right)\left(\frac{-2}{B}\right)\left(\frac{e}{6}\right) w_6(e,f).$$

Multiplying both sides by $(\frac{\epsilon}{p})$, we obtain

$$\left(\frac{6+2\sqrt{6}}{p}\right) = \left(\frac{-2}{B}\right)\left(\frac{e}{6}\right) w_6(e,f) = \left(\frac{-2}{Be}\right)\left(\frac{3}{e}\right) w_6(e,f).$$

Since $(\frac{-1}{Be}) = (-1)^f$, it remains to prove that

$$\left(\frac{2}{Be}\right) = w_6(e,f).$$

By (1.4), we have

$$\left(\frac{2}{Be}\right) = (-1)^{((e+6f)^2 - e^2)/8} = (-1)^{f(e+3f)/2} = w_6(e,f),$$

which completes the proof of (3.13). □

Consider the special case of Corollary 4 where $p \equiv 1 \pmod{24}$. Then by (3.6),

$$\left(\frac{2-\sqrt{6}}{p}\right) = (-1)^f \left(\frac{-2}{e}\right);$$

multiplying this by (3.13), we obtain the quartic residuacity criterion

$$\left(\frac{6}{p}\right)_4 = \left(\frac{-6}{e}\right).$$

For the proofs of all remaining corollaries except Corollary 11, we omit the details, giving only the values of the relevant parameters in (1.5).

Corollary 5. *Let p be a prime congruent to 1 modulo 24, so that -6 is a square modulo p. Then there are positive integers e and f (with e odd and f even) satisfying*

$$p = e^2 + 6f^2$$

and

$$\left(\frac{12+\sqrt{-6}}{p}\right) = \left(\frac{6}{e}\right).$$

Proof. Choose

$$a = 6, \quad b = -1, \quad c = d = s = 1, \quad r = 2, \quad t = 5, \quad \delta = 1. \qquad \square$$

As $(\frac{-2}{p}) = (\frac{3}{p}) = (\frac{6}{p}) = 1$, $(\frac{-1}{p})_4 = 1$ and $12+\sqrt{-6} = \sqrt{-6}(\sqrt{3}-\sqrt{-2})^2$, it follows from Corollary 5 that

$$\left(\frac{6}{p}\right)_4 = \left(\frac{-6}{p}\right)_4 = \left(\frac{\sqrt{-6}}{p}\right) = \left(\frac{12+\sqrt{-6}}{p}\right) = \left(\frac{6}{e}\right).$$

Corollary 6. *Let p be a prime congruent to $\pm 1, \pm 9$ or ± 25 modulo 56, so that 7 is a square modulo p. Then for each $\epsilon = \pm 1$, there are positive integers e and f (with e odd and f even) satisfying*

$$p = \epsilon(e^2 - 28f^2)$$

and

$$\left(\frac{3+\sqrt{7}}{p}\right) = (-1)^{f/2}\left(\frac{2}{e}\right).$$

Proof. Choose

$$a = 2, \quad b = 14\epsilon, \quad c = \epsilon, \quad d = s = 1, \quad r = 3, \quad t = 2, \quad \delta = \epsilon. \qquad \square$$

Consider the special case of Corollary 6 where $\epsilon = 1$, so that p is congruent to 1, 9 or 25 modulo 56. We have

$$\left(\frac{3+\sqrt{7}}{p}\right) = \left(\frac{(3+\sqrt{7})^2}{p}\right)_4 = \left(\frac{2(8+3\sqrt{7})}{p}\right)_4 = \left(\frac{2}{p}\right)_4\left(\frac{\epsilon_7}{p}\right)_4.$$

Hence, by Corollary 6, we obtain

$$\left(\frac{\epsilon_7}{p}\right)_4 = (-1)^{f/2}\left(\frac{2}{e}\right)\left(\frac{2}{p}\right)_4, \quad \text{when } p \equiv 1, 9 \text{ or } 25 \pmod{56},$$

which is equivalent to a result of Leonard and Williams [11, p. 103].

Corollary 7. *Let p be a prime congruent to $\pm 1, \pm 9$ or ± 25 modulo 56, so that 14 is a square modulo p. Then for each $\epsilon = \pm 1$, there are positive integers e and f (with e odd and f even) satisfying*

$$p = \epsilon(e^2 - 14f^2)$$

and

$$\left(\frac{4+\sqrt{14}}{p}\right) = \left(\frac{2}{e}\right).$$

Proof. Choose

$$a = 2, \quad b = 7\epsilon, \quad c = \epsilon, \quad d = s = t = 1, \quad r = 2, \quad \delta = \epsilon. \qquad \square$$

For $p \equiv 1, 9$ or $25 \pmod{56}$ we have

$$\left(\frac{4+\sqrt{14}}{p}\right) = \left(\frac{(4+\sqrt{14})^2}{p}\right)_4 = \left(\frac{2(15+4\sqrt{14})}{p}\right)_4 = \left(\frac{2}{p}\right)_4\left(\frac{\epsilon_{14}}{p}\right)_4.$$

Hence, by Corollary 7, we deduce

$$\left(\frac{\epsilon_{14}}{p}\right)_4 = \left(\frac{2}{e}\right)\left(\frac{2}{p}\right)_4, \quad \text{when } p \equiv 1, 9 \text{ or } 25 \pmod{56},$$

which is equivalent to a result of Leonard and Williams [11, p. 103].

Corollary 8. *Let p be a prime congruent to 1 or 9 modulo 40, so that 10 is a square modulo p. Then there are positive integers e and f (with e odd) satisfying*

$$p = e^2 - 40f^2$$

and

$$\left(\frac{\epsilon_{10}}{p}\right) = \left(\frac{3+\sqrt{10}}{p}\right) = \left(\frac{-1}{e}\right)(-1)^f.$$

Proof. Choose

$$a = 2, \quad b = 20, \quad c = d = s = 1, \quad r = 3, \quad t = 1, \quad \delta = -2. \qquad \square$$

Corollary 9. *Let p be a prime congruent to ± 1 or ± 49 modulo 120, so that 15 is a square modulo p. Then for each $\epsilon = \pm 1$ there are positive integers e and f (with e*

odd and f even) satisfying

$$p = \epsilon(15e^2 - 4f^2)$$

and

$$\left(\frac{5+\sqrt{15}}{p}\right) = \left(\frac{f}{5}\right)\left(\frac{2}{e}\right)(-1)^{f/2}.$$

Proof. Choose

$$a = 2, \quad b = 2\epsilon, \quad c = 5\epsilon, \quad d = 3, \quad r = s = 1, \quad t = 2, \quad \delta = \epsilon. \qquad \square$$

Consider the special case of Corollary 9 where $\epsilon = -1$, so that p is congruent to 1 or 49 modulo 120. With

$$a = 2, \quad b = -2, \quad c = -3, \quad d = 5, \quad r = s = 1, \quad t = 2, \quad \delta = 1,$$

the theorem gives

$$\left(\frac{3+\sqrt{15}}{p}\right) = \left(\frac{-3}{f}\right)\left(\frac{2}{e}\right)(-1)^{f/2}.$$

Together with Corollary 9, this yields the quartic residuacity formula

$$\left(\frac{15}{p}\right)_4 = \left(\frac{-15}{f}\right).$$

Corollary 10. *Let p be a prime congruent to $1, 9, 25, 49$ or 81 modulo 88, so that 22 is a square modulo p. Then there are positive integers e and f (with e odd and f odd) satisfying*

$$p = 11e^2 - 2f^2$$

and

$$\left(\frac{2+\sqrt{22}}{p}\right) = \left(\frac{-2}{e}\right).$$

Proof. Choose

$$a = 2, \quad b = c = 1, \quad d = 11, \quad r = s = 1, \quad t = 3, \quad \delta = -1. \qquad \square$$

Each of our last four corollaries below provides an infinite class of examples, one for each q. Every quadratic form in these corollaries represents infinitely many primes in any arithmetic progression compatible with the form's generic characters, by a classical theorem of Meyer [12]. (See [15, p. 72] for additional references.) Hence, no example below is vacuous.

Corollary 11. *For any fixed odd integer u, let $q := u^2+2$ (so that $q \equiv 3 \pmod 8$). Let p be a prime congruent to 1 modulo 8 with $(p, qu) = 1$ such that*

$$p = qe^2 - 2f^2$$

for positive odd integers e and f. Then

$$\left(\frac{2+\sqrt{2q}}{p}\right) = \left(\frac{-2}{e}\right), \quad \left(\frac{q+\sqrt{2q}}{p}\right) = \left(\frac{q}{f}\right), \tag{3.14}$$

and

$$\left(\frac{2q}{p}\right)_4 = \left(\frac{-2}{e}\right)\left(\frac{q}{f}\right). \tag{3.15}$$

Proof. To prove the first equality in (3.14), choose

$$a = 2, \quad b = c = 1, \quad d = q, \quad r = s = 1, \quad t = u, \quad \delta = -1.$$

Since e and q are odd, so is $B = qe + 2f$. By (1.4),

$$w_2(qe, f) = \left(\frac{-1}{ef}\right).$$

The theorem thus gives

$$\left(\frac{2+\sqrt{2q}}{p}\right) = \left(\frac{-1}{f}\right)\left(\frac{e}{2}\right) w_2(qe, f) = \left(\frac{-1}{e}\right)\left(\frac{e}{2}\right),$$

and the first equality in (3.14) follows. For the second equality in (3.14), choose

$$a = 1, \quad b = 2, \quad c = q, \quad d = r = s = 1, \quad t = u, \quad \delta = 1.$$

Then $B = e + f$ is even. By the theorem, the first factor on the right side of (1.11) equals $(\frac{q}{f})$, and each of the remaining eight factors equals 1. This proves the second equality in (3.14). Finally, (3.15) follows from the two equalities in (3.14). □

Observe that Corollary 10 can be deduced from the case $u = 3$ of Corollary 11. If $u = 1$ (so that $q = 3$ and $p \equiv 1 \pmod{24}$), then Corollary 11 shows that the unit $\sqrt{2} + \sqrt{3}$ satisfies

$$\left(\frac{\sqrt{2}+\sqrt{3}}{p}\right) = \left(\frac{2}{p}\right)_4 \left(\frac{-2}{e}\right) = \left(\frac{3}{p}\right)_4 \left(\frac{3}{f}\right).$$

Corollary 12. *For any fixed nonzero integer u, let $q := 4u^2+1$ (so that $q \equiv 1 \pmod 4$). Let p be a prime congruent to 1 modulo 4 with $(p, qu) = 1$ such that*

$$p = qe^2 - 4f^2$$

for positive integers e and f. Then

$$\left(\frac{1+\sqrt{q}}{p}\right) = \left(\frac{-1}{e}\right), \quad \left(\frac{q+\sqrt{q}}{p}\right) = \left(\frac{2f}{q}\right)(-1)^f, \tag{3.16}$$

and

$$\left(\frac{q}{p}\right)_4 = \left(\frac{-1}{e}\right)\left(\frac{2f}{q}\right)(-1)^f. \tag{3.17}$$

Proof. To prove the first equality in (3.16), choose

$$a = 2, \quad b = 2, \quad d = q, \quad c = r = s = 1, \quad t = 2u, \quad \delta = -2.$$

For the second equality in (3.16), choose

$$a = 2, \quad b = 2, \quad c = q, \quad d = r = s = 1, \quad t = 2u, \quad \delta = 2.$$

Finally, (3.17) follows from the two equalities in (3.16). □

Suppose that the prime p is congruent to 1 or 9 modulo 20. Then the hypotheses of Corollary 12 hold with $u = 1$ and $q = 5$, by the table in [16] for discriminant 80. Thus by (3.16),

$$\left(\frac{\epsilon_5}{p}\right) = \left(\frac{-1}{e}\right)\left(\frac{2}{p}\right). \tag{3.18}$$

This is equivalent to a result of Leonard and Williams [11, p. 102]. By (3.17),

$$\left(\frac{5}{p}\right)_4 = \left(\frac{-1}{e}\right)\left(\frac{f}{5}\right)(-1)^{f+1}. \tag{3.19}$$

(A different criterion for the quartic residuacity of 5 may be found in [2, p. 217].) Combining (3.18) and (3.19), we see that

$$\left(\frac{\epsilon_5}{p}\right) = \left(\frac{5}{p}\right)_4\left(\frac{2}{p}\right)\left(\frac{f}{5}\right)(-1)^{f+1} = \begin{cases} +\left(\dfrac{5}{p}\right)_4 & \text{if } p \equiv 1 \pmod{20}, \\ -\left(\dfrac{5}{p}\right)_4 & \text{if } p \equiv 9 \pmod{20}, \end{cases}$$

which is a result of Lehmer [8, Eq. (11)].

Corollary 13. *For any fixed odd integer u, let $q := u^2 - 2$ (so that $q \equiv 7 \pmod 8$). Let p be a prime with $(p, qu) = 1$ such that either*

$$p = qe^2 + 2f^2 \tag{3.20}$$

or

$$p = e^2 + 2qf^2 \tag{3.21}$$

for positive integers e and f. (In particular, $p \equiv \pm 1 \pmod 8$.) Then

$$\left(\frac{2+\sqrt{-2q}}{p}\right) = \begin{cases} \left(\dfrac{2}{e}\right) & \text{if } 2 \nmid f, \\ \left(\dfrac{2}{e}\right)(-1)^{f/2} & \text{if } 2 \mid f. \end{cases} \tag{3.22}$$

and when $p \equiv 1 \pmod 8$,

$$\left(\frac{q+\sqrt{-2q}}{p}\right) = \begin{cases} \left(\dfrac{q}{f}\right) & \text{if } 2 \nmid f, \\ \left(\dfrac{q}{e}\right)(-1)^{f/2} & \text{if } 2 \mid f. \end{cases} \tag{3.23}$$

Thus when $p \equiv 1 \pmod 8$, *we have*

$$\left(\frac{-2q}{p}\right)_4 = \begin{cases} \left(\dfrac{2}{e}\right)\left(\dfrac{q}{f}\right) & \text{if } 2 \nmid f, \\ \left(\dfrac{2q}{e}\right) & \text{if } 2 \mid f. \end{cases} \tag{3.24}$$

Proof. To prove (3.22) when (3.20) holds, choose

$$a = 2, \quad b = -1, \quad d = q, \quad c = r = s = 1, \quad t = u, \quad \delta = 1.$$

To prove (3.22) when (3.21) holds, choose

$$a = 2, \quad b = -q, \quad c = d = r = s = 1, \quad t = u, \quad \delta = 1.$$

Now suppose that $p \equiv 1 \pmod 8$. To prove (3.23) when (3.20) holds, choose

$$a = 1, \quad b = -2, \quad c = q, \quad d = r = s = 1, \quad t = u, \quad \delta = 1.$$

To prove (3.23) when (3.21) holds, choose

$$a = q, \quad b = -2, \quad c = d = r = s = 1, \quad t = u, \quad \delta = 1.$$

Finally, (3.24) follows by multiplying together (3.22) and (3.23). □

From the case $u = 1$ of (3.22), we can deduce (3.1).

Corollary 14. *For any fixed odd integer* u, *let* $q := (u^2+1)/2$ (*so that* $q \equiv 1 \pmod 4$). *Let* p *be a prime with* $(p, qu) = 1$ *such that*

$$p = e^2 - 2qf^2$$

for positive integers e *and* f (*so that* $p \equiv (-1)^f \pmod 8$). *Then*

$$\left(\frac{2q+\sqrt{2q}}{p}\right) = \begin{cases} \left(\dfrac{2q}{e}\right) & \text{if } 2 \nmid f, \\ \left(\dfrac{2q}{e}\right)(-1)^{f/2} & \text{if } 2 \mid f. \end{cases} \tag{3.25}$$

Moreover, when f *is even, we have*

$$\left(\frac{1+\sqrt{2q}}{p}\right) = \left(\frac{-1}{e}\right)(-1)^{f/2}, \quad \left(\frac{2q}{p}\right)_4 = \left(\frac{-2q}{e}\right). \tag{3.26}$$

Proof. To prove (3.25), choose

$$a = 2q, \quad b = c = d = r = s = 1, \quad t = u, \quad \delta = 1.$$

To prove (3.26) when f is even, choose

$$a = 1, \quad b = 2q, \quad c = d = r = s = 1, \quad t = u, \quad \delta = -1. \qquad \square$$

References

[1] P. Barrucand and H. Cohn, Note on primes of type $x^2 + 32y^2$, class number, and residuacity, *J. Reine Angew. Math.* **238** (1969) 67–70.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums* (Wiley-Interscience, New York, 1998).

[3] H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer, Berlin, 2000).

[4] H. Cohn, A numerical study of the relative class numbers of real quadratic integral domains, *Math. Comp.* **16** (1962) 127–140.

[5] ———, *Advanced Number Theory* (Dover, New York, 1980).

[6] R. J. Evans, Residuacity of primes, *Rocky Mountain J. Math.* **19** (1989) 1069–1081.

[7] D. Flath, *Introduction to Number Theory* (Wiley, New York, 1989).

[8] E. Lehmer, On the quadratic character of the Fibonacci root, *Fibonacci Quart.* **4** (1966) 135–138.

[9] F. Lemmermeyer, Rational quartic reciprocity II, *Acta Arith.* **80**(3) (1997) 273–276.

[10] ———, *Reciprocity Laws* (Springer, Berlin, 2000).

[11] P. A. Leonard and K. S. Williams, The quadratic and quartic character of certain quadratic units I, *Pacific J. Math.* **71** (1977) 101–106.

[12] A. Meyer, Über einen Satz von Dirichlet, *J. Reine Angew. Math.* **103** (1888) 98–117.

[13] R. A. Mollin and A. Srinivasan, Residuacity and genus theory of forms, *J. Number Theory* **132** (2012) 103–116.

[14] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers* (PWN, Warsaw, 1974).

[15] ———, *The Development of Prime Number Theory* (Springer, Berlin, 2000).

[16] H. E. Rose, *A Course in Number Theory* (Oxford University Press, Oxford, 1994).

[17] Z.-H. Sun, On the quadratic character of quadratic units, *J. Number Theory* **128** (2008) 1295–1335.

[18] ———, Congruences for $(A + \sqrt{A^2 + mB^2})^{(p-1)/2}$ and $(b + \sqrt{a^2 + b^2})^{(p-1)/4}$ (mod p), *Acta Arith.* **149**(3) (2011) 275–296.

[19] M. Tsunekawa, Relation entre $(\frac{a+\sqrt{m}}{p})$ et la loi des résidues quadratiques dans le champ de nombres quadratiques $R(\sqrt{m})$, *Bull. Nagoya Inst. Technol.* **7** (1955) 253–255 (English summary).

[20] H. C. Williams, The quadratic character of a certain quadratic surd, *Utilitas Math.* **5** (1974) 49–55.

[21] K. S. Williams, Note on a result of Barrucand and Cohn, *J. Reine Angew. Math.* **285** (1976) 218–220.

[22] K. S. Williams, K. Hardy and C. Friesen, On the evaluation of the Legendre symbol $(\frac{A+B\sqrt{m}}{p})$, *Acta Arith.* **45** (1985) 255–272.