ACTA ARITHMETICA
170.4 (2015)

Some new evaluations of the Legendre symbol $\left(\frac{a+b\sqrt{q}}{p}\right)$

by

Lerna Pehlivan (Halifax) and Kenneth S. Williams (Ottawa)

1. Introduction. The principal positive-definite integral binary quadratic form of discriminant d (< 0) is

$$p_d(x,y) := \begin{cases} x^2 - \frac{d}{4}y^2 & \text{if } d \equiv 0 \pmod 4, \\ x^2 + xy + \frac{1-d}{4}y^2 & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

It is well-known that if $d \in \{-3,-4,-7,-8,-11,-19,-43,-67,-163\}$ and p is an odd prime such that $\left(\frac{d}{p}\right) = 1$ then there are integers x and y such that $p = p_d(x,y)$. Moreover the number of such pairs of integers (x,y) is

$$\begin{cases} 12 & \text{if } d = -3, \\ 8 & \text{if } d = -4, \\ 4 & \text{if } d = -7,-8,-11,-19,-43,-67,-163, \end{cases}$$

by a theorem of Dirichlet (see [7]). Knowing the number of such pairs enables us to specify a unique solution (x,y) to $p = p_d(x,y)$ for each $d \in \{-3,-4,-7,-8,-11,-19,-43,-67,-163\}$. For these d, if A is an integer such that $p_d(A,1)$ (resp. $p_{-28}(A,1)$) if $d \neq -7$ (resp. $d = -7$) is an odd prime q, we show that for odd primes p satisfying $\left(\frac{d}{p}\right) = \left(\frac{q}{p}\right) = 1$ there are integers $r \equiv r(A)$ and $s \equiv s(A)$ such that the Legendre symbol $\left(\frac{r+s\sqrt{q}}{p}\right)$ is well-defined and nonzero whatever square root of q is taken modulo p, and we give its value explicitly. We prove nine theorems of this type, one for each of the nine values of d.

The central element in each of the proofs of our theorems is the law of quadratic reciprocity in the imaginary quadratic field

$$\begin{cases} \mathbb{Q}(\sqrt{d}) & \text{if } d = -3,-7,-11,-19,-43,-67,-163, \\ \mathbb{Q}(\sqrt{d/4}) & \text{if } d = -4,-8, \end{cases}$$

of class number 1. This law is due to Dörrie [4] and is stated in Section 2.

2010 *Mathematics Subject Classification*: Primary 11A15.
Key words and phrases: rational reciprocity laws, Dörrie's law of quadratic reciprocity, imaginary quadratic fields of class number 1, binary quadratic forms.

DOI: 10.4064/aa170-4-4

We prove the following theorems in Sections 3–7. In Theorems 1.1–1.9, $\sqrt{q}$ denotes any solution of the congruence $w^2 \equiv q \pmod{p}$.

THEOREM 1.1. ($d=-3$) *Let $q = A^2+A+1$ ($A \in \mathbb{Z}$) be a prime. Replacing A by $-A-1$ if necessary we may suppose that $A \equiv 0 \pmod 2$. Let p be an odd prime such that*

$$\left(\frac{-3}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

Then there is a unique solution $(x,y) \in \mathbb{Z}^2$ to $p = x^2+xy+y^2$ satisfying

$$x \equiv 1 \pmod 4, \quad y \equiv 3(p-1) \pmod 8, \quad (1-(-1)^{(p-1)/2})x+y > 0. \tag{1.1}$$

Further $x - Ay \not\equiv 0 \pmod q$, the Legendre symbol $\left(\frac{-2A-1-2\sqrt{q}}{p}\right)$ is well-defined and nonzero, and

$$\left(\frac{-2A-1-2\sqrt{q}}{p}\right) = \left(\frac{x-Ay}{q}\right).$$

We remark that $A \to -A-1$ leaves A^2+A+1 invariant and changes $2A+1 \to -(2A+1)$ so that

$$\begin{aligned}\left(\frac{-2A-1-2\sqrt{q}}{p}\right) \to \left(\frac{(2A+1)-2\sqrt{q}}{p}\right) &= \left(\frac{2A+1+2\sqrt{q}}{p}\right)\\ &= \left(\frac{-1}{p}\right)\left(\frac{-2A-1-2\sqrt{q}}{p}\right).\end{aligned}$$

The special case $A=-2$ of Theorem 1.1 is:

COROLLARY 1.1.1. ($A=-2$) *Let p be an odd prime with $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right) = 1$, equivalently $p \equiv 1 \pmod{12}$. Let $(x,y) \in \mathbb{Z}^2$ be the unique solution to $p = x^2+xy+y^2$ satisfying* (1.1). *Then*

$$\left(\frac{3+2\sqrt{3}}{p}\right) = \begin{cases} +1 & \text{if } x-y \equiv 1 \pmod 3,\\ -1 & \text{if } x-y \equiv 2 \pmod 3.\end{cases}$$

For a prime $p \equiv 1 \pmod{12}$ the classical criterion for -3 to be a quartic residue modulo p is

$$\left(\frac{-3}{p}\right)_4 = 1 \quad \text{if and only if} \quad b \equiv 0 \pmod 3,$$

where $p = a^2+b^2$, a odd, b even (see for example [1, Theorem 7.2.1, p. 216]). Corollary 1.1.1 enables us to give a new criterion for -3 to be a quartic residue modulo a prime $p \equiv 1 \pmod{12}$. As $2(2+\sqrt{3}) = (1+\sqrt{3})^2$ we have

$$\left(\frac{3+2\sqrt{3}}{p}\right) = \left(\frac{\sqrt{3}}{p}\right)\left(\frac{2+\sqrt{3}}{p}\right) = \left(\frac{3}{p}\right)_4\left(\frac{2}{p}\right)$$
$$= \left(\frac{3}{p}\right)_4\left(\frac{-1}{p}\right)_4 = \left(\frac{-3}{p}\right)_4,$$

so that

$$\left(\frac{-3}{p}\right)_4 = 1 \quad \text{if and only if} \quad x - y \equiv 1 \pmod 3.$$

We can use this result to give another proof of the criterion of Hudson and Williams [5, Theorem 2, p. 135] for 3 to be a fourth power modulo p, which was originally proved using cyclotomic numbers of order 6. We define integers c, d, u and v uniquely by

$$\begin{cases} p = c^2 + 3d^2, & c \equiv 1 \pmod 3,\ d > 0, \\ p = u^2 + 3v^2, & u \equiv 1 \pmod 4,\ v > 0. \end{cases}$$

Clearly, we have

$$c = \left(\frac{-3}{u}\right)u, \qquad u = \left(\frac{-4}{c}\right)c, \qquad d = v,$$

and

$$u = (-1)^{(p-1)/4}(x + y/2), \qquad v = y/2.$$

Then

$$\begin{aligned}\left(\frac{3}{p}\right)_4 = 1 \ &\Leftrightarrow \left(\frac{-1}{p}\right)_4 = \left(\frac{-3}{p}\right)_4 \\ &\Leftrightarrow p \equiv 1 \pmod 8,\ x - y \equiv 1 \pmod 3 \\ &\qquad \text{or} \\ &\qquad p \equiv 5 \pmod 8,\ x - y \equiv 2 \pmod 3 \\ &\Leftrightarrow u \equiv 1 \pmod 3 \ \Leftrightarrow\ c = u \ \Leftrightarrow\ c \equiv 1 \pmod 4,\end{aligned}$$

which is the Hudson–Williams criterion.

Our second corollary to Theorem 1.1 evaluates the symbol $\left(\frac{-2A-1-2\sqrt{q}}{p}\right)$ when $q \equiv 1 \pmod 4$ in terms of a and b, where $p = a^2 + 3b^2$.

COROLLARY 1.1.2. *Let $q = A^2 + A + 1$ be a prime, where $A \equiv 0 \pmod 4$, so that $q \equiv 1 \pmod 4$. Let p be an odd prime such that $\left(\frac{-3}{p}\right) = \left(\frac{q}{p}\right) = 1$. Then there are integers a and b such that $p = a^2 + 3b^2$ and for any such pair (a, b) we have*

$$\left(\frac{-2A-1-2\sqrt{q}}{p}\right) = \left(\frac{a-(2A+1)b}{q}\right).$$

Thus for example with $A = 8$ we see that if p is an odd prime with $\left(\frac{-3}{p}\right) = \left(\frac{73}{p}\right) = 1$ then

$$\left(\frac{-17-2\sqrt{73}}{p}\right) = \left(\frac{a-17b}{73}\right)$$

for any integers a and b with $p = a^2 + 3b^2$.

THEOREM 1.2. ($d = -4$) *Let $q = A^2 + 1$ ($A \in \mathbb{N}$) be an odd prime so that $A \equiv 0 \pmod 2$ and $q \equiv 1 \pmod 4$. Let p be an odd prime such that*

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

Then there are unique integers x and y such that

$$p = x^2 + y^2, \qquad x \equiv 1 \pmod 4, \qquad y \equiv \tfrac{1}{2}(p-1) \pmod 4, \quad y > 0. \tag{1.2}$$

Further $x - Ay \not\equiv 0 \pmod q$, the Legendre symbol $\left(\frac{A+\sqrt{q}}{p}\right)$ is well-defined and nonzero, and

$$\left(\frac{A+\sqrt{q}}{p}\right) = \left(\frac{x-Ay}{q}\right).$$

Theorem 1.2 is a simple consequence of the rational reciprocity laws of Burde [3] and Scholz [10]. As $p = x^2 + y^2$ (x odd) and $q = 1^2 + A^2$ (A even), Burde's law [9, p. 167] gives

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{x-Ay}{q}\right).$$

As $A+\sqrt{q}$ is the fundamental integral unit of $\mathbb{Q}(\sqrt{q})$, Scholz's law [9, p. 167] gives

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{A+\sqrt{q}}{p}\right).$$

Equating these two expressions, we obtain Theorem 1.2.

The special case $A = 2$ of Theorem 1.2 is:

COROLLARY 1.2.1. ($A = 2$) *Let p be an odd prime such that $\left(\frac{-4}{p}\right) = \left(\frac{5}{p}\right) = 1$, equivalently $p \equiv 1, 9 \pmod{20}$. Let $(x, y) \in \mathbb{Z}^2$ be the unique solution to $p = x^2 + y^2$ satisfying* (1.2). *Then*

$$\left(\frac{2+\sqrt{5}}{p}\right) = \left(\frac{x-2y}{5}\right).$$

Corollary 1.2.1 is a theorem of E. Lehmer [8]. The fundamental unit of the real quadratic field $\mathbb{Q}(\sqrt{5})$ is $\epsilon_5 = (1+\sqrt{5})/2$. We note that $\epsilon_5^3 = 2+\sqrt{5}$

so that $\left(\frac{2+\sqrt{5}}{p}\right) = \left(\frac{\epsilon_5}{p}\right)$. Also

$$\begin{cases} p \equiv 1 \pmod 5 \ \Leftrightarrow \ (x,y) \equiv (0,\pm 1) \text{ or } (\pm 1, 0) \pmod 5, \\ p \equiv 4 \pmod 5 \ \Leftrightarrow \ (x,y) \equiv (0,\pm 2) \text{ or } (\pm 2, 0) \pmod 5. \end{cases}$$

Hence, we have

$$\begin{aligned} &p \equiv 1 \pmod 5,\ y \equiv 0 \pmod 5 \quad \text{or} \quad p \equiv 4 \pmod 5,\ x \equiv 0 \pmod 5 \\ &\quad \Rightarrow x \equiv \pm 1 \pmod 5,\ y \equiv 0 \pmod 5 \quad \text{or} \quad x \equiv 0 \pmod 5,\ y \equiv \pm 2 \pmod 5 \\ &\quad \Rightarrow x - 2y \equiv \pm 1 \pmod 5 \ \Rightarrow \ \left(\frac{x-2y}{5}\right) = 1 \ \Rightarrow \ \left(\frac{\epsilon_5}{p}\right) = 1, \end{aligned}$$

and similarly

$$\begin{aligned} &p \equiv 1 \pmod 5,\ x \equiv 0 \pmod 5 \quad \text{or} \quad p \equiv 4 \pmod 5,\ y \equiv 0 \pmod 5 \\ &\qquad \Rightarrow \ \left(\frac{\epsilon_5}{p}\right) = -1. \end{aligned}$$

These two assertions comprise Lehmer's theorem.

Since $p_{-7}(A,1) = A^2 + A + 2$ is always even, it cannot represent an odd prime. Thus in Theorem 1.3 we use $p_{-28}(A,1) = A^2+7$ in place of $p_{-7}(A,1)$.

THEOREM 1.3. ($d = -7$) *Let* $q = A^2 + 7$ ($A \in \mathbb{N} \cup \{0\}$) *be a prime* (*so that* $A \equiv 0 \pmod 2$ *and* $q \equiv 3 \pmod 4$)*. Let* p *be an odd prime such that*

$$\left(\frac{-7}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

If $p \equiv 1 \pmod 4$ *there is a unique solution* $(x,y) \in \mathbb{Z}^2$ *to* $p = x^2 + 7y^2$ *satisfying*

$$x \equiv 1 \pmod 4, \qquad y \equiv \tfrac{1}{2}(p-1) \pmod 4, \qquad y > 0. \tag{1.3}$$

If $p \equiv 3 \pmod 4$ *there is a unique solution* $(x,y) \in \mathbb{Z}^2$ *to* $p = x^2 + 7y^2$ *satisfying*

$$x \equiv \tfrac{1}{2}(p-7) \pmod 4, \qquad x > 0, \qquad y \equiv 1 \pmod 4. \tag{1.4}$$

Further $x - Ay \not\equiv 0 \pmod q$, *the Legendre symbol* $\left(\frac{A+\sqrt{q}}{p}\right)$ *is well-defined and nonzero, and*

$$\left(\frac{A+\sqrt{q}}{p}\right) = (-1)^{(p-1)(q-3)/8}\left(\frac{x-Ay}{q}\right).$$

The special case $A = 0$ gives a criterion for 7 to be a quartic residue modulo p in terms of the residue of $x \pmod 7$ where $p = x^2+7y^2$. Criteria for the quartic reciprocity of 7 modulo a prime p were first given by Bickmore [2]. These were in terms of the representation $p = a^2 + b^2$ (see [1, pp. 230–231]). Another criterion for 7 to be a fourth power modulo a prime $p \equiv 1 \pmod{28}$ was given by Hudson and Williams [6].

The special case $A = 2$ is:

Corollary 1.3.1. ($A = 2$) *Let p be an odd prime such that $\left(\frac{-7}{p}\right) = \left(\frac{11}{p}\right) = 1$. Let $(x, y) \in \mathbb{Z}^2$ be the unique solution to $p = x^2 + 7y^2$ specified in* (1.3) *if $p \equiv 1 \pmod 4$ and in* (1.4) *if $p \equiv 3 \pmod 4$. Then*

$$\left(\frac{2+\sqrt{11}}{p}\right) = \begin{cases} +1 & \text{if } x - 2y \equiv 1, 3, 4, 5, 9 \pmod{11}, \\ -1 & \text{if } x - 2y \equiv 2, 6, 7, 8, 10 \pmod{11}. \end{cases}$$

Theorem 1.4. ($d = -8$) *Let $q = A^2 + 2$ ($A \in \mathbb{N}$) be an odd prime (so that $A \equiv 1 \pmod 2$ and $q \equiv 3 \pmod 8$). Replace A by $-A$ if necessary so that $A \equiv 1 \pmod 4$. Let p be an odd prime such that*

$$\left(\frac{-8}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

Then there is a unique solution $(x, y) \in \mathbb{Z}^2$ to $p = x^2 + 2y^2$ satisfying

$$(1.5) \qquad x \equiv 1 \pmod 4, \qquad y \equiv \begin{cases} 0 \pmod 2,\ y > 0, & \text{if } p \equiv 1 \pmod 8, \\ 3 \pmod 4 & \text{if } p \equiv 3 \pmod 8. \end{cases}$$

Further $x - Ay \not\equiv 0 \pmod q$, the Legendre symbol $\left(\frac{A+\sqrt{q}}{p}\right)$ is well-defined and nonzero, and

$$\left(\frac{A+\sqrt{q}}{p}\right) = (-1)^{(p+1)y/4}\left(\frac{x - Ay}{q}\right).$$

The special case $A = 1$ is:

Corollary 1.4.1. ($A = 1$) *Let p be an odd prime such that $\left(\frac{-8}{p}\right) = \left(\frac{3}{p}\right) = 1$, equivalently $p \equiv 1, 11 \pmod{24}$. Let $(x, y) \in \mathbb{Z}^2$ be the unique solution to $p = x^2 + 2y^2$ satisfying* (1.5). *If $p \equiv 1 \pmod{24}$ then*

$$\left(\frac{1+\sqrt{3}}{p}\right) = \begin{cases} +1 & \text{if } x - y \equiv 1, 11 \pmod{12}, \\ -1 & \text{if } x - y \equiv 5, 7 \pmod{12}, \end{cases}$$

and if $p \equiv 11 \pmod{24}$ then

$$\left(\frac{1+\sqrt{3}}{p}\right) = \begin{cases} +1 & \text{if } y \equiv 1 \pmod 3, \\ -1 & \text{if } y \equiv 2 \pmod 3. \end{cases}$$

Theorem 1.5. ($d = -11$) *Let $q = A^2 + A + 3$ ($A \in \mathbb{Z}$) be a prime. Replace A by $-A - 1$ if necessary so that $A \equiv 0 \pmod 2$. Let p be an odd prime such that*

$$\left(\frac{-11}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

Then there is a unique solution $(x, y) \in \mathbb{Z}^2$ of $p = x^2 + xy + 3y^2$ satisfying

$$(1.6) \qquad x \equiv 1 \pmod 4, \qquad y \equiv 1 - p \pmod 8, \qquad (1 - (-1)^{(p-1)/2})x + y > 0,$$

or

$$x \equiv 3 - p \pmod 8, \qquad y \equiv 1 \pmod 4. \tag{1.7}$$

Further $x - Ay \not\equiv 0 \pmod q$, *the Legendre symbol* $\left(\frac{2A+1+2\sqrt{q}}{p}\right)$ *is well-defined and nonzero, and*

$$\left(\frac{2A+1+2\sqrt{q}}{p}\right) = \begin{cases} (-1)^{(p-1)/2}\left(\frac{x-Ay}{q}\right) & \text{if (1.6) holds,} \\ (-1)^{(p+1)(q+1)/4-1}\left(\frac{x-Ay}{q}\right) & \text{if (1.7) holds.} \end{cases}$$

The next corollary is the special case $A = -2$.

Corollary 1.5.1. $(A = -2)$ *Let* p *be an odd prime such that* $\left(\frac{-11}{p}\right) = \left(\frac{5}{p}\right) = 1$. *Let* $(x, y) \in \mathbb{Z}^2$ *be the unique solution of* $p = x^2 + xy + 3y^2$ *given by* (1.6) *or* (1.7). *Then*

$$\left(\frac{3+2\sqrt{5}}{p}\right) = \left(\frac{x+2y}{5}\right) = \begin{cases} +1 & \text{if } x + 2y \equiv \pm 1 \pmod 5, \\ -1 & \text{if } x + 2y \equiv \pm 2 \pmod 5. \end{cases}$$

If we impose the requirement that $q \equiv 1 \pmod 4$ then $(-1)^{(p+1)(q+1)/4-1} = (-1)^{(p-1)/2}$ and Theorem 1.5 gives the following result.

Corollary 1.5.2. *Let* $q = A^2 + A + 3$ *be a prime where* $A \equiv 2 \pmod 4$ *so that* $q \equiv 1 \pmod 4$. *Let* p *be an odd prime such that* $\left(\frac{-11}{p}\right) = \left(\frac{q}{p}\right) = 1$. *Then there are integers* a *and* b *such that* $4p = a^2 + 11b^2$ *and for any such pair* (a, b) *we have*

$$\left(\frac{-2A-1+2\sqrt{q}}{p}\right) = \left(\frac{(a-(2A+1)b)/2}{q}\right).$$

In particular with $A = -2$ we have

$$\left(\frac{3+2\sqrt{5}}{p}\right) = -\left(\frac{a-2b}{5}\right)$$

for any integers a and b with $4p = a^2 + 11b^2$.

Theorem 1.6. $(d = -19)$ *Let* $q = A^2 + A + 5$ *be a prime* $(A \in \mathbb{Z})$. *Replace* A *by* $-A - 1$ *if necessary so that* $A \equiv 0 \pmod 2$. *Let* p *be an odd prime such that*

$$\left(\frac{-19}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

Then there is a unique solution $(x, y) \in \mathbb{Z}^2$ *of* $p = x^2 + xy + 5y^2$ *satisfying*

$$x \equiv 1 \pmod 4, \qquad y \equiv 1 - p \pmod 8, \qquad (1 - (-1)^{(p-1)/2})x + y > 0, \tag{1.8}$$

or

$$x \equiv 5 - p \pmod 8, \qquad y \equiv 1 \pmod 4. \tag{1.9}$$

Further $x - Ay \not\equiv 0 \pmod q$, *the Legendre symbol* $\left(\frac{2A+1+2\sqrt{q}}{p}\right)$ *is well-defined and nonzero, and*

$$\left(\frac{2A+1+2\sqrt{q}}{p}\right) = \begin{cases} (-1)^{(p-1)/2}\left(\frac{x-Ay}{q}\right) & \text{if (1.8) holds,} \\ (-1)^{(p+1)(q+1)/4-1}\left(\frac{x-Ay}{q}\right) & \text{if (1.9) holds.} \end{cases}$$

The next corollary results from imposing the condition $q \equiv 1 \pmod 4$ in Theorem 1.6.

COROLLARY 1.6.1. *Let* $q = A^2 + A + 5$ *be a prime where* $A \equiv 0 \pmod 4$ *so that* $q \equiv 1 \pmod 4$. *Let* p *be an odd prime such that* $\left(\frac{-19}{p}\right) = \left(\frac{q}{p}\right) = 1$. *Then there are integers* a *and* b *such that* $4p = a^2 + 19b^2$ *and for any such pair* (a, b) *we have*

$$\left(\frac{-2A-1+2\sqrt{q}}{p}\right) = \left(\frac{(a-(2A+1)b)/2}{q}\right).$$

In particular with $A = -4$ we have

$$\left(\frac{7+2\sqrt{17}}{p}\right) = \left(\frac{a+7b}{17}\right),$$

for any integers a and b with $4p = a^2 + 19b^2$.

THEOREM 1.7. ($d = -43$) *Let* $q = A^2 + A + 11$ ($A \in \mathbb{Z}$) *be a prime. Replace* A *by* $-A-1$ *if necessary so that* $A \equiv 0 \pmod 2$. *Let* p *be an odd prime such that*

$$\left(\frac{-43}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

Then there is a unique solution $(x, y) \in \mathbb{Z}^2$ *of* $p = x^2 + xy + 11y^2$ *satisfying*

$$(1.10) \qquad x \equiv 1 \pmod 4, \quad y \equiv 1 - p \pmod 8, \quad (1-(-1)^{(p-1)/2})x + y > 0,$$

or

$$(1.11) \qquad x \equiv 3 - p \pmod 8, \quad y \equiv 1 \pmod 4.$$

Further $x - Ay \not\equiv 0 \pmod q$, *the Legendre symbol* $\left(\frac{2A+1+2\sqrt{q}}{p}\right)$ *is well-defined and nonzero, and*

$$\left(\frac{2A+1+2\sqrt{q}}{p}\right) = \begin{cases} (-1)^{(p-1)/2}\left(\frac{x-Ay}{q}\right) & \text{if (1.10) holds,} \\ (-1)^{(p+1)(q+1)/4-1}\left(\frac{x-Ay}{q}\right) & \text{if (1.11) holds.} \end{cases}$$

COROLLARY 1.7.1. *Let* $q = A^2 + A + 11$ *be a prime where* $A \equiv 2 \pmod 4$ *so that* $q \equiv 1 \pmod 4$. *Let* p *be an odd prime such that* $\left(\frac{-43}{p}\right) = \left(\frac{q}{p}\right) = 1$.

Then there are integers a and b such that $4p = a^2 + 43b^2$ and for any such pair (a,b) we have

$$\left(\frac{-2A-1+2\sqrt{q}}{p}\right) = \left(\frac{(a-(2A+1)b)/2}{q}\right).$$

In particular with $A = -2$ we have

$$\left(\frac{3+2\sqrt{13}}{p}\right) = -\left(\frac{a+3b}{13}\right),$$

for any integers a and b with $4p = a^2 + 43b^2$.

THEOREM 1.8. $(d = -67)$ *Let $q = A^2 + A + 17$ $(A \in \mathbb{Z})$ be a prime. Replace A by $-A-1$ if necessary so that $A \equiv 0 \pmod 2$. Let p be an odd prime such that*

$$\left(\frac{-67}{p}\right) = \left(\frac{q}{p}\right) = 1.$$

Then there is a unique solution $(x,y) \in \mathbb{Z}^2$ of $p = x^2 + xy + 17y^2$ satisfying

$$x \equiv 1 \pmod 4, \quad y \equiv 1-p \pmod 8, \quad (1-(-1)^{(p-1)/2})x + y > 0, \tag{1.12}$$

or

$$x \equiv 1-p \pmod 8, \quad y \equiv 1 \pmod 4. \tag{1.13}$$

Further $x - Ay \not\equiv 0 \pmod q$, the Legendre symbol $\left(\frac{2A+1+2\sqrt{q}}{p}\right)$ is well-defined and nonzero, and

$$\left(\frac{2A+1+2\sqrt{q}}{p}\right) = \begin{cases} (-1)^{(p-1)/2}\left(\frac{x-Ay}{q}\right) & \text{if (1.12) holds,} \\ (-1)^{(p+1)(q+1)/4-1}\left(\frac{x-Ay}{q}\right) & \text{if (1.13) holds.} \end{cases}$$

For $q \equiv 1 \pmod 4$, Theorem 1.8 yields the following corollary.

COROLLARY 1.8.1. *Let $q = A^2 + A + 17$ be a prime where $A \equiv 0 \pmod 4$ so that $q \equiv 1 \pmod 4$. Let p be an odd prime such that $\left(\frac{-67}{p}\right) = \left(\frac{q}{p}\right) = 1$. Then there are integers a and b such that $4p = a^2 + 67b^2$ and for any such pair (a,b) we have*

$$\left(\frac{-2A-1+2\sqrt{q}}{p}\right) = \left(\frac{(a-(2A+1)b)/2}{q}\right).$$

In particular with $A = -4$ we have

$$\left(\frac{7+2\sqrt{29}}{p}\right) = -\left(\frac{a+7b}{29}\right)$$

for any integers a and b with $4p = a^2 + 67b^2$.

Theorem 1.9. ($d=-163$) *Let $q=A^2+A+41$ ($A\in\mathbb{Z}$) be a prime. Replace A by $-A-1$ if necessary so that $A\equiv 0 \pmod 2$. Let p be an odd prime such that*

$$\left(\frac{-163}{p}\right)=\left(\frac{q}{p}\right)=1.$$

Then there is a unique solution $(x,y)\in\mathbb{Z}^2$ of $p=x^2+xy+41y^2$ satisfying

$$(1.14)\qquad x\equiv 1 \pmod 4,\quad y\equiv 1-p \pmod 8,\quad (1-(-1)^{(p-1)/2})x+y>0,$$

or

$$(1.15)\qquad x\equiv 1-p \pmod 8,\quad y\equiv 1 \pmod 4.$$

Further $x-Ay\not\equiv 0 \pmod q$, the Legendre symbol $\left(\frac{2A+1+2\sqrt{q}}{p}\right)$ is well-defined and nonzero, and

$$\left(\frac{2A+1+2\sqrt{q}}{p}\right)=\begin{cases}(-1)^{(p-1)/2}\left(\frac{x-Ay}{q}\right) & \text{if (1.14) holds,}\\ (-1)^{(p+1)(q+1)/4-1}\left(\frac{x-Ay}{q}\right) & \text{if (1.15) holds.}\end{cases}$$

We impose the condition $q\equiv 1 \pmod 4$ in Theorem 1.9 to obtain our final corollary.

Corollary 1.9.1. *Let $q=A^2+A+41$ be a prime where $A\equiv 0 \pmod 4$ so that $q\equiv 1 \pmod 4$. Let p be an odd prime such that $\left(\frac{-163}{p}\right)=\left(\frac{q}{p}\right)=1$. Then there are integers a and b such that $4p=a^2+163b^2$ and for any such pair (a,b) we have*

$$\left(\frac{-2A-1+2\sqrt{q}}{p}\right)=\left(\frac{(a-(2A+1)b)/2}{q}\right).$$

In particular with $A=-4$ we have

$$\left(\frac{7+2\sqrt{53}}{p}\right)=-\left(\frac{a+7b}{53}\right)$$

for any integers a and b with $4p=a^2+163b^2$.

For an overview of evaluations of the Legendre symbol $\left(\frac{a+b\sqrt{q}}{p}\right)$, see [1] and [9].

2. Dörrie's law of quadratic reciprocity. Let K denote an imaginary quadratic field. Let O_K denote the ring of integers of K. We assume that O_K is a unique factorization domain. Stark [11], [12] has shown that this occurs only for the nine imaginary quadratic fields $K=\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$. We have $O_K=\mathbb{Z}+\mathbb{Z}\omega$, where

$$(2.1)\qquad \omega=\begin{cases}\sqrt{m} & \text{if } m=-1,-2,\\ \frac{1+\sqrt{m}}{2} & \text{if } m=-3,-7,-11,-19,-43,-67,-163.\end{cases}$$

Let π be a prime of O_K with $(\pi, 2) = 1$. For $\alpha \in O_K$ with $(\pi, \alpha) = 1$ we define the symbol $\left[\frac{\alpha}{\pi}\right]$ of quadratic reciprocity $\pmod{\pi}$ in O_K by

$$\left[\frac{\alpha}{\pi}\right] = \begin{cases} 1 & \text{if the congruence } \beta^2 \equiv \alpha \pmod{\pi} \\ & \text{is solvable for some } \beta \in O_K, \\ -1 & \text{otherwise.} \end{cases} \tag{2.2}$$

Now let $\pi = a + b\omega$ $(a, b \in \mathbb{Z})$ and $\kappa = c + d\omega$ $(c, d \in \mathbb{Z})$ be two primes in O_K with $\pi\bar{\pi} = p$ and $\kappa\bar{\kappa} = q$, where p and q are distinct odd rational primes.

Define nonnegative integers B, D and H, and odd integers b', d' and h', by

$$b = 2^B b', \qquad d = 2^D d', \qquad ad - bc = 2^H h'. \tag{2.3}$$

Dörrie's law of quadratic reciprocity for O_K [4] states that

$$\left[\frac{\pi}{\kappa}\right]\left[\frac{\kappa}{\pi}\right] = \pi_1 \kappa_1, \tag{2.4}$$

where

$$\pi_1 = (-1)^{(B+H)\frac{p^2-1}{8} + (\frac{b'-1}{2} + \frac{-h'-1}{2})\frac{p-1}{2}}, \tag{2.5}$$

$$\kappa_1 = (-1)^{(D+H)\frac{q^2-1}{8} + (\frac{d'-1}{2} + \frac{h'-1}{2})\frac{q-1}{2}}. \tag{2.6}$$

Since $(p^2-1)/8$, $(p-1)/2$, $(q^2-1)/8$ and $(q-1)/2$ are specified modulo 2, if p and q are known modulo 8, we can simplify the expression for $\pi_1\kappa_1$ given by multiplying (2.5) and (2.6) together (see Table 1).

Table 1. Values of $\pi_1\kappa_1$

p (mod 8)	q (mod 8)	$\pi_1\kappa_1$	p (mod 8)	q (mod 8)	$\pi_1\kappa_1$
1	1	1	5	1	$(-1)^{B+H}$
1	3	$(-1)^{D+H+\frac{d'-1}{2}+\frac{h'-1}{2}}$	5	3	$(-1)^{B+D+\frac{d'-1}{2}+\frac{h'-1}{2}}$
1	5	$(-1)^{D+H}$	5	5	$(-1)^{B+D}$
1	7	$(-1)^{\frac{d'-1}{2}+\frac{h'-1}{2}}$	5	7	$(-1)^{B+H+\frac{d'-1}{2}+\frac{h'-1}{2}}$
3	1	$(-1)^{B+H+\frac{b'-1}{2}+\frac{h'+1}{2}}$	7	1	$(-1)^{\frac{b'-1}{2}+\frac{h'+1}{2}}$
3	3	$(-1)^{B+D+\frac{b'-1}{2}+\frac{d'+1}{2}}$	7	3	$(-1)^{D+H+\frac{b'-1}{2}+\frac{d'+1}{2}}$
3	5	$(-1)^{B+D+\frac{b'-1}{2}+\frac{h'+1}{2}}$	7	5	$(-1)^{D+H+\frac{b'-1}{2}+\frac{h'+1}{2}}$
3	7	$(-1)^{B+H+\frac{b'-1}{2}+\frac{d'+1}{2}}$	7	7	$(-1)^{\frac{b'-1}{2}+\frac{d'+1}{2}}$

3. Proof of Theorem 1.1. As $p \equiv 1 \pmod 3$, there are integers x and y such that $p = x^2 + xy + y^2$. By Dirichlet's theorem [7] there are 12 such pairs (x,y). If (x,y) is one of these solutions, all of them are

$$(3.1)\qquad \begin{cases} (x,y),\ (x+y,-x),\ (y,-x-y), \\ (-x,-y),\ (-x-y,x),\ (-y,x+y), \\ (y,x),\ (x+y,-y),\ (x,-x-y), \\ (-y,-x),\ (-x-y,y),\ (-x,x+y). \end{cases}$$

As p is odd, at least one of x and y is odd. Replacing (x,y) by (y,x) if necessary we may take x to be odd. Replacing (x,y) by $(x,-x-y)$ if necessary we may suppose that y is even. Replacing (x,y) by $(-x,-y)$ if necessary we may suppose that $x \equiv 1 \pmod 4$. If $p \equiv 1 \pmod 4$ then $y \equiv 0 \pmod 4$ so replacing (x,y) by $(x+y,-y)$ if necessary we may suppose that $y > 0$. If $p \equiv 3 \pmod 4$ then $y \equiv 2 \pmod 4$ so replacing (x,y) by $(-x-y,y)$ if necessary we may suppose that $2x+y>0$. Thus $p = x^2+xy+y^2$ has a solution $(x,y) \in \mathbb{Z}^2$ satisfying

$$x \equiv 1 \ (\mathrm{mod}\ 4), \qquad y \equiv p-1 \ (\mathrm{mod}\ 4), \qquad \left(1-\left(\frac{-1}{p}\right)\right)x+y>0.$$

Reducing $p = x^2+xy+y^2$ modulo 8, we obtain $p \equiv 1+3y \pmod 8$, so that $y \equiv 3(p-1) \pmod 8$. It is easily seen from (3.1) that the solution (x,y) determined in this manner is unique. This proves (1.1).

Let (x,y) be the unique solution of $p = x^2+xy+y^2$ satisfying (1.1). Suppose $x - Ay \equiv 0 \pmod q$. Then $p = x^2+xy+y^2 \equiv (A^2+A+1)y^2 = qy^2 \equiv 0 \pmod q$, so, as p and q are both primes, we have $p = q$. This contradicts $\left(\frac{q}{p}\right) = 1$. Hence $x - Ay \not\equiv 0 \pmod q$.

As $\left(\frac{q}{p}\right) = 1$, the congruence $w^2 \equiv q \pmod p$ is solvable and has exactly two solutions modulo p, namely w and $-w$. Since we are writing $\sqrt{q}$ for one of these solutions, the other solution is $-\sqrt{q}$. As

$$\left(\frac{2A+1+2\sqrt{q}}{p}\right)\left(\frac{2A+1-2\sqrt{q}}{p}\right) = \left(\frac{(2A+1)^2-4q}{p}\right) = \left(\frac{-3}{p}\right) = 1,$$

we see that $2A+1 \pm 2\sqrt{q} \not\equiv 0 \pmod p$ and

$$\left(\frac{2A+1+2\sqrt{q}}{p}\right) = \left(\frac{2A+1-2\sqrt{q}}{p}\right).$$

Hence $\left(\frac{2A+1+2\sqrt{q}}{p}\right)$ is well-defined and nonzero.

We now work in the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$. This ring is $O_{\mathbb{Q}(\sqrt{-3})} = \mathbb{Z}+\mathbb{Z}\omega$, where $\omega = \frac{1+\sqrt{-3}}{2}$. It is a unique factorization domain. Let $\pi = x+y\omega \in \mathbb{Z}+\mathbb{Z}\omega$ and $\kappa = A+\omega \in \mathbb{Z}+\mathbb{Z}\omega$. Then $N(\pi) = N(x+y\omega) = x^2+xy+y^2 = p$ and $N(\kappa) = N(A+\omega) = A^2+A+1 = q$. By Dörrie's law of quadratic reciprocity in $\mathbb{Z}+\mathbb{Z}\omega$, we have

$$\left[\frac{\pi}{\kappa}\right]\left[\frac{\kappa}{\pi}\right]=\pi_1\kappa_1,$$

where $\pi_1\kappa_1$ is given in Table 1. Here in the notation of (2.3) we have

$$a=x,\qquad b=y,\qquad c=A,\qquad d=1,\qquad ad-bc=x-Ay,$$

so

$$2^B \parallel y,\quad b'=y/2^B,\quad D=0,\quad d'=1,\quad H=0,\quad h'=x-Ay\equiv 1 \pmod 4.$$

As $y\equiv 3(p-1) \pmod 8$, we have

$$\begin{cases} B\ge 3 & \text{if } p\equiv 1 \pmod 8,\\ B=2 & \text{if } p\equiv 5 \pmod 8,\\ B=1,\ b'\equiv 1 \pmod 4 & \text{if } p\equiv 7 \pmod 8.\end{cases}$$

Then from Table 1 we deduce $\pi_1\kappa_1=(-1)^{(p-1)/2}$ so that

$$\left[\frac{\pi}{\kappa}\right]\left[\frac{\kappa}{\pi}\right]=\left(\frac{-1}{p}\right).$$

As $\left(\frac{-3}{p}\right)=1$, there is an integer v such that $v^2\equiv -3 \pmod p$. Now

$$2(2A+1+v)(2A+1+2w)\equiv(2A+1+v+2w)^2 \pmod p$$

so

$$\left(\frac{2}{p}\right)\left(\frac{2A+1+v}{p}\right)\left(\frac{2A+1+2w}{p}\right)=1.$$

Hence

$$\begin{aligned}\left(\frac{2A+1+2\sqrt{q}}{p}\right)&=\left(\frac{2A+1+2w}{p}\right)=\left(\frac{2}{p}\right)\left(\frac{2A+1+v}{p}\right)\\&=\left(\frac{A+\frac{1+v}{2}}{p}\right)=\left[\frac{A+\omega}{x+y\omega}\right]=\left(\frac{-1}{p}\right)\left[\frac{x+y\omega}{A+\omega}\right]\\&=\left(\frac{-1}{p}\right)\left[\frac{x-Ay}{A+\omega}\right]=\left(\frac{-1}{p}\right)\left(\frac{x-Ay}{q}\right),\end{aligned}$$

which gives the asserted formula. Theorem 1.1 is proved.

Proof of Corollary 1.1.2. Let (x,y) be the unique solution to $p=x^2+xy+y^2$ satisfying (1.1). As $y\equiv 3(p-1) \pmod 8$, we have $y\equiv 0 \pmod 2$. Define integers a and b by

$$a=x+y/2,\qquad b=y/2$$

so that

$$p=a^2+3b^2. \tag{3.2}$$

Now $x - Ay = a - b - 2Ab = a - (2A+1)b$ so that by Theorem 1.1 we have

$$\left(\frac{-2A-1-2\sqrt{q}}{p}\right) = \left(\frac{a-(2A+1)b}{q}\right).$$

As (a,b), $(a,-b)$, $(-a,b)$, $(-a,-b)$ are all the solutions of (3.2), and $\left(\frac{-1}{q}\right) = \left(\frac{p}{q}\right) = 1$, we have

$$\begin{aligned}\left(\frac{a-(2A+1)b}{q}\right) &= \left(\frac{a+(2A+1)b}{q}\right) = \left(\frac{-a-(2A+1)b}{q}\right)\\ &= \left(\frac{-a+(2A+1)b}{q}\right)\end{aligned}$$

and the corollary follows. ∎

4. Proof of Theorem 1.2. As $p \equiv 1 \pmod 4$, there are integers x and y such that $p = x^2 + y^2$. By Dirichlet's theorem there are eight solutions $(x,y) \in \mathbb{Z}^2$ of $p = x^2 + y^2$. Let (x,y) be one of these solutions. Then all of them are

$$\text{(4.1)} \qquad \begin{cases} (x,y),\ (-x,y),\ (x,-y),\ (-x,-y),\\ (y,x),\ (-y,x),\ (y,-x),\ (-y,-x).\end{cases}$$

As p is odd, exactly one of x and y is odd. Replacing (x,y) by (y,x) if necessary we may suppose that x is odd and y is even. Replacing (x,y) by $(-x,y)$ if necessary we may suppose that $x \equiv 1 \pmod 4$. Then replacing (x,y) by $(x,-y)$ if necessary we may suppose that $y > 0$, so that the solution satisfies (1.2). Appealing to (4.1) we easily see that this solution is unique. Taking $p = x^2 + y^2$ modulo 8, as $x \equiv 1 \pmod 4$ and $y \equiv 0 \pmod 2$, we obtain $y \equiv \frac{1}{2}(p-1) \pmod 4$.

Let $(x,y) \in \mathbb{Z}^2$ be the unique solution to $p = x^2 + y^2$ satisfying (1.2). Suppose $x - Ay \equiv 0 \pmod q$. Then $p = x^2 + y^2 \equiv (A^2+1)y^2 = qy^2 \equiv 0 \pmod q$, so, as p and q are both primes, we have $p = q$, contradicting $\left(\frac{q}{p}\right) = 1$. Hence $x - Ay \not\equiv 0 \pmod q$.

As $\left(\frac{q}{p}\right) = 1$, the congruence $w^2 \equiv q \pmod p$ is solvable and has precisely two solutions modulo p, namely w and $-w$. Since we are writing $\sqrt{q}$ for one of these solutions, the other is $-\sqrt{q}$. Now

$$\left(\frac{A+\sqrt{q}}{p}\right)\left(\frac{A-\sqrt{q}}{p}\right) = \left(\frac{A^2-q}{p}\right) = \left(\frac{-1}{p}\right) = 1,$$

so that $A \pm \sqrt{q} \not\equiv 0 \pmod p$ and

$$\left(\frac{A+\sqrt{q}}{p}\right) = \left(\frac{A-\sqrt{q}}{p}\right).$$

Hence $\left(\frac{A+\sqrt{q}}{p}\right)$ is well-defined and nonzero.

We now make use of the arithmetic of the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-1})$. This ring is $O_{\mathbb{Q}(\sqrt{-1})} = \mathbb{Z} + \mathbb{Z}i$. It is a unique factorization domain. Let $\pi = x + yi \in \mathbb{Z} + \mathbb{Z}i$ and $\kappa = A + i \in \mathbb{Z} + \mathbb{Z}i$. Then

$$N(\pi) = x^2 + y^2 = p, \qquad N(\pi) = A^2 + 1 = q.$$

By Dörrie's law of quadratic reciprocity in $\mathbb{Z} + \mathbb{Z}i$, we have

$$\left[\frac{\pi}{\kappa}\right]\left[\frac{\kappa}{\pi}\right] = \pi_1\kappa_1,$$

where $\pi_1\kappa_1$ is given in Table 1.

Here in the notation of (2.3) we have

$$a = x, \qquad b = y, \qquad c = A, \qquad d = 1, \qquad ad - bc = x - Ay,$$

so

$$2^B \parallel y, \quad b' = y/2^B, \quad D = 0, \quad d' = 1, \quad H = 0, \quad h' = x - Ay \equiv 1 \pmod 4.$$

As $y \equiv \frac{1}{2}(p-1) \pmod 4$, we have

$$\begin{cases} B \geq 2 & \text{if } p \equiv 1 \pmod 8, \\ B = 1 & \text{if } p \equiv 5 \pmod 8). \end{cases}$$

Then from Table 1 we deduce

$$\pi_1\kappa_1 = (-1)^{(p-1)/4}$$

so that

$$\left[\frac{\pi}{\kappa}\right]\left[\frac{\kappa}{\pi}\right] = \left(\frac{2}{p}\right). \tag{4.2}$$

As $\left(\frac{-1}{p}\right) = 1$, there is an integer v such that $v^2 \equiv -1 \pmod p$. Recall that $w^2 \equiv q \pmod p$. Now

$$2(A+v)(A+w) \equiv (A+v+w)^2 \pmod p,$$

so

$$\left(\frac{2}{p}\right)\left(\frac{A+v}{p}\right)\left(\frac{A+w}{p}\right) = 1.$$

Hence, appealing to (4.2), we obtain

$$\left(\frac{A+\sqrt{q}}{p}\right) = \left(\frac{A+w}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{A+v}{p}\right) = \left(\frac{2}{p}\right)\left[\frac{A+i}{x+yi}\right] = \left(\frac{2}{p}\right)\left[\frac{\kappa}{\pi}\right]$$
$$= \left[\frac{\pi}{\kappa}\right] = \left[\frac{x+yi}{A+i}\right] = \left[\frac{x-Ay}{A+i}\right] = \left(\frac{x-Ay}{q}\right),$$

as asserted.

5. Proof of Theorem 1.3. As $\left(\frac{-7}{p}\right) = 1$, there are integers u and v such that $p = u^2 + uv + 2v^2$. Set $r = 2u + v \in \mathbb{Z}$ and $s = v \in \mathbb{Z}$ so that $4p = r^2 + 7s^2$. Hence, as p is odd, we have $r^2 + 7s^2 \equiv 4 \pmod 8$, so $r \equiv s \equiv 0 \pmod 2$. Set $r = 2x$ and $s = 2y$, where $x, y \in \mathbb{Z}$. Then $p = x^2 + 7y^2$. It is easily checked that the only solutions to $p = x^2 + 7y^2$ are

$$(x, y),\ (x, -y),\ (-x, y),\ (-x, -y). \tag{5.1}$$

If $p \equiv 1 \pmod 4$ then $x \equiv 1 \pmod 2$ and $y \equiv 0 \pmod 2$ and a unique solution is given by (1.3). If $p \equiv 3 \pmod 4$ then $x \equiv 0 \pmod 2$ and $y \equiv 1 \pmod 2$ and a unique solution is given by (1.4). Taking $p = x^2 + 7y^2$ modulo 8, we obtain

$$\begin{cases} y \equiv \frac{1}{2}(p-1) \pmod 4 & \text{if } p \equiv 1 \pmod 4, \\ x \equiv \frac{1}{2}(p-7) \pmod 4 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Let (x, y) be the unique solution of $p = x^2 + 7y^2$ given by (1.3) if $p \equiv 1 \pmod 4$ and by (1.4) if $p \equiv 3 \pmod 4$. It is easy to check that $x - Ay \not\equiv 0 \pmod q$ and $\left(\frac{A+\sqrt{q}}{p}\right) = \left(\frac{A-\sqrt{q}}{p}\right) \neq 0$.

We now make use of the arithmetic of the ring of integers of the imaginary quadratic field $\mathbb{Q}(\sqrt{-7})$. This ring is $O_{\mathbb{Q}(\sqrt{-7})} = \mathbb{Z} + \mathbb{Z}\omega$, where $\omega = (1 + \sqrt{-7})/2$. It is a unique factorization domain. Let $\pi = x + y\sqrt{-7} = x - y + 2y\omega \in \mathbb{Z} + \mathbb{Z}\omega$ and $\kappa = A + \sqrt{-7} = A - 1 + 2\omega \in \mathbb{Z} + \mathbb{Z}\omega$. We have $N(\pi) = x^2 + 7y^2 = p$ and $N(\kappa) = A^2 + 7 = q$. In the notation of (2.3) we have

$$\begin{aligned} &a = x - y, \quad b = 2y = 2^B b', \quad c = A - 1, \quad d = 2 = 2^D d', \\ &ad - bc = 2(x - Ay) = 2^H h', \end{aligned}$$

so that

$$2^{B-1} \parallel y, \quad b' = \frac{y}{2^{B-1}}, \quad D = d' = 1, \quad 2^{H-1} \parallel x - Ay, \quad h' = \frac{x - Ay}{2^{H-1}}.$$

Suppose first that $p \equiv 1 \pmod 4$. In this case $x \equiv 1 \pmod 4$ and $y \equiv 0 \pmod 2$, so $x - Ay \equiv 1 \pmod 4$ and thus

$$H = 1, \quad h' = x - Ay \equiv 1 \pmod 4.$$

From $y \equiv \frac{1}{2}(p-1) \pmod 4$ we deduce that

$$\begin{cases} B \geq 3 & \text{if } p \equiv 1 \pmod 8, \\ B = 2 & \text{if } p \equiv 5 \pmod 8. \end{cases}$$

Appealing to Table 1 for the cases $(p, q) \equiv (1, 3), (1, 7), (5, 3)$ and $(5, 7)$

(mod 8), we obtain

$$\pi_1\kappa_1 = (-1)^{(p-1)/4} \quad \text{if } p \equiv 1 \pmod 4. \tag{5.2}$$

Now suppose that $p \equiv 3 \pmod 4$. In this case $x \equiv 0 \pmod 2$ and $y \equiv 1 \pmod 4$, so

$$B = 1, \quad b' = y \equiv 1 \pmod 4.$$

Also $x - Ay \equiv 0 \pmod 2$ and thus $H \geq 2$. From $x \equiv \frac{1}{2}(p-7) \pmod 4$, we deduce that

$$\begin{cases} x \equiv 2 \pmod 4 & \text{if } p \equiv 3 \pmod 8, \\ x \equiv 0 \pmod 4 & \text{if } p \equiv 7 \pmod 8. \end{cases}$$

Taking $q = A^2 + 7$ modulo 8, we get

$$\begin{cases} A \equiv 2 \pmod 4 & \text{if } q \equiv 3 \pmod 8, \\ A \equiv 0 \pmod 4 & \text{if } q \equiv 7 \pmod 8. \end{cases}$$

Thus

$$\begin{cases} x - Ay \equiv 0 \pmod 4 & \text{if } p \equiv q \pmod 8, \\ x - Ay \equiv 2 \pmod 4 & \text{if } p \not\equiv q \pmod 8. \end{cases}$$

Hence

$$\begin{cases} H \geq 3 & \text{if } p \equiv q \pmod 8, \\ H = 2 & \text{if } p \not\equiv q \pmod 8. \end{cases}$$

Appealing to Table 1 for the cases $(p,q) = (3,3), (3,7), (7,3)$ and $(7,7)$ (mod 8), we obtain

$$\pi_1\kappa_1 = (-1)^{(p+q-2)/4} \quad \text{if } p \equiv 3 \pmod 4. \tag{5.3}$$

In view of (5.2) and (5.3) set

$$\epsilon := \begin{cases} (-1)^{(p-1)/4} & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{(p+q-2)/4} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

so that by Dörrie's law of quadratic reciprocity we have

$$\left[\frac{\pi}{\kappa}\right]\left[\frac{\kappa}{\pi}\right] = \epsilon. \tag{5.4}$$

An examination of cases yields

$$\left(\frac{2}{p}\right)\epsilon = (-1)^{(p-1)(q-3)/8}. \tag{5.5}$$

As $\left(\frac{-7}{p}\right) = \left(\frac{q}{p}\right) = 1$ there are integers v and w such that $v^2 \equiv -7 \pmod p$ and $w^2 \equiv q \pmod p$. As

$$2(A+v)(A+w) \equiv (A+v+w)^2 \pmod p,$$

we have

$$\left(\frac{2}{p}\right)\left(\frac{A+v}{p}\right)\left(\frac{A+w}{p}\right)=1.$$

Hence, appealing to (5.4) and (5.5), we deduce

$$\begin{aligned}
\left(\frac{A+\sqrt{q}}{p}\right) &= \left(\frac{A+w}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{A+v}{p}\right) \\
&= \left(\frac{2}{p}\right)\left[\frac{A+\sqrt{-7}}{x+y\sqrt{-7}}\right] = \left(\frac{2}{p}\right)\left[\frac{\kappa}{\pi}\right] = \left(\frac{2}{p}\right)\epsilon\left[\frac{\pi}{\kappa}\right] \\
&= (-1)^{(p-1)(q-3)/8}\left[\frac{x+y\sqrt{-7}}{A+\sqrt{-7}}\right] = (-1)^{(p-1)(q-3)/8}\left[\frac{x-Ay}{A+\sqrt{-7}}\right] \\
&= (-1)^{(p-1)(q-3)/8}\left(\frac{x-Ay}{q}\right),
\end{aligned}$$

as asserted.

6. Proof of Theorem 1.4. As $\left(\frac{-8}{p}\right)=1$, there are integers x and y such that $p=x^2+2y^2$. By Dirichlet's theorem there are four solutions $(x,y)\in\mathbb{Z}^2$ to $p=x^2+2y^2$. If one of these is (x,y), all four of them are

$$(x,y),\ (x,-y),\ (-x,y),\ (-x,-y).$$

Clearly $x\equiv 1 \pmod 2$ and $y\equiv \frac{1}{2}(p-1) \pmod 2$. The existence and uniqueness of the solution satisfying (1.5) now follows easily.

The rest of the proof goes as for Theorems 1.1–1.3. Here we use $\pi = x+y\sqrt{-2}\in\mathbb{Z}+\mathbb{Z}\sqrt{-2}$ and $\kappa = A+\sqrt{-2}\in\mathbb{Z}+\mathbb{Z}\sqrt{-2}$ so that $N(\pi)=p$ and $N(\kappa)=q$. Dörrie's law of quadratic reciprocity in $\mathbb{Z}+\mathbb{Z}\sqrt{-2}$ yields

$$\left[\frac{\pi}{\kappa}\right]\left[\frac{\kappa}{\pi}\right] = \pi_1\kappa_1 = \begin{cases} (-1)^{y/2} & \text{if } p\equiv 1 \pmod 8, \\ 1 & \text{if } p\equiv 3 \pmod 8, \end{cases}$$

and we continue as before.

7. Proofs of Theorems 1.5–1.9

Proof of Theorem 1.5. As $\left(\frac{-11}{p}\right)=1$, there are integers x and y such that $p=x^2+xy+3y^2$. By Dirichlet's theorem there are four solutions $(x,y)\in\mathbb{Z}^2$ to $p=x^2+xy+3y^2$. If one of these is (x,y), all four of them are

$$(x,y),\ (-x,-y),\ (-x-y,y),\ (x+y,-y).$$

Clearly x and y are not both even as p is odd. If x and y are both odd, we can replace (x,y) by $(x+y,-y)$ if necessary to obtain $x\equiv 0 \pmod 2$ and $y\equiv 1 \pmod 2$. Then replacing (x,y) by $(-x,-y)$ if necessary we get a solution with $x \equiv 0 \pmod 2$ and $y \equiv 1 \pmod 4$. Then, from $p = x^2 + xy + 3y^2$ modulo 8, we deduce that $x \equiv 3 - p \pmod 8$. If x is odd and y is even, we can replace (x, y) by $(-x, -y)$ if necessary to ensure that $x \equiv 1 \pmod 4$. Then, from $p = x^2 + xy + 3y^2$ modulo 8, we deduce that $y \equiv 1 - p \pmod 8$. If $p \equiv 1 \pmod 4$, so that $y \equiv 0 \pmod 4$, we replace (x, y) by $(x + y, -y)$ if necessary so that $y > 0$. If $p \equiv 3 \pmod 4$, so that $y \equiv 2 \pmod 4$, we replace (x, y) by $(-x - y, y)$ if necessary so that $2x + y > 0$. The uniqueness of the determined solution follows easily.

The rest of the proof proceeds as in the previous theorems. Here we use $\pi = x + y\omega \in \mathbb{Z} + \mathbb{Z}\omega$ and $\kappa = A + \omega \in \mathbb{Z} + \mathbb{Z}\omega$, where $\omega = (1 + \sqrt{-11})/2$, so that $N(\pi) = p$ and $N(\kappa) = q$. Dörrie's law of quadratic reciprocity in $\mathbb{Z} + \mathbb{Z}\omega$ yields

$$\left[\frac{\pi}{\kappa}\right]\left[\frac{\kappa}{\pi}\right] = \begin{cases} (-1)^{(p-1)/2} & \text{if (1.6) holds,} \\ (-1)^{(p+1)(q+1)/4-1} & \text{if (1.7) holds,} \end{cases}$$

and the remainder of the proof proceeds as in Theorem 1.1. ■

Proof of Corollary 1.5.2. As $\left(\frac{-11}{p}\right) = 1$, there are integers a and b such that $4p = a^2 + 11b^2$. Moreover the only such pairs are (a, b), $(a, -b)$, $(-a, b)$ and $(-a, -b)$. As $\left(\frac{q}{p}\right) = 1$ and $q \equiv 1 \pmod 4$, by the law of quadratic reciprocity we have $\left(\frac{p}{q}\right) = 1$. Then it is easy to check that

$$\left(\frac{a - (2A + 1)b}{q}\right) = \left(\frac{a + (2A + 1)b}{q}\right) = \left(\frac{-a + (2A + 1)b}{q}\right) = \left(\frac{-a - (2A + 1)b}{q}\right),$$

so $\left(\frac{a-(2A+1)b}{q}\right)$ is independent of the choice of (a, b). Choose $a = 2x + y$ and $b = y$. By Theorem 1.5 we have

$$\left(\frac{2A + 1 + 2\sqrt{q}}{p}\right) = (-1)^{(p-1)/2}\left(\frac{x - Ay}{q}\right),$$

so as $a - (2A + 1)b = 2(x - Ay)$ we deduce

$$\left(\frac{-2A - 1 + 2\sqrt{q}}{p}\right) = \left(\frac{(a - (2A + 1)b)/2}{q}\right),$$

as claimed. ■

Proofs of Theorems 1.6–1.9. The proofs are very similar to that of Theorem 1.5 and we omit them.

Acknowledgments. We thank the referee for his/her helpful suggestions.

References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1998.

[2] C. E. Bickmore, *On the numerical factors of $a^n - 1$*, Messenger Math. 25 (1895), 1–44.

[3] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. 235 (1969), 175–184.

[4] H. Dörrie, *Das quadratische Reciprocitätsgesetz im quadratischen Zahlkörper mit der Classenzahl 1*, Inaugural Dissertation, Georg-Augusts-Universität, Göttingen, 1898.

[5] R. H. Hudson and K. S. Williams, *Some new residuacity criteria*, Pacific J. Math. 91 (1980), 135–143.

[6] R. H. Hudson and K. S. Williams, *A new criterion for 7 to be a fourth power* (*mod p*), Israel J. Math. 38 (1981), 221–230.

[7] P. Kaplan and K. S. Williams, *On a formula of Dirichlet*, Far East J. Math. Sci. 5 (1997), 153–157.

[8] E. Lehmer, *On the quadratic character of the Fibonacci root*, Fibonacci Quart. 4 (1966), 135–138; Correction, ibid., 354.

[9] F. Lemmermeyer, *Reciprocity Laws. From Fuler to Eisenstein*, Springer, Berlin, 2000.

[10] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. 39 (1935), 95–111.

[11] H. M. Stark, *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. 14 (1967), 1–27.

[12] H. M. Stark, *On the "gap" in a theorem of Heegner*, J. Number Theory 1 (1969), 16–27.

Lerna Pehlivan
Department of Mathematics and Statistics
Dalhousie University
Halifax, Nova Scotia, Canada B3H 4R2
E-mail: lr608779@dal.ca

Kenneth S. Williams
Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario, Canada K1S 5B6
E-mail: kennethwilliams@cunet.carleton.ca

Received on 6.12.2014
and in revised form on 29.7.2015 (8022)