Замечание. Пусть $p > n$ — простое. Выбирая в теореме 3 $k = n$ и $q_\nu = p^\nu$ $(\nu = 1, 2, \ldots, n)$ для числа решений системы

$$\left.\begin{array}{l} x_1 + \ldots + x_n \equiv \lambda_1 \pmod{p} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_1^n + \ldots + x_n^n \equiv \lambda_n \pmod{p^n} \end{array}\right\}; \qquad (x_1, \ldots, x_n)_n \pmod{p^n}$$

получим оценки из работ [3] и [1]:

$$T_n = p^{n(n-1)/2} T_n(\lambda_1, \ldots, \lambda_n; p) \leqslant n!\, p^{n(n-1)/2}.$$

Аналогично этому, (ср. [2]) выбирая $k = n$ и

$$q_\nu = \begin{cases} p^\nu & \text{если} \quad 1 \leqslant \nu \leqslant r, \\ p^r & \text{если} \quad r \leqslant \nu \leqslant n, \end{cases}$$

при $1 \leqslant r \leqslant n$ для числа решений системы

$$\left.\begin{array}{l} x_1 + \ldots + x_n \equiv \lambda_1 \pmod{p} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_1^r + \ldots + x_n^r \equiv \lambda_r \pmod{p^r} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_1^n + \ldots + x_n^n \equiv \lambda_n \pmod{p^r} \end{array}\right\}; \qquad (x_1, \ldots, x_n)_n \pmod{p^r}$$

получим

$$T_n^{(r)} = p^{r(r-1)/2} T_n(\lambda_1, \ldots, \lambda_n; p) \leqslant n!\, p^{r(r-1)/2}.$$

Цитированная литература

[1] А. А. Карацуба, Н. М. Коробов, *О теореме о среднем*, ДАН СССР 149, 2 (1963), стр. 245–248.

[2] А. А. Карацуба, *О системах сравнений*, Изв. АН СССР, сер. матем., 29 (1965), стр. 959–968.

[3] Ю. В. Линник, *О суммах Weyl'я*, ДАН СССР 34, 7 (1942), стр. 201–203.

МАТЕМАТИЧЕСКИЙ ИНСТИТУТ ИМ В. А. СТЕКЛОВА АН СССР

Получено 8. 8. 1971 (205)

ACTA ARITHMETICA
XXI (1972)

On some special quartic reciprocity laws

by

EMMA LEHMER (Berkeley, Calif.)

In memory of Wacław Sierpiński

In a recent paper [6] we gave an elementary proof of a theorem due to Scholz [9], which can be stated as follows:

Let $p \equiv q \equiv 1 \pmod 4$ be two distinct primes which are quadratic residues of each other and let ε_p and ε_q be the fundamental units in the quadratic fields $Q(\sqrt{p})$ and $Q(\sqrt{q})$, then

$$\left(\frac{\varepsilon_p}{q}\right) = \left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4. \tag{1}$$

Traditionally, the quartic character of q with respect to p is expressed in terms of the quadratic partition $p = a^2 + 4b^2$. Thus for $q = 5$ we have

5 is a quartic residue of p if and only if 5 divides b.

In a recent paper of Muskat and Whiteman [7] it was shown, using cyclotomy of order 20, that for $p \equiv 1 \pmod{20}$ this can also be stated in terms of the partition $p = c^2 + 5d^2$ as follows:

5 is a quartic residue of $p \equiv 1 \pmod{20}$ if and only if d is even.

Using (1) this gives at once

$$\left(\frac{\varepsilon_5}{p}\right) = \left(\frac{(1+\sqrt{5})/2}{p}\right) = (-1)^d. \tag{2}$$

About the same time Brandler [2], using the theory of quartic fields, showed that if $p = c^2 + qd^2$, then

$$\left(\frac{\varepsilon_q}{p}\right) = (-1)^d \quad \text{for} \quad q = 5, 13 \tag{3}$$

and that for $q = 17$ we have $\left(\frac{\varepsilon_{17}}{p}\right) = \pm 1$, according as p or $2p$ is represented by $c^2 + 17d^2$.

It is the purpose of this paper to show that all these results are special cases of a more general theorem, which can be proved by the most elementary means, and to obtain corresponding theorems for forms of discriminant $-8q$ and for indefinite forms of discriminant q and $2q$. We also qive applications of these theorems to the solvability of the Pell equation $t^2-pqu^2=-1$ and to the divisibility of the class number of $h(\sqrt{-q})$ and $h(\sqrt{-2q})$ by 8.

It should be pointed out that these theorems having to do with two primes $p\equiv q\equiv 1 \pmod 4$ such that $\left(\frac{p}{q}\right)=1$ have known counterparts when one of the primes, say q is 2 and the other $p\equiv 1 \pmod 8$ so that $\left(\frac{2}{p}\right)=1$.

Barrucand and Cohn [1] proved that for $p=c^2+8d^2=e^2-32f^2$

$$\left(\frac{\varepsilon_2}{p}\right)=\left(\frac{1+\sqrt{2}}{p}\right)=(-1)^d=(-1)^{h/4}=\left(\frac{-1}{e}\right) \tag{4}$$

where $h=h(\sqrt{-p})$ is the class number of $Q(\sqrt{-p})$.

Similarly Hasse [5] proved that $h(\sqrt{-2p})\equiv 0 \pmod 8$ if and only if $\left(\frac{-2}{e}\right)=1$. This can be restated as

$$\left(\frac{2}{p}\right)_4=(-1)^{h/4}=\left(\frac{-2}{e}\right)=(-1)^{h(\sqrt{-2p})/4}. \tag{5}$$

It was proved by Epstein [4] that the Pell equation $t^2-Du^2=-1$ has no solutions for $D=2p$ if $p=c^2+8d^2$ and d is odd. Redei [8] gave another proof of this theorem and showed that the equation has no solution if $\left(\frac{\varepsilon_2}{p}\right)=-1$. Scholz [9] showed that for $D=pq$ with $p\equiv q\equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right)=1$ the equation has no solutions if $\left(\frac{\varepsilon_p}{q}\right)=-1$.

In the present paper we will establish the analogue of Epstein's theorem, namely that the Pell equation $t^2-pqu^2=-1$ has no solutions if $p=c^2+qd^2$ and d is odd when $p\equiv q\equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right)=1$.

We will assume throughout the paper that p and q are primes with $p\equiv q\equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right)=1$, that ε_n is the fundamental unit in the quadratic field $Q(\sqrt{n})$, that all the integers in the representation of p by binary quadratic forms are positive and prime to each other and that ν is odd.

THEOREM 1. *Let*

$$rp^{\nu}=c^2+qd^2. \tag{6}$$

Then if $r=s^2$ and r is odd

$$\left(\frac{\varepsilon_p}{q}\right)=\left(\frac{\varepsilon_q}{p}\right)=\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4=\begin{cases}\left(\frac{s}{q}\right) & \text{if}\quad q=8n+1,\\ (-1)^d\left(\frac{s}{q}\right) & \text{if}\quad q=8n+5,\end{cases}$$

while if $r=2$, or $r\equiv 1 \pmod 4$ is a prime, such that $\left(\frac{r}{q}\right)=1$, then

$$\left(\frac{\varepsilon_p}{q}\right)=\left(\frac{\varepsilon_q}{p}\right)=\left(\frac{p}{q}\right)_4\left(\frac{q}{p}\right)_4=\begin{cases}\left(\frac{\varepsilon_r}{q}\right) & \text{if}\quad q=8n+1,\\ (-1)^d\left(\frac{\varepsilon_r}{q}\right) & \text{if}\quad q=8n+5.\end{cases}$$

Proof. Taking (6) modulo q and p we get

$$\left(\frac{r}{q}\right)_4\left(\frac{p}{q}\right)_4=\left(\frac{c}{q}\right),\qquad \left(\frac{q}{p}\right)_4=\left(\frac{2cd}{p}\right),$$

since

$$\left(\frac{-1}{p}\right)_4=\left(\frac{2}{p}\right)\quad \text{if}\quad p\equiv 1 \pmod 4.$$

Hence we have by (1)

$$\left(\frac{\varepsilon_q}{p}\right)=\left(\frac{r}{q}\right)_4\left(\frac{c}{q}\right)\left(\frac{2cd}{p}\right). \tag{7}$$

Let γ be the largest odd factor of c and δ of d, then from (6)

$$\left(\frac{r}{\gamma}\right)\left(\frac{p}{\gamma}\right)=\left(\frac{q}{\gamma}\right),\qquad \left(\frac{r}{\delta}\right)\left(\frac{p}{\delta}\right)=1, \tag{8}$$

where the symbols are Jacobi symbols. We now consider two cases.

Case 1, d even. Hence cr is odd and $d/2$ is odd if and only if $rp\equiv 5 \pmod 8$. If $r=s^2$, then by (8) we have $\gamma=c$, $\delta=d/2$ if $p\equiv 5 \pmod 8$, hence

$$\left(\frac{c}{p}\right)=\left(\frac{c}{q}\right)\quad\text{and}\quad\left(\frac{d}{p}\right)=\left(\frac{2}{p}\right).$$

Hence by (7) we have

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{s}{q}\right) \quad \text{if} \quad r = s^2 \text{ and } p \equiv 5 \pmod 8.$$

If r is an odd prime we can take (6) modulo r and get

$$\left(\frac{c}{r}\right) = \left(\frac{q}{r}\right)_4 \left(\frac{2d}{r}\right) \tag{9}$$

while (8) becomes

$$\left(\frac{c}{r}\right)\left(\frac{c}{p}\right) = \left(\frac{c}{q}\right), \qquad \left(\frac{2d}{r}\right) = \left(\frac{2d}{p}\right).$$

Substituting this into (7) we obtain by (1) for r a prime

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{r}{q}\right)_4 \left(\frac{q}{r}\right)_4 = \left(\frac{\varepsilon_r}{q}\right).$$

Case 2, d odd. Then c is even if r is odd, and $c/2$ is odd if and only if $rp \not\equiv q \pmod 8$. Hence by (4) if $r = s^2$ we have

$$\left(\frac{2c}{p}\right)\left(\frac{2c}{q}\right) = 1, \qquad \left(\frac{d}{p}\right) = 1$$

and hence by (7)

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{2s}{q}\right) \quad \text{if} \quad r = s^2$$

while if r is an odd prime (8) gives

$$\left(\frac{2c}{r}\right)\left(\frac{2c}{p}\right) = \left(\frac{2c}{q}\right), \qquad \left(\frac{d}{r}\right) = \left(\frac{d}{p}\right)$$

which together with (9) reduces (7) to

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{2}{q}\right)\left(\frac{\varepsilon_r}{q}\right) \quad \text{if} \quad r \text{ is an odd prime.}$$

Now finally if $r = 2$, then c is odd and hence $q \equiv 1 \pmod 8$ and (8) becomes

$$\left(\frac{c}{p}\right)\left(\frac{c}{q}\right) = \left(\frac{2}{c}\right), \qquad \left(\frac{d}{p}\right) = \left(\frac{2}{d}\right)$$

which makes (7)

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{2}{q}\right)_4 \left(\frac{2}{c}\right)\left(\frac{2}{d}\right)\left(\frac{2}{p}\right).$$

One can easily ascertain by going through the cases modulo 16 that

$$\left(\frac{2}{c}\right)\left(\frac{2}{d}\right) = (-1)^{(q-1)/8}\left(\frac{2}{p}\right).$$

By a theorem of Barrucand and Cohn [1]

$$\left(\frac{2}{q}\right)_4 (-1)^{(q-1)/8} = \left(\frac{\varepsilon_2}{q}\right). \tag{10}$$

Hence

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{\varepsilon_2}{q}\right) \quad \text{if} \quad r = 2.$$

Combining all the cases, the theorem follows.

Corollary 1. *If*

$$p = c^2 + qd^2 \tag{11}$$

then

$$\left(\frac{\varepsilon_p}{q}\right) = \left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \begin{cases} 1 & \text{if} \quad q = 8n+1, \\ (-1)^d & \text{if} \quad q = 8n+5. \end{cases}$$

This is an immediate consequence of the theorem with $\nu = r = 1$.

If the class number $h(\sqrt{-q}) = 2$, then every prime p under consideration can be represented by (11). Recently Weinberger [10] showed that the only such primes are $q = 5$, 13, and 37. Therefore we can extend (3) to read:

Corollary 1.1. *If $q = 5, 13$, or 37 then $p = c^2 + qd^2$ and*

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^d.$$

More generally if $h(\sqrt{-q}) = 2k$, where k is odd, then we can be sure that a representation with ν odd exists, since ν divides k.

Corollary 1.2. *If $h(\sqrt{-q}) = 4$, then*

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \begin{cases} 1 & \text{if} \quad p = c^2 + qd^2, \\ -1 & \text{if} \quad 2p = c^2 + qd^2. \end{cases}$$

Proof. First of all if $h = 4$, then $q \equiv 1 \pmod 8$ and the first statement follows from the theorem with $\nu = r = 1$. Putting $r = 2$ and using (4) the second line follows.

Since $h = 4$ every $p \equiv 1 \pmod 4$ is represented by one of these two forms. It has been conjectured by Gauss and others that $q = 17, 73, 97$, and 193 are the only values of q for which $h(\sqrt{-q}) = 4$, but this has not been proved.

Corollary 1.3. *If* $h(\sqrt{-q}) = 8$, *then*

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \begin{cases} 1 & \text{if } p \text{ or } 2p = c^2+qd^2, \\ -1 & \text{otherwise.} \end{cases}$$

Proof. In this case $\left(\frac{\varepsilon_2}{q}\right) = 1$ by (4), so that $r = 1$ or 2 lead to $\left(\frac{\varepsilon_q}{p}\right) = 1$. The known primes for which $h(\sqrt{-q}) = 8$ are

$$q = 41,\ 113,\ 137,\ 313,\ 337,\ 457,\ 577.$$

It is again not known whether the list is complete or not. In order to find a value of r, which gives $\left(\frac{\varepsilon_q}{p}\right) = -1$, we can choose either a square of a non-residue of q, like 9 for $q = 41$, or a prime $\left(\frac{r}{q}\right) = 1$ such that $\left(\frac{\varepsilon_r}{q}\right) = -1$, like $r = 5$ for $q = 41 = 6^2+5$, since by Corollary 1 it is a suitable multiplier. In this case we cannot be sure that an odd power of p will be represented when p itself is not, since h has no odd divisors. More generally, using (4) we obtain with $r = 2$

Corollary 1.4. *If* $q = 8n+1$ *and if there exists a representation* $2p = c^2+qd^2$ *then*

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

Similarly using the theorem of Scholz [9] that the Pell equation $t^2-pqu^2 = -1$ has no solutions if $\left(\frac{\varepsilon_p}{q}\right) = -1$, we have

Corollary 1.5. *If* $p^\nu = c^2+qd^2$, *where* $q \equiv 5 \pmod 8$ *and* d *is odd, then the Pell equation* $t^2-pqu^2 = -1$ *has no solutions in integers.*

For $q = 5, 13$, and 37 the representation $p = c^2+qd^2$ always exists and Corollary 1.5 is applicable with $\nu = 1$. It can be used to explain the unsolvability of equations like $x^2-221y^2 = -1$ cited by Harvey Cohn [3] as illustrating the "unpredictability of algebraic number theory." For in this case $221 = 13\cdot 17$ and $17 = 2^2+13\cdot 1^2$. Epstein's [4] theorem mentioned in the introduction similarly disposes of Cohn's example with $D = 2p = 34$ since $17 = 3^2+8\cdot 1^2$. The least value of D not covered by known theorems is $D = 505 = 5\cdot 101$ since $101 = 9^2+5\cdot 2^2$, but the equation is not solvable. For $D = 2p$ the corresponding example is $D = 514 = 2\cdot 257$. Here d is obviously even, but there is no solution.

In case $q = 8n+1$ we have the following:

Corollary 1.6. *If* $rp^\nu = c^2+qd^2$, *where* $q \equiv 1 \pmod 8$ *and if* $r = s^2$ *with* $\left(\frac{s}{q}\right) = -1$, *or if* $r \equiv 1 \pmod 4$ *is a prime such that* $\left(\frac{\varepsilon_r}{q}\right) = -1$ *then* $t^2-pqu^2 = -1$ *has no integer solution, if* d *is odd.*

By Corollary 1.2 there will be no solution with $q = 17, 73, 97$, and 193 for all $p \equiv 1 \pmod 4$, for which $2p = c^2+qd^2$, such as $p = 89$. Thus $2\cdot 89 = 178 = 5^2+17\cdot 3^2$, hence $t^2-1513u^2 = -1$ has no solution.

On the other hand if $t^2-pru^2 = -1$ is solvable so that $N(\varepsilon_{pr}) = -1$ then if $r = 2$ or if $r \equiv 1 \pmod 4$ is a prime

$$\left(\frac{\varepsilon_p}{q}\right)\left(\frac{\varepsilon_r}{q}\right) = \left(\frac{\varepsilon_{pr}}{q}\right).$$

This result has been communicated to the author in a letter by Pierre Barrucand and can be made to follow from equation (30) of [8]. Applying it to Theorem 1 we obtain

Corollary 1.7. *If* $r = 2$ *or if* $r \equiv 1 \pmod 4$ *is a prime such that* $\left(\frac{r}{q}\right) = 1$, $N(\varepsilon_{pr}) = -1$ *and* $rp^\nu = c^2+qd^2$ *then*

$$\left(\frac{\varepsilon_{pr}}{q}\right) = \begin{cases} 1 & \text{if } q = 8n+1, \\ (-1)^d & \text{if } q = 8n+5. \end{cases}$$

Theorem 2. *Let*

$$p^\nu = c_1^2+8qd_1^2 \tag{12}$$

then

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{d_1}\left(\frac{\varepsilon_2}{p}\right).$$

Proof. First of all c_1 must be odd and $p \equiv 1 \pmod 8$. Then

$$\left(\frac{2}{c_1}\right) = (-1)^{(c_1^2-1)/8} = (-1)^{(p-1)/8}(-1)^{d_1}. \tag{13}$$

Taking (12) modulo q and p gives

$$\left(\frac{p}{q}\right)_4 = \left(\frac{c_1}{q}\right), \quad \left(\frac{q}{p}\right)_4 = \left(\frac{2}{p}\right)_4 \left(\frac{c_1 d_1}{p}\right).$$

If δ is the largest odd factor of d, then $\left(\frac{\delta}{p}\right) = 1$ and hence

$$\left(\frac{d_1}{p}\right) = 1 \quad \text{and} \quad \left(\frac{c_1}{p}\right) = \left(\frac{2}{c_1}\right)\left(\frac{c_1}{q}\right)$$

so that by (10) and (13)

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{2}{p}\right)_4 \left(\frac{2}{c_1}\right) = (-1)^{d_1} \left(\frac{\varepsilon_2}{p}\right).$$

A more general theorem for multiples of p, paralleling Theorem 1, can also be derived along the same lines. Since there is always a representation (12) for all primes p under consideration in case $h(\sqrt{-2q}) = 2$, i.e. only for $q = 5$ and $q = 29$, as proved by Weinberger [10], we can state

COROLLARY 2.1. *Let $p = 8n+1$ be a prime and let $q = 5$ or 29, then*

$$p = c_1^2 + 8qd_1^2 \quad \text{and} \quad \left(\frac{\varepsilon_q}{p}\right) = (-1)^{d_1} \left(\frac{\varepsilon_2}{p}\right).$$

Combining this with Corollary 1.1 we obtain

COROLLARY 2.2. *Let $p = 40n+1, 9$ be a prime, then*

$$p = c^2 + 5d^2 = c_1^2 + 40d_1^2$$

and

$$\left(\frac{\varepsilon_5}{p}\right) = (-1)^{d} = (-1)^{d_1} \left(\frac{\varepsilon_2}{p}\right).$$

Hence we get an unexpected dividend in the form

$$\left(\frac{\varepsilon_2}{p}\right) = (-1)^{d+d_1}$$

to add to the criteria obtained by Barrucand and Cohn [1].

THEOREM 3. *Let $p \equiv q \equiv 1 \pmod 8$ and let*

(14) $$p^{\nu} = 8c_2^2 + qd_2^2.$$

Then

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{\varepsilon_2}{p}\right) \left(\frac{\varepsilon_2}{q}\right) (-1)^{c_2}.$$

Proof. Since d_2 must be odd, $p \equiv qd_2^2 \pmod{16}$ if and only if c_2 is even, hence

(15) $$\left(\frac{2}{d_2}\right) = (-1)^{(pq-1)/8} (-1)^{c_2}.$$

Taking (14) modulo p and q we get

$$\left(\frac{p}{q}\right)_4 = \left(\frac{2}{q}\right)_4 \left(\frac{c_2}{p}\right), \qquad \left(\frac{q}{p}\right)_4 = \left(\frac{2}{p}\right)_4 \left(\frac{c_2 d_2}{p}\right).$$

If γ is the largest odd factor of c_2, then $\left(\frac{p}{\gamma}\right) = \left(\frac{q}{\gamma}\right)$ and

$$\left(\frac{c_2}{p}\right) = \left(\frac{c_2}{q}\right), \qquad \left(\frac{d_2}{p}\right) = \left(\frac{2}{d_2}\right).$$

Hence

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{2}{p}\right)_4 \left(\frac{2}{q}\right)_4 \left(\frac{2}{d_2}\right) = \left(\frac{\varepsilon_2}{p}\right) \left(\frac{\varepsilon_2}{q}\right) (-1)^{c_2}$$

by (10) and (15).

Using (5) and noting that if $h(\sqrt{-2q}) = 4$, then p itself must be represented by either (12) or (14), we can state

COROLLARY 3.1. *Let $p \equiv 1 \pmod 8$ and let $q = 17, 41$, or any other prime q (if it exists) with $h(\sqrt{-2q}) = 4$, then*

$$\left(\frac{\varepsilon_p}{q}\right) = \begin{cases} \left(\frac{2}{p}\right)_4 \left(\frac{2}{c_1}\right) & \text{if} \quad p = c_1^2 + 8qd_1^2, \\ -\left(\frac{2}{p}\right)_4 \left(\frac{2}{d_2}\right) & \text{if} \quad p = 8c_2^2 + qd_2^2. \end{cases}$$

We next turn to indefinite forms and obtain analogous theorems.

THEOREM 4. *Let*

(16) $$p^{\nu} = e^2 - 4qf^2$$

then

$$\left(\frac{\varepsilon_p}{q}\right) = \left(\frac{-1}{e}\right).$$

Proof. Taking (16) modulo p and q we have

$$\left(\frac{\varepsilon_p}{q}\right) = \left(\frac{e}{q}\right) \left(\frac{2ef}{p}\right).$$

Since e is odd, $p \equiv 1 \pmod 8$ if f is even. Hence

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

and therefore

(17) $$\left(\frac{\varepsilon_p}{q}\right) = \left(\frac{-1}{e}\right).$$

For real fields $h(\sqrt{q}) = 1$ is a common occurrence in which case p itself has the representation (16). Since h is odd the representation (16) always exists with ν some divisor of $h(\sqrt{q})$.

Combining Corollary 1 with Theorem 4, we have

COROLLARY 4.1. *Let* $p = c^2+qd^2 = e^2-4qf^2$, *then*

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{-1}{e}\right) = \begin{cases} 1 & \text{if} \quad q = 8n+1, \\ (-1)^d & \text{if} \quad q = 8n+5. \end{cases}$$

THEOREM 5. *Let*

(18) $$p^\nu = e_1^2-8qf_1^2$$

then

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{2}{p}\right)_4 \left(\frac{-2}{e_1}\right).$$

Proof. As before e_1 is odd and $p \equiv 1 \pmod 8$ and we get

$$\left(\frac{\varepsilon_p}{q}\right) = \left(\frac{2}{p}\right)_4 \left(\frac{e_1 f_1}{p}\right)\left(\frac{e_1}{q}\right)$$

while

$$\left(\frac{e_1}{p}\right) = \left(\frac{-2}{e_1}\right)\left(\frac{e_1}{q}\right), \qquad \left(\frac{f_1}{p}\right) = 1$$

and hence

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{2}{p}\right)_4 \left(\frac{-2}{e_1}\right).$$

Combining this with (5) we have

COROLLARY 5.1. *If* $p^\nu = e_1^2-8qf_1^2$ *then*

$$\left(\frac{\varepsilon_q}{p}\right) = \left(\frac{-2}{e_1}\right)(-1)^{h(\sqrt{-2q})/4}.$$

In particular for $q = 17$ and 41, when $h(\sqrt{-2q}) = 4$ we have

$$\left(\frac{\varepsilon_q}{p}\right) = -\left(\frac{-2}{e_1}\right).$$

Combining Theorems 4 and 5 we get one more expression for the quartic character of 2, namely

COROLLARY 5.2. *If* $p^\nu = e^2-4qf^2 = e_1^2-8qf_1^2$ *then*

$$\left(\frac{2}{p}\right)_4 = \left(\frac{2}{ee_1}\right).$$

For example for $q = 5$ and $p = 41 = 19^2-20\cdot 4^2 = 9^2-40\cdot 1^2$. Hence

$$\left(\frac{2}{p}\right)_4 = \left(\frac{2}{19}\right) = -1.$$

References

[1] P. Barrucand and H. Cohn, *Note on primes of the type* x^2+32y^2, J. Reine Angew. Math. 238 (1969), pp. 67–70.
[2] Jacob Brandler, *Residuacity properties of real quadratic units*, Thesis, University of Arizona, Tucson, Arizona, 1970.
[3] Harvey Cohn, *A Second Course in Number Theory*, New York 1962, p. 187.
[4] P. Epstein, *Zur Auflösbarkeit der Gleichung* $x^2-Dy^2 = -1$, J. Reine Angew. Math. 171 (1934), pp. 243–252.
[5] H. Hasse, *Über die Klassenzahl des Korpers* $P(\sqrt{-2p})$ *mit einer Primzahl* $p \neq 2$, Jurnal Number Theory, 1 (1969), pp. 231–234.
[6] Emma Lehmer, *On the quadratic character of some quadratic surds*, J. Reine Angew. Math. 250 (1971), pp. 42–48.
[7] J. Muskat and A. L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. 17 (1970), pp. 185–216.
[8] L. Redei, *Über die Pellsche Gleichung* $t^2-du^2 = -1$, J. Reine Angew. Math. 173 (1935), pp. 193–221.
[9] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2-Du^2 = -4$, Math. Zeitschr. 39 (1934), p. 97.
[10] P. Weinberger, *Proof of a conjecture of Gauss on class number two*, Thesis, University of California, Berkeley, 1969.

Received on 17. 8. 1971 (207)