Can. J. Math., Vol. XXXVII, No. 2, 1985, pp. 337-370

CRITERIA FOR BIQUADRATIC RESIDUACITY MODULO A PRIME p INVOLVING QUATERNARY REPRESENTATIONS OF p

KENNETH S. WILLIAMS, CHRISTIAN FRIESEN AND LAWRENCE J. HOWE

1. Introduction. In 1958, Hasse [**10**, p. 236], in connection with his work on the 2^n-th power character of 2 in the cyclotomic field $Q(\exp(2\pi i/2^n))$, proved that for every prime $p \equiv 1 \pmod{16}$ the pair of equations

$$\begin{cases} p = x^2 + 2u^2 + 2v^2 + 2w^2, \\ 2xw = v^2 - 2uv - u^2, \end{cases}$$

is always solvable in integers x, u, v, w. Later in 1972 Giudici, Muskat, and Robinson [**7**, p. 388] showed in their work on Brewer's character sums that Hasse's system is also solvable for primes $p \equiv 7 \pmod{16}$. Moreover they also showed [**7**, p. 345] that for primes $p \equiv 1 \pmod 5$ the pair of equations

$$\begin{cases} p = x^2 + 5u^2 + 5v^2 + 5w^2, \\ xw = v^2 - uv - u^2, \end{cases}$$

is solvable in integers x, u, v, w. In this paper we consider a pair of diophantine equations (involving a prime p and an integer m) which includes the above two systems as the special cases when $m = 2$ and $m = 5$. The system is then used to give criteria for m to be a biquadratic residue moduio p.

Let m denote an odd nonsquare positive integer which is expressible as the sum of two squares, say,

$$m = a_1^2 + a_2^2,\ a_1 \text{ odd},\ a_2 \text{ even},\ a_1 > 0,\ a_2 > 0.$$

Clearly we have $m \equiv 1 \pmod 4$ and

$$a_2 \equiv \frac{1}{2}(m - 1) \pmod 4.$$

Received December 13, 1983 and in revised form June 5, 1984. The research of the first author was supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233, while that of the second and third authors was supported by Natural Sciences and Engineering Research Council Canada Undergraduate Summer Research Awards.

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

We shall be interested in those odd primes p (not dividing m, a_1 or a_2) for which there are integers x, u, v, w, a non-negative integer n, and an odd positive integer l such that either

$$\text{(1.1)} \quad \begin{cases} 2^n p^l = x^2 + mu^2 + mv^2 + mw^2, \\ 2xw = a_1 v^2 - 2a_2 uv - a_1 u^2, \end{cases}$$

or

$$\text{(1.2)} \quad \begin{cases} 2^n p^l = x^2 + mu^2 + mv^2 + mw^2, \\ 2xw = a_2 v^2 - 2a_1 uv - a_2 u^2, \end{cases}$$

holds.

We note that it follows from (1.1), (1.2) and the identity

$$(a_1 v^2 \mp 2a_2 uv - a_1 u^2)^2 + (a_2 v^2 \pm 2a_1 uv - a_2 u^2)^2$$
$$= m(u^2 + v^2)^2,$$

that solutions of (1.1) satisfy

$$\text{(1.3)} \quad 2^{n+2} p^l x^2 = (2x^2 + mu^2 + mv^2)^2$$
$$-m(a_2 v^2 + 2a_1 uv - a_2 u^2)^2$$

and the solutions of (1.2) satisfy

$$\text{(1.4)} \quad 2^{n+2} p^l x^2 = (2x^2 + mu^2 + mv^2)^2$$
$$-m(a_1 v^2 + 2a_2 uv - a_1 u^2)^2.$$

Use of the equations (1.3) and (1.4) will be made on a number of occasions throughout the paper.

It will be shown in the lemma in Section 2 that if $n \geqq 5$ the integers x, u, v, w given by either (1.1) or (1.2) are all even, so dividing each of x, u, v, w by the highest power of 2 in their G. C. D. gives a representation of the same type with $n \leqq 4$. Henceforth we will assume $n \leqq 4$.

In the case of the representation (1.1), it will be shown in the lemma that all of x, u, v, w are even if $n \geqq 2$. Thus for the representation (1.1) we may further assume that $n = 0$ or 1. Moreover it will also be shown in the lemma that when $n = 1$ we must have $m \equiv 1 \pmod 8$.

Also in the case of the representation (1.2), it will be shown in the lemma that x, u, v, w are all even in the following cases:

$$n = 2,\ m \equiv 5 \pmod 8,$$

$$n = 3,$$

$$n = 4,\ m \equiv 1 \pmod 8).$$

Thus in these cases the system (1.2) can be reduced to a similar system with $n \leqq 2$. Moreover when $n = 1$ it will be shown that we must have $m \equiv 1 \pmod 8$.

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

Summarizing we see that we need consider (1.1) only when $n = 0$ or $n = 1$, $m \equiv 1 \pmod 8$; and (1.2) only when $n = 0$ or $n = 1$, $m \equiv 1 \pmod 8$ or $n = 2$, $m \equiv 1 \pmod 8$ or $n = 4$, $m \equiv 5 \pmod 8$.

Next for both the representation (1.1) and the representation (1.2) we have

$$\left(\frac{m}{p}\right) = \left(\frac{p}{m}\right)$$

(by the law of quadratic reciprocity)

$$= \left(\frac{2}{m}\right)^n \left(\frac{2^n p^l}{m}\right)$$

(as l is odd)

$$= \left(\frac{2}{m}\right)^n \left(\frac{x^2 + mu^2 + mv^2 + mw^2}{m}\right)$$

(by (1.1) and (1.2))

$$= \left(\frac{2}{m}\right)^n \left(\frac{x^2}{m}\right)$$

$$= \left(\frac{2}{m}\right)^n$$

(as GCD$(x, m) = 1$)

$$= 1$$

(as $m \equiv 1 \pmod 8$ when $n = 1$). Hence m is a quadratic residue $(\bmod\ p)$.

In this paper we prove, using only the law of quadratic reciprocity, necessary and sufficient conditions for m to be a biquadratic residue modulo a prime $p \equiv 1 \pmod 4$ in terms of the parameters x, u, v, w in either the representation (1.1) or the representation (1.2). We prove in Section 3 the following theorem.

THEOREM 1. *Let m be an odd nonsquare positive integer such that $m = a_1^2 + a_2^2$, a_1 odd, a_2 even. Let $p \equiv 1 \pmod 4$ be a prime (not dividing m, a_1 or a_2) such that either* (1.1) *or* (1.2) *is solvable.*

(a) *If* (1.1) *is solvable with $n = 0$ then*

$$u \equiv v \equiv 0 \pmod 2 \quad \textit{and}$$

$$\left(\frac{m}{p}\right)_4 = (-1)^{(u-v)/2}.$$

(b) *If* (1.1) *is solvable with $n = 1$ then*

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

$$m \equiv 1 \pmod 8 \quad \textit{and}$$

$$\left(\frac{m}{p}\right)_4 = (-1)^{\frac{x}{2}+\frac{m-1}{8}} = (-1)^{\frac{w}{2}+\frac{m-1}{8}}.$$

(c) *If* (1.2) *is solvable with* $n = 0$ *then*

$$\left(\frac{m}{p}\right)_4 = \begin{cases} +1, \textit{ if } m \equiv 1 \pmod 8, \\ (-1)^{x+1} = (-1)^{w} = (-1)^{\frac{p-1}{4}+\frac{u-v}{2}}, \\ \qquad\qquad \textit{if } m \equiv 5 \pmod 8. \end{cases}$$

(d) *If* (1.2) *is solvable with* $n = 1$ *then*

$$m \equiv 1 \pmod 8 \textit{ and } a_2 \equiv 0 \pmod 8, \quad \textit{and}$$

$$\left(\frac{m}{p}\right)_4 = (-1)^{(m-1)/8}.$$

(e) *If* (1.2) *is solvable with* $n = 2$ *and* x, u, v, w *not all even, then* $m \equiv 1 \pmod 8$ *and*

$$\left(\frac{m}{p}\right)_4 = (-1)^{a_2/4}.$$

(f) *If* (1.2) *is solvable with* $n = 4$ *and* x, u, v, w *not all even, then* $m \equiv 5 \pmod 8$ *and*

$$\left(\frac{m}{p}\right)_4 = (-1)^{\frac{x^2w^2-1}{8}+\frac{m-5}{8}}.$$

Example. The system (1.1) is solvable with $m = 5$, $a_1 = 1$, $a_2 = 2$, $n = 0$, $l = 3$, $p = 29$, $x = 142$, $u = -6$, $v = 28$, $w = 5$. By Theorem 1 (a) we have

$$\left(\frac{5}{29}\right)_4 = (-1)^{(-6-28)/2} = -1.$$

Indeed we have

$$5 \equiv 11^2 \pmod{29}, \quad \left(\frac{11}{29}\right) = -1.$$

In the remainder of the paper for simplicity we just treat the case when m is an odd prime. It is hoped to treat the case of composite m in another paper. If $m \equiv 1 \pmod 8$ we will need, on occasion, the following result of Gauss, namely,

$$\left(\frac{2}{m}\right)_4 = (-1)^{a_2/4}.$$

Let

$$(1.5)\quad \begin{aligned} K_1 &= Q(i\sqrt{m \pm a_1\sqrt{m}}) = Q(i\sqrt{2m \pm 2a_2\sqrt{m}}) \\ K_2 &= Q(i\sqrt{m \pm a_2\sqrt{m}}) = Q(i\sqrt{2m \pm 2a_1\sqrt{m}}). \end{aligned}$$

Each field K_j $(j = 1, 2)$ is a cyclic extension of degree 4 over the rationals, see for example [**6**]. In Section 4 the arithmetic of these fields, together with some results on their class numbers due to Brown and Parry [**3**] [**4**], is used to give a wide range of instances where the systems (1.1) $(j = 1)$ and (1.2) $(j = 2)$ are solvable. Denoting the class number of K_j $(j = 1, 2)$ by h_j, we prove the following theorem in Section 4.

THEOREM 2. *Let $m \equiv 1 \pmod 4$ be a prime so that there are unique positive integers a_1 and a_2 such that $m = a_1^2 + a_2^2$, a_1 odd, a_2 even.*

(i) *Let p be an odd prime $(p \nmid ma_1a_2)$ such that*

$$\left(\frac{p}{m}\right) = 1, \quad \left(\frac{p}{m}\right)_4 = \left(\frac{2(-1)^{(m-5)/4}}{p}\right).$$

Then

(a) *if $m \equiv 5 \pmod 8$, (1.1) is solvable with $l = h_1/2 \equiv 1 \pmod 2$ and $n = 0$;*

(b) *if $m \equiv 1 \pmod 8$ and $\left(\frac{2}{m}\right)_4 = -1$, (1.1) is solvable with $l = h_1/4 \equiv 1 \pmod 2$ and $n = 0$ or 1 according as*

$$\left(\frac{p}{m}\right)_4 = \left(\frac{-2}{p}\right) = 1 \quad \text{or} \quad \left(\frac{p}{m}\right)_4 = \left(\frac{-2}{p}\right) = -1.$$

(ii) *Let p be an odd prime $(p \nmid ma_1a_2)$ such that*

$$\left(\frac{p}{m}\right) = 1, \quad \left(\frac{p}{m}\right)_4 = \left(\frac{(-1)^{(m-5)/4}}{p}\right).$$

Then

(a) *if $m \equiv 5 \pmod 8$, (1.2) is solvable with $l = h_2 \equiv 1 \pmod 2$ and $n = 0$ or 4 according as $m = 5$ or $m > 5$;*

(b) *if $m \equiv 1 \pmod 8$ and $\left(\frac{2}{m}\right)_4 = -1$, (1.2) is solvable with $l = h_2/4 \equiv 1 \pmod 2$ and $n = 2$ or 1 according as*

$$\left(\frac{p}{m}\right)_4 = \left(\frac{-1}{p}\right) = 1 \quad \text{or} \quad \left(\frac{p}{m}\right)_4 = \left(\frac{-1}{p}\right) = -1.$$

Putting Theorems 1 and 2 together we obtain immediately the following theorem.

THEOREM 3. (a) *Let $m = a_1^2 + a_2^2 \equiv 5 \pmod 8$ be a prime and let $p \equiv 1 \pmod 4$ be a prime $(p \nmid a_1a_2)$ such that*

$$\left(\frac{p}{m}\right) = 1 \quad \left(\frac{p}{m}\right)_4 = \left(\frac{2}{p}\right)$$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

Then

$$\left(\frac{m}{p}\right)_4 = (-1)^{(u-v)/2},$$

where

$$\begin{cases} p^{h_1/2} = x^2 + mu^2 + mv^2 + mw^2, \\ 2xw = a_1v^2 - 2a_2uv - a_1u^2. \end{cases}$$

(b) *Let* $m = a_1^2 + a_2^2 \equiv 1 \pmod 8$ *be a prime such that* $\left(\frac{2}{m}\right)_4 = -1$ *and let* $p \equiv 1 \pmod 4$ *be a prime* $(p \nmid a_1a_2)$ *such that*

$$\left(\frac{p}{m}\right) = 1, \quad \left(\frac{p}{m}\right)_4 = \left(\frac{2}{p}\right).$$

If $\left(\frac{p}{m}\right)_4 = \left(\frac{2}{p}\right) = 1$ *then*

$$\left(\frac{m}{p}\right)_4 = (-1)^{(u-v)/2},$$

where

$$\begin{cases} p^{h_1/4} = x^2 + mu^2 + mv^2 + mw^2, \\ 2xw = a_1v^2 - 2a_2uv - a_1u^2, \end{cases}$$

and if $\left(\frac{p}{m}\right)_4 = \left(\frac{2}{p}\right) = -1$ *then*

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

where

$$\begin{cases} 2p^{h_1/4} = x^2 + mu^2 + mv^2 + mw^2, \\ 2xw = a_1v^2 - 2a_2uv - a_1u^2. \end{cases}$$

(c) *Let* $m = a_1^2 + a_2^2 \equiv 5 \pmod 8$ *be a prime* > 5 *and let* $p \equiv 1 \pmod 4$ *be a prime* $(p \nmid a_1a_2)$ *such that*

$$\left(\frac{p}{m}\right) = \left(\frac{p}{m}\right)_4 = 1.$$

Then

$$\left(\frac{m}{p}\right)_4 = \begin{cases} (-1)^{\frac{x}{4}+1} = (-1)^{w/4} = (-1)^{\frac{p-1}{4}+\frac{u-v}{8}}, \\ \quad \text{if } x, u, v, w \text{ are all even}, \\ (-1)^{\frac{x^2w^2-1}{8}+\frac{m-5}{8}}, \text{ if } x, u, v, w \text{ are not all even}, \end{cases}$$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

where

$$\begin{cases} 16p^{h_2} = x^2 + mu^2 + mv^2 + mw^2, \\ 2xw = a_2v^2 - 2a_1uv - a_2u^2. \end{cases}$$

[*We note that for* $m = 5$, *we have* $h_2 = 1$, *and the result in this case is as follows*:

Let $p \equiv 1 \pmod{20}$ *be a prime then*

$$\left(\frac{5}{p}\right)_4 = (-1)^{x+1} = (-1)^w = (-1)^{\frac{p-1}{4}+\frac{u-v}{2}},$$

where

$$\begin{cases} p = x^2 + 5u^2 + 5v^2 + 5w^2, \\ xw = v^2 - uv - u^2.] \end{cases}$$

(d) *Let* $m = a_1^2 + a_2^2 \equiv 1 \pmod 8$ *be a prime such that* $\left(\frac{2}{m}\right)_4 = -1$ *and let* $p \equiv 1 \pmod 4$ *be a prime* ($p \nmid a_1a_2$) *such that*

$$\left(\frac{p}{m}\right) = \left(\frac{p}{m}\right)_4 = 1.$$

Then

$$\left(\frac{m}{p}\right)_4 = (-1)^w,$$

where

$$\begin{cases} 4p^{h_2/4} = x^2 + mu^2 + mv^2 + mw^2 \\ 2xw = a_2v^2 - 2a_1uv - a_2u^2. \end{cases}$$

A computer program was run to determine the values of h_1 and h_2, from a formula of Hasse [**9**], for all primes $m \equiv 1 \pmod 4$ which are less than 1000. For those values of m covered by Theorem 3 the corresponding values of l were than calculated. For $m < 100$ these values are given below in Table I, while the complete table of values is given in Table 4 in Section 5.

m	h_1	l	h_2	l
5	2	1	1	1
13	2	1	1	1
17	4	1	4	1
29	26	13	1	1
37	50	25	1	1
41	20	5	4	1
53	18	9	1	1
61	82	41	1	1
73	16	–	40	–
89	64	–	8	–
97	20	5	52	13

TABLE 1

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

For those cases with $l = 1$ Theorems 2 and 3 take a particularly simple form, which lends itself to numerical calculation, as only representations of multiples of p (rather than powers of p) are involved. Moreover, we show that in these cases all the solutions of (1.1) or (1.2) are given in terms of one solution (x, u, v, w), as follows:

$$\text{(1.6)} \qquad \pm(x, u, v, w), \pm(x, -v, u, -w),$$
$$\pm(x, -u, -v, w), \pm(x, v, -u, -w).$$

A summary of the results in these cases is given in Tables 2 and 3.

m	n	$2^n p = x^2 + mu^2 + mv^2 + mw^2$ $2xw = a_1 v^2 - 2a_2 uv - a_1 u^2$ is solvable for p given below	$\left(\frac{m}{p}\right)_4 \ (p \equiv 1(4))$
5	0	$\left(\frac{p}{5}\right) = 1, \left(\frac{p}{5}\right)_4 = \left(\frac{2}{p}\right)$	$(-1)^{(u-v)/2}$
13	0	$\left(\frac{p}{13}\right) = 1, \left(\frac{p}{13}\right)_4 = \left(\frac{2}{p}\right)$	$(-1)^{(u-v)/2}$
17	0	$\left(\frac{p}{17}\right) = \left(\frac{p}{17}\right)_4 = \left(\frac{-2}{p}\right) = 1$	$(-1)^{(u-v)/2}$
	1	$\left(\frac{p}{17}\right) = 1, \left(\frac{p}{17}\right)_4 = \left(\frac{-2}{p}\right) = -1$	$(-1)^{w/2}$

TABLE 2

TABLE 3

m	n	$2^n p = x^2 + mu^2 + mv^2 + mw^2$ $2xw = a_2 v^2 - 2a_1 uv - a_2 u^2$ is solvable for p given below	$\left(\frac{m}{p}\right)_4 \ (p \equiv 1(4))$	References
5	0	$\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)_4 = 1$	$(-1)^w$	Part of this is given in [**7**, Theorem 8]
13	4	$\left(\frac{p}{13}\right) = \left(\frac{p}{13}\right)_4 = 1$	$(-1)^{w/4}$ (w even) $(-1)^{(x^2w^2+7)/8}$ (w odd)	Part of this can be deduced from [**16**, Theorem 1]
17	2	$\left(\frac{p}{17}\right) = \left(\frac{p}{17}\right)_4 = \left(\frac{-1}{p}\right) = 1$	$(-1)^w$	
	1	$\left(\frac{p}{17}\right) = 1, \left(\frac{p}{17}\right)_4 = \left(\frac{-1}{p}\right) = -1$		
29	4	$\left(\frac{p}{29}\right) = \left(\frac{p}{29}\right)_4 = 1$	$(-1)^{w/4}$ (w even) $(-1)^{(x^2w^2+7)/8}$ (w odd)	Part of this can be deduced from [**12**]
37	4	$\left(\frac{p}{37}\right) = \left(\frac{p}{37}\right)_4 = 1$	$(-1)^{w/4}$ (w even) $(-1)^{(x^2w^2-1)/8}$ (w odd)	Part of this can be deduced from [**12**]

TABLE 3 (continued)

41	2	$\left(\frac{p}{41}\right) = \left(\frac{p}{41}\right)_4 = \left(\frac{-1}{p}\right) = 1$	$(-1)^w$	
	1	$\left(\frac{p}{41}\right) = 1, \left(\frac{p}{41}\right)_4 = \left(\frac{-1}{p}\right) = -1$		Part of this can be deduced from [**12**]
53	4	$\left(\frac{p}{53}\right) = \left(\frac{p}{53}\right)_4 = 1$	$(-1)^{w/4}$ (w even) $(-1)^{(x^2w^2-1)/8}$ (w odd)	
61	4	$\left(\frac{p}{61}\right) = \left(\frac{p}{61}\right)_4 = 1$	$(-1)^{w/4}$ (w even) $(-1)^{(x^2w^2+7)/8}$ (w odd)	Part of this can be deduced from [**12**]

Finally we remark that we have not been able to formulate the results corresponding to Theorems 2 and 3 for a general prime $m \equiv 1 \pmod 8$ for which $\left(\frac{2}{m}\right)_4 = 1$ (this includes $m = 73$ and 89). In these cases both h_1 and h_2 are divisible by 8. However in the special case of a prime $m \equiv 9 \pmod{16}$ for which $\left(\frac{2}{m}\right)_4 = 1$ we do have a conjecture concerning the solvability of (1.2).

CONJECTURE. *Let* $m = a_1^2 + a_2^2 \equiv 9 \pmod{16}$ *be a prime such that* $\left(\frac{2}{m}\right)_4 = 1$ *and let p be an odd prime* ($p \nmid ma_1a_2$) *such that*

$$\left(\frac{p}{m}\right) = 1, \quad \left(\frac{p}{m}\right)_4 = \left(\frac{(-1)^{(m-5)/4}}{p}\right).$$

Then (1.2) *is always insolvable if*

$$\left(\frac{p}{m}\right)_4 = \left(\frac{-1}{p}\right) = -1,$$

whereas, if

$$\left(\frac{p}{m}\right)_4 = \left(\frac{-1}{p}\right) = 1,$$

(1.2) *is solvable with* $l = h_2/8 \equiv 1 \pmod 2$ *and either* $n = 1$ *or* 2.

If this conjecture is true then applying Theorem 1 we obtain the following result.

THEOREM 4. *Let* $m = a_1^2 + a_2^2 \equiv 9 \pmod{16}$ *be a prime such that* $\left(\frac{2}{m}\right)_4 = +1$ *and let* $p \equiv 1 \pmod 4$ *be a prime such that*

$$\left(\frac{p}{m}\right) = \left(\frac{p}{m}\right)_4 = 1.$$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

Then assuming the truth of the above conjecture we have

$$\left(\frac{m}{p}\right)_4 = \begin{cases} +1, \text{ if } \begin{cases} 4p^{h_2/8} = x^2 + mu^2 + mv^2 + mw^2 \\ 2xw = a_2v^2 - 2a_1uv - a_2u^2 \end{cases}, \\ \\ -1, \text{ if } \begin{cases} 2p^{h_2/8} = x^2 + mu^2 + mu^2 + mw^2 \\ 2xw = a_2v^2 - 2a_1uv - a_2u^2 \end{cases}. \end{cases}$$

2. *Proof of lemma.* In the lemma below we give congruences satisfied by solutions of (1.1) and (1.2). These congruences are all obtained in an elementary way by considering (1.1) and (1.2) modulo small powers of 2. These congruences will be used on many occasions in the proofs of the three theorems. Although the details are different, the proofs of the various cases in the lemma are so similar we only give the proofs of two of the cases.

LEMMA. (a) *If the system* (1.1) *is solvable with* $n = 0$ *then*

$$x \equiv w + 1 \pmod 2, \ u \equiv v \pmod 2,$$

and

$$u \equiv v \equiv 0 \pmod 2, \text{ if } p \equiv 1 \pmod 4,$$
$$u \equiv v \equiv 1 \pmod 2, \text{ if } p \equiv 3 \pmod 4.$$

Moreover

$$\begin{aligned} xw &\equiv 0 \pmod 4, \text{ if } m \equiv 1 \pmod 8, p \equiv 3 \pmod 8, \\ x &\equiv 1 \pmod 2, \text{ if } m \equiv 5 \pmod 8, p \equiv 1 \pmod 8, \\ x &\equiv 2 \pmod 4, \text{ if } m \equiv 5 \pmod 8, p \equiv 3 \pmod 8, \\ x &\equiv 0 \pmod 2, \text{ if } m \equiv p \equiv 5 \pmod 8, \\ w &\equiv 2 \pmod 4, \text{ if } m \equiv 5 \pmod 8, p \equiv 7 \pmod 8. \end{aligned}$$

The case $m \equiv 1 \pmod 8$, $p \equiv 5$ *or* $7 \pmod 8$ *does not occur.*

(b) *If the system* (1.1) *is solvable with* $n = 1$ *then* $m \equiv 1 \pmod 8$ *and*

$$x \equiv w \equiv 0 \pmod 2, \ u \equiv v \equiv 1 \pmod 2,$$
$$x \equiv w + p - 1 \pmod 4$$

and

$$p \equiv 1, 3 \pmod 8, \quad \text{if } a_2 \equiv 0 \pmod 8,$$
$$p \equiv 5, 7 \pmod 8, \quad \text{if } a_2 \equiv 4 \pmod 8.$$

(c) *If the system* (1.1) *is solvable with* $n \geqq 2$ *then* x, u, v, w *are all even.*

(d) *If the system* (1.2) *is solvable with* $n = 0$ *then we have the following congruences.*

$m \pmod 8$	$p \pmod 4$	*congruences*
1	1	$x \equiv w + 1 \pmod 2$, $xw \equiv 0 \pmod 4$, $u \equiv v \equiv 0 \pmod 2$, $u \equiv v + \frac{1}{2}(p - 1) \pmod 4$

$m \pmod 8$	$p \pmod 4$	*congruences*
		or $x \equiv w \equiv 0 \pmod 2$, $x \equiv w + \frac{1}{2}(a_2 + p - 1) \pmod 4$, $u \equiv v + 1 \pmod 2$, $uv \equiv \frac{a_2}{2} \pmod 4$
1	3	*does not occur*
5	1	$x \equiv 1 \pmod 2$, $w \equiv 0 \pmod 4$, $u \equiv v \equiv 0 \pmod 2$, $u \equiv v + \frac{1}{2}(p - 1) \pmod 4$ *or* $x \equiv 0 \pmod 4$, $w \equiv 1 \pmod 2$, $u \equiv v \equiv 0 \pmod 2$, $u \equiv v + \frac{1}{2}(p - 5) \pmod 4$
5	3	$x \equiv w \equiv 1 \pmod 2$, $u \equiv v + 1 \pmod 2$

(e) *If the system* (1.2) *is solvable with* $n = 1$ *then* $m \equiv 1 \pmod 8$ *and*

$$x \equiv w + 1 \pmod 2, \quad u \equiv v + 1 \pmod 2$$

and

$$p \equiv 1 \pmod 4, \text{ if } a_2 \equiv 0 \pmod 8,$$

$$p \equiv 3 \pmod 4, \text{ if } a_2 \equiv 4 \pmod 8.$$

(f) *if the system* (1.2) *is solvable with* $n = 2$ *then*

$$\begin{cases} x \equiv u \equiv v \equiv w \pmod 2, \ p \equiv 1 \pmod 4, & \text{if } m \equiv 1 \pmod 8, \\ x \equiv u \equiv v \equiv w \equiv 0 \pmod 2, & \text{if } m \equiv 5 \pmod 8. \end{cases}$$

(g) *If the system* (1.2) *is solvable with* $n = 3$ *then* x, u, v, w *are all even.*

(h) *If the system* (1.2) *is solvable with* $n = 4$ *then*

$$\begin{cases} x \equiv u \equiv v \equiv w \equiv 0 \pmod 2, & \text{if } m \equiv 1 \pmod 8, \\ x \equiv u \equiv v \equiv w \pmod 2, & \text{if } m \equiv 5 \pmod 8. \end{cases}$$

(i) *If the system* (1.2) *is solvable with* $n \geqq 5$ *then* x, u, v, w *are all even.*

Proof of (b). Taking the first equation in (1.1) modulo 4 we obtain

$$2 \equiv x^2 + u^2 + v^2 + w^2 \pmod 4,$$

so that exactly two of x, u, v, w are even. From the second equation in (1.1) we see that $u \equiv v \pmod 2$ so that

$$x \equiv w \pmod 2.$$

Reducing the second equation in (1.1) modulo 4 we obtain

$$x \equiv w \equiv 0 \pmod 2,$$

and thus

$$u \equiv v \equiv 1 \pmod{2}.$$

The first equation in (1.1) taken modulo 8 gives

$$2p \equiv x^2 + 2 + w^2 \pmod{8}$$

so that

$$x \equiv w + p - 1 \pmod{4}.$$

Then from the second equation in (1.1), taken modulo 8, we get

$$a_2 \equiv 0 \pmod{4}$$

so that $m \equiv 1 \pmod{8}$. Next, taking (1.1) modulo 16, we have

$$\begin{cases} 2p \equiv x^2 + u^2 + v^2 + w^2 \pmod{16}, \\ 2xw \equiv v^2 - u^2 - 2a_2 \pmod{16}, \end{cases}$$

so modulo 16 we have

$$\begin{aligned} 2a_2 &\equiv v^2 - u^2 - (x + w)^2 + x^2 + w^2 \\ &\equiv v^2 - u^2 - (p - 1)^2 + 2p - u^2 - v^2 \\ &\equiv 3 - (p - 2)^2 - 2u^2 \\ &\equiv 1 - (p - 2)^2, \end{aligned}$$

which gives the required result.

Proof of (i). Taking the first equation in (1.2) modulo 8 gives

$$x^2 + m(u^2 + v^2 + w^2) \equiv 0 \pmod{8}.$$

If $m \equiv 1 \pmod{8}$ then clearly x, u, v, w are all even as required. If $m \equiv 5 \pmod{8}$ then either

$$x \equiv u \equiv v \equiv w \equiv 0 \pmod{2},$$

as required, or

$$x \equiv u \equiv v \equiv w \equiv 1 \pmod{2}.$$

In the latter case we define integers A and B by

$$A = \frac{1}{4}(2x^2 + mu^2 + mv^2),$$

$$B = \frac{1}{4}(a_1(v^2 - u^2) + 2a_2uv).$$

Then we have

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

$$4A \equiv 2 + 5 + 5 \equiv 4 \pmod{8},$$

$$4B \equiv 0 + 4 \equiv 4 \pmod{8},$$

so both A and B are odd. From (1.4) we have

$$2^{n-2}p^l x^2 = A^2 - mB^2.$$

Taking this equation modulo 8 we clearly get a contradiction. Hence x, u, v, w are not all odd and the result is proved.

3. Proof of theorem 1. As the proofs of the six parts of Theorem 1 all follow along the same lines with only the technical details differing, we will just give the proof of (b).

Let (x, u, v, w) be a solution of

$$(3.1) \qquad \begin{cases} 2p^l = x^2 + mu^2 + mv^2 + mw^2, \\ 2xw = a_1v^2 - 2a_2uv - a_1u^2, \end{cases}$$

where p is a prime $\equiv 1 \pmod 4$ and l is a positive odd integer. By the lemma we have $m \equiv 1 \pmod 8$ (so that $a_2 \equiv 0 \pmod 4$) and

$$(3.2) \qquad x \equiv w \equiv 0 \pmod 2, \ u \equiv v \equiv 1 \pmod 2, \ x \equiv w \pmod 4.$$

From (3.2) we see that

$$(3.3) \qquad 2x^2 + mu^2 + mv^2 \equiv 2 \pmod 8,$$

$$a_2v^2 + 2a_1uv - a_2u^2 \equiv 2 \pmod 4,$$

so that we can define a positive odd integer g by

$$(3.4) \qquad 2g = \mathrm{GCD}(2x^2 + mu^2 + mv^2, |a_2v^2 + 2a_1uv - a_2u^2|).$$

Next we define positive coprime odd integers A and B by

$$(3.5) \qquad A = \frac{2x^2 + mu^2 + mv^2}{2g}, \ B = \frac{|a_2v^2 + 2a_1uv - a_2u^2|}{2g}.$$

We note that a simple argument shows that

$$(3.6) \qquad \mathrm{GCD}\,(g, p) = 1.$$

Appealing to (1.3) we obtain

$$(3.7) \qquad 2p^l x^2 = g^2(A^2 - mB^2).$$

From (3.7) we deduce that

$$(3.8) \qquad x = 2gX,$$

where X is an integer satisfying

$$(3.9) \qquad 8p^l X^2 = A^2 - mB^2.$$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

Further it is easy to deduce from (3.9) that

$$(3.10) \quad \mathrm{GCD}(A, p) = \mathrm{GCD}(B, p) = \mathrm{GCD}(A, X) = \mathrm{GCD}(B, X) = \mathrm{GCD}(A, m) = 1.$$

Next we show that g is a square. Suppose g is not a square. Then there exists an odd prime $q \neq p$ such that $q^{2K+1} \| g$ for some integer K. Hence we have

$$(3.11) \quad q^{2K+1} | x,$$

$$(3.12) \quad q^{2K+1} | 2x^2 + mu^2 + mv^2,$$

$$(3.13) \quad q^{2K+1} | \mathrm{a}_2 v^2 + 2a_1 uv - a_2 u^2.$$

From (3.1) and (3.11) we have

$$(3.14) \quad q^{2K+1} | a_1 v^2 - 2a_2 uv - a_1 u^2.$$

Hence from (3.13) and (3.14) we obtain

$$q^{2K+1} | a_1(a_2 v^2 + 2a_1 uv - a_2 u^2) - a_2(a_1 v^2 - 2a_2 uv - a_1 u^2),$$

that is

$$q^{2K+1} | 2muv.$$

As $\mathrm{GCD}(x, m) = 1$ we have $q|m$ and so

$$(3.15) \quad q^{2K+1} | uv.$$

Hence from (3.13), (3.14) and (3.15) we have

$$q^{2K+1} | a_2(v^2 - u^2), \quad q^{2K+1} | a_1(v^2 - u^2),$$

and so,

$$q^{2K+1} | m(v^2 - u^2),$$

that is

$$(3.16) \quad q^{2K+1} | v^2 - u^2.$$

From (3.15) and (3.16) we have

$$q^{K+1} | u, \quad q^{K+1} | v.$$

Hence we have

$$q^{2K+2} | 2x^2 + mu^2 + mv^2$$

and

$$q^{2K+2} | a_2 v^2 + 2a_1 uv - a_2 u^2,$$

which contradicts that $q^{2K+1} \| g$. This completes the proof that g is a

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

square. Hence $g \equiv 1 \pmod 8$ and so

$$A \equiv 1 \pmod 4.$$

From (3.5) we obtain

$$(3.17) \quad 2A \equiv 4x + m(u^2 + v^2) \equiv 4x + a_1^2(u^2 + v^2) \pmod{16}$$

and

$$(3.18) \quad B \equiv \pm a_1 uv \pmod 8.$$

Next by the law of quadratic reciprocity we have

$$\left(\frac{A}{p}\right) = \left(\frac{p}{A}\right)$$

(as $p \equiv 1 \pmod 4$)

$$= \left(\frac{2}{A}\right)\left(\frac{8p^lX^2}{A}\right)$$

(as l is odd)

$$= \left(\frac{2}{A}\right)\left(\frac{-m}{A}\right)$$

(by (3.9))

$$= \left(\frac{2}{A}\right)\left(\frac{A}{m}\right)$$

(as $A \equiv 1 \pmod 4$)

$$= \left(\frac{2}{A}\right)\left(\frac{2gA}{m}\right)$$

(as g is a square and $m \equiv 1 \pmod 8$)

$$= \left(\frac{2}{A}\right)$$

(by (3.5)), and

$$\left(\frac{B}{p}\right) = \left(\frac{p}{B}\right)$$

(as $p \equiv 1 \pmod 4$)

$$= \left(\frac{2}{B}\right)\left(\frac{8p^lX^2}{B}\right)$$

(as l is odd)

$$= \left(\frac{2}{B}\right) \text{ (by (3.9)).}$$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

Finally we have

$$\left(\frac{m}{p}\right)_4 = \left(\frac{mB^4}{p}\right)_4$$

$$= \left(\frac{mB^2}{p}\right)_4 \left(\frac{B^2}{p}\right)_4$$

$$= \left(\frac{A^2}{p}\right)_4 \left(\frac{B^2}{p}\right)_4$$

(by (3.9))

$$= \left(\frac{A}{p}\right)\left(\frac{B}{p}\right)$$

$$= \left(\frac{2}{A}\right)\left(\frac{2}{B}\right)$$

$$= (-1)^{\frac{(A-1)}{4} - \frac{(B^2-1)}{8}}$$

(as $A \equiv 1 \pmod 4$))

$$= (-1)^{\frac{x}{2} + \frac{a_1^2-1}{8} - \frac{a_1^2}{8}(u^2-1)(v^2 \ -1)}$$

(by (3.17) and (3.18))

$$= (-1)^{\frac{x}{2} + \frac{m \ -1}{8}},$$

as required.

4. Proof of theorem 2. We just give the proof of (ii) (b) as the other cases can be proved similarly. In the case under consideration m is a prime such that

$$m \equiv 1 \pmod 8 \quad \text{and} \quad \left(\frac{2}{m}\right)_4 = -1.$$

Let p be an odd prime ($p \nmid a_1a_2$) such that

$$\left(\frac{p}{m}\right) = 1, \quad \left(\frac{p}{m}\right)_4 = \left(\frac{-1}{p}\right).$$

By the law of quadratic reciprocity we have $\left(\frac{m}{p}\right) = 1$, so there exists an integer k such that

$$k^2 \equiv m \pmod p.$$

It follows from Lehmer's criterion for quartic residuacity [**13**, p. 24] that

$$\left(\frac{2m \pm 2a_1k}{p}\right) = \left(\frac{-1}{p}\right)^{\frac{1}{4}(m-1)}\left(\frac{p}{m}\right)_4,$$

so that

$$\left(\frac{-2m \pm 2a_1k}{p}\right) = 1.$$

Hence there exist integers R and S such that

$$\begin{cases} -2m + 2a_1k \equiv R^2 \pmod{p}, \\ -2m - 2a_1k \equiv S^2 \pmod{p}. \end{cases}$$

Adding and subtracting we obtain

$$\begin{cases} -4m \equiv R^2 + S^2 \pmod{p}, \\ 4a_1k \equiv R^2 - S^2 \pmod{p}, \end{cases}$$

so that

$$\begin{aligned} (2RS)^2 &= (R^2 + S^2)^2 - (R^2 - S^2)^2 \\ &\equiv 16m^2 - 16a_1^2k \pmod{p} \\ &\equiv 16mk^2 - 16a_1^2k^2 \pmod{p} \\ &\equiv 16a_2^2k^2 \pmod{p}, \end{aligned}$$

giving

$$2RS \equiv \pm 4a_2k \pmod{p}.$$

Hence we have

$$\begin{aligned} 4(-m \pm a_2k) &= -4m \pm 4a_2k \\ &\equiv R^2 + S^2 \pm 2RS \pmod{p} \\ &\equiv (R \pm S)^2 \pmod{p} \end{aligned}$$

so that

$$\left(\frac{-m \pm a_2k}{p}\right) = 1.$$

Hence there exist integers r and s such that

$$a_2k - m \equiv r^2 \pmod{p}, \quad -a_2k - m \equiv s^2 \pmod{p},$$

and so the polynomial $x^4 + 2mx^2 + ma_1^2$ factors into four distinct linear factors (mod p), namely

$$x^4 + 2mx^2 + ma_1^2 \equiv (x - r)(x + r)(x - s)(x + s) \pmod{p}.$$

Thus, as $x^4 + 2mx^2 + ma_1^2$ is the minimal polynomial of

$$i\sqrt{m + a_2\sqrt{m}},$$

the principal ideal (p) factors as the product of four distinct conjugate prime ideals in

$$K_2 = Q(i\sqrt{m + a_2\sqrt{m}}),$$

say,

$$(p) = P\sigma(P)\sigma^2(P)\sigma^3(P),$$

where σ is the automorphism of order 4 given by

$$\sigma(i\sqrt{m + a_2\sqrt{m}}) = i\sqrt{m - a_2\sqrt{m}}.$$

As m is a prime $\equiv 9 \pmod{16}$ such that $\left(\frac{2}{m}\right)_4 = -1$, appealing to the work of Brown and Parry [**4**, Theorem 5], we see that the structure of the ideal class group $H(K_2)$ of K_2 is of the form

$$H(K_2) \simeq \mathbf{Z}_2 \times \mathbf{Z}_2 \times G,$$

where $\mathbf{Z}_a$ denotes the cyclic group of order a and where the group G has odd order. Moreover the 2-part of $H(K_2)$ is generated by the ideal classes containing the ideals P_1 and $P_2 = \sigma(P_1)$ of K_2, where the prime ideals P_1 and P_2 are given by

$$(2, \frac{1}{2}(1 + \sqrt{m})) = P_1^2, \quad (2, \frac{1}{2}(1 - \sqrt{m})) = P_2^2, \quad P_1^2P_2^2 = (2).$$

Hence for Q equal to one of (1), P_1, P_2, P_1P_2, $QP^{h_2/4}$ is a principal ideal, say $QP^{h_2/4} = (\alpha)$, where α is an integer of K_2.

We note that

$$Q\sigma(Q)\sigma^2(Q)\sigma^3(Q) = (q),$$

where

$$q = \begin{cases} 1, \text{ if } Q = (1), \\ 2, \text{ if } Q = P_1 \text{ or } P_2, \\ 4, \text{ if } Q = P_1P_2. \end{cases}$$

Now

$$(qp^{h_2/4}) = (\alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\alpha))$$

so

$$qp^{h_2/4} = u\alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\alpha),$$

where u is a unit of the ring of integers of K_2. As both $qp^{h_2/4}$ and $\alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\alpha)$ are positive integers, we must have $u = 1$, so

$$qp^{h_2/4} = \alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^3(\alpha).$$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

Since $\alpha\sigma(\alpha)$ is an integer of K_2 we have

$$\alpha\sigma(\alpha) = \frac{1}{2}(X + Ui\sqrt{m + a_2\sqrt{m}} + Vi\sqrt{m - a_2\sqrt{m}} + W\sqrt{m}),$$

where X, U, V, W are integers such that

$$X \equiv W \pmod 2,\ U \equiv V \pmod 2,$$

see for example [**8**]. Further, as

$$\sigma^2(\alpha)\sigma^3(\alpha) = \frac{1}{2}(X - Ui\sqrt{m + a_2\sqrt{m}} - Vi\sqrt{m - a_2\sqrt{m}} + W\sqrt{m}),$$

we have

$$\begin{cases} 4qp^{h_2/4} = X^2 + mU^2 + mV^2 + mW^2, \\ 2XW = a_2V^2 - 2a_1UV - a_2U^2. \end{cases}$$

If $q = 2$ or 4, X, U, V, W are all even by Lemma (g)(h). Hence (1.2) is solvable with either $n = 1$ or 2.

If (1.2) is solvable with $n = 1$ then, as

$$a_2 \equiv 4 \pmod 8,$$

we have $p \equiv 3 \pmod 4$ by Lemma (e), so that

$$\left(\frac{m}{p}\right)_4 = \left(\frac{-1}{p}\right) = -1$$

in this case.

On the other hand if (1.2) is solvable with $n = 2$ then by Lemma (f) we have $p \equiv 1 \pmod 4$, so that

$$\left(\frac{m}{p}\right)_4 = \left(\frac{-1}{p}\right) = 1$$

in this case.

This completes the proof.

As we have already remarked, the other cases of Theorem 2 can be proved in a similar manner. The only detail which is a little different occurs in the proof of (ii) (a) when $m = 5$. In this case the method used yields a solution (x, u, v, w) of the system

$$(4.2)\qquad \begin{cases} 16p = x^2 + 5u^2 + 5v^2 + 5w^2, \\ xw = v^2 - uv - u^2, \end{cases}$$

and we must show that we can construct a solution of (1.2) with $m = 5$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

and $n = 0$ from this. If x is even, by (h) of the lemma, we have that x, u, v, w are all even. Then, by (f) of the lemma, we see that x, u, v, w are in fact all divisible by 4 and this gives the required solution. If, on the other hand, x is odd then, by (h) of the lemma, x, u, v, w are all odd. Replacing the solution (x, u, v, w) by $(-x, -u, -v, -w)$, if necessary, we can suppose that

$$x \equiv 1 \pmod 4.$$

Next replacing (x, u, v, w) by $(x, v, -u, -w)$, if necessary, we can suppose that

$$w \equiv 3 \pmod 4.$$

Then replacing (x, u, v, w) by $(x, -u, -v, w)$, if necessary, we can suppose

$$u \equiv 1 \pmod 4.$$

Then it follows from the second equation in (4.2) that

$$v \equiv 1 \pmod 4.$$

Taking the second equation in (4.2) modulo 16 gives

$$x + u + v - w \equiv 4 \pmod{16}.$$

Hence we can define integers X, U, V, W by

$$\begin{aligned} 16X &= x + 5u + 5v - 5w, \\ 16X &= -x - u - v - 3w, \\ 16V &= -x - u + 3v + w, \\ 16W &= -x + 3u - v + w, \end{aligned}$$

and (X, U, V, W) is a solution of (1.2) with $m = 5$, $n = 0$ as required.

The remainder of this section is devoted to showing that whenever $l = 1$ in Theorem 2 the system (1.1) or (1.2), as appropriate, has only the eight solutions given in (1.6). We provide the details just for the case (ii) (b) of Theorem 2.

Let (x, u, v, w) be a solution of (1.2) with $l = 1$ and $n = 1$. The case $n = 2$ can be treated similarly. Set

$$\theta = x + ui\sqrt{m + a_2\sqrt{m}} + vi\sqrt{m - a_2\sqrt{m}} + w\sqrt{m}.$$

θ is an integer of K_2 such that

$$\theta\bar{\theta} = 2p.$$

Hence we have

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

$$(\theta)(\bar{\theta}) = (2)(p)$$
$$= P_1^2P_2^2P\sigma(P)\sigma^2(P)\sigma^3(P),$$

and so

$$(\theta) = P_1P_2P\sigma(P),\ P_1P_2P\sigma^3(P),$$
$$P_1P_2\sigma(P)\sigma^2(P), \text{ or } P_1P_2\sigma^2(P)\sigma^3(P).$$

Replacing P by an appropriate conjugate, as necessary, we can suppose without loss of generality that

$$(\theta) = P_1P_2P\sigma(P).$$

Let (x_1, u_1, v_1, w_1) be another solution of (1.2) with $l = 1$ and $n = 1$ and set

$$\theta_1 = x_1 + u_1 i\sqrt{m + a_2\sqrt{m}} + v_1 i\sqrt{m - a_2\sqrt{m}} + w\sqrt{m}.$$

Again we have $\theta_1\bar{\theta}_1 = 2p$ so as above we must have

$$(\theta_1) = P_1P_2P\sigma(P),\ P_1P_2P\sigma^3(P),$$
$$P_1P_2\sigma(P)\sigma^2(P), \text{ or } P_1P_2\sigma^2(P)\sigma^3(P).$$

Thus

$$(\theta_1) = (\sigma^j(\theta)),\quad j = 0, 1, 2, 3.$$

Hence

$$\theta_1 = \epsilon\sigma^j(\theta),$$

where ϵ is a unit of the ring of integers of K_2. Appealing to a result of Hasse [**9**, p. 36] we have

$$\epsilon = \pm\epsilon_m^k,\ k = 0, \pm 1, \pm 2, \dots,$$

where $\epsilon_m(> 1)$ is the fundamental unit of $Q(\sqrt{m})$. Thus we have

$$\theta_1 = \pm\epsilon_m^k\sigma^j(\theta),$$

and so

$$2p = \theta_1\bar{\theta}_1 = 2p\epsilon_m^{2k}$$

that is $\epsilon_m^{2k} = 1$, and so $k = 0$. Hence we have

$$\theta_1 = \pm\sigma^j(\theta), j = 0, 1, 2, 3,$$

that is

$$x_1 + u_1 i\sqrt{m + a_2\sqrt{m}} + v_1 i\sqrt{m - a_2\sqrt{m}} + w_1\sqrt{m}$$
$$= \pm(x + ui\sqrt{m + a_2\sqrt{m}} + vi\sqrt{m - a_2\sqrt{m}} + w\sqrt{m})$$

or

$$\pm (x - vi \sqrt{m + a_2 \sqrt{m}} + ui \sqrt{m - a_2 \sqrt{m}} - w \sqrt{m})$$

or

$$\pm (x - ui \sqrt{m + a_2 \sqrt{m}} - vi \sqrt{m - a_2 \sqrt{m}} + w \sqrt{m})$$

or

$$\pm (x + vi \sqrt{m + a_2 \sqrt{m}} - ui \sqrt{m - a_2 \sqrt{m}} - w \sqrt{m}),$$

proving the result.

5. Calculation of h_1 and h_2. In this section we put a formula of Hasse [**9**, p. 74] in an explicit form suitable for the calculation of h_1 and h_2.

We begin by showing that the conductor f_j of K_j ($j = 1, 2$) is given by

$$(5.1) \qquad \begin{aligned} f_1 &= 8m, \\ f_2 &= \begin{cases} 4m, \text{ if } m \equiv 1 \pmod 8 \\ m, \text{ if } m \equiv 5 \pmod 8). \end{cases} \end{aligned}$$

Let

$$\zeta_f = \exp(2\pi i/f).$$

For $\left(\frac{k}{m}\right) = 1$ we have

$$(5.2) \qquad \eta\left(\frac{k}{m}\right)_4 i^{\frac{m-1}{4}} \sqrt{2m + 2a\sqrt{m}} = \sum_{x=0}^{m-1} \zeta_{\mathrm{m}}^{kx^4} - m,$$

where $\eta = \pm 1$ depends only on m, and

$$a = (-1)^{\frac{a_1+1}{2} + \frac{m-1}{4}} a_1.$$

The equation (5.2) can be derived from the work of Berndt and Evans, see [**1**, Theorem 3.11]. Thus we have

$$K_1 \subseteq Q(\zeta_{8m}),$$

$$K_2 \subseteq \begin{cases} Q(\zeta_{4m}), \text{ if } m \equiv 1 \pmod 8, \\ Q(\zeta_m), \text{ if } m \equiv 5 \pmod 8. \end{cases}$$

The automorphism σ_k of $Q(\zeta_{rm})$, where

$r = 8$, for K_1,

$r = 4$, for K_2, $m \equiv 1 \pmod 8$,

$r = 1$, for K_2, $m \equiv 5 \pmod 8$, is defined by

$$\sigma_k(\zeta_{rm}) = \zeta_{rm}^k, \quad 1 \leqq k \leqq rm, \ (k, rm) = 1.$$

We wish to determine those automorphisms σ_k which leave $K_j (j = 1, 2)$ invariant. Such automorphisms must fix $\sqrt{m}$, so that

$$\sqrt{m} = \sigma_k(\sqrt{m}) = \sigma_k\left(\sum_{x=0}^{m-1} \zeta_m^{x^2}\right) = \sum_{x=0}^{m-1} \zeta_m^{kx^2} = \left(\frac{k}{m}\right)\sqrt{m},$$

showing that we need only consider those σ_k for which $\left(\frac{k}{m}\right) = 1$. Applying σ_k to (5.2) (with $k = 1$) we obtain for K_1

$$\sigma_k(i\sqrt{m + a\sqrt{m}})$$

$$= \sigma_k\left(\frac{\eta\left(\sum_{x=0}^{m-1} \zeta_m^{x^4} - \sqrt{m}\right)}{i^{\frac{m-5}{4}}\sqrt{2}}\right)$$

$$= \frac{\eta\left(\sum_{x=0}^{m-1} \zeta_m^{kx^4} - \sqrt{m}\right)}{(\sigma_k(i))^{\frac{m-5}{4}}\sigma_k(\sqrt{2})}$$

$$= \frac{\left(\frac{k}{m}\right)_4 i^{\frac{m-1}{4}}\sqrt{2}\sqrt{m + a\sqrt{m}}}{\left(\left(\frac{-1}{k}\right)_i\right)^{\frac{m-5}{4}}\left(\frac{2}{k}\right)\sqrt{2}},$$

that is

$$(5.3) \qquad \sigma_k(i\sqrt{m + a\sqrt{m}}) = \left(\frac{k}{m}\right)_4 \left(\frac{(-1)^{\frac{m-5}{4}}2}{k}\right) i\sqrt{m + a\sqrt{m}},$$

and similarly for K_2 we have

$$(5.4) \qquad \sigma_k(i\sqrt{2m + 2a\sqrt{m}}) = \left(\frac{k}{m}\right)_4 \left(\frac{(-1)^{\frac{m-5}{4}}}{k}\right) i\sqrt{2m + 2a\sqrt{m}}.$$

Identifying the Galois group

$$G_j = \mathrm{Gal}(Q(\zeta_{rm})/Q) \quad (j = 1, 2)$$

with the multiplicative group of residues (mod rm), which are coprime to rm, and

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

$$H_j = \mathrm{Gal}(Q(\zeta_{rm})/K_j)$$

as a subgroup of G_j, we have from (5.3) and (5.4)

$$H_1 = \left\{ h \ (\mathrm{mod}\ 8m) \ \middle| \ \left(\frac{h}{m}\right) = 1, \left(\frac{h}{m}\right)_4 = \left(\frac{(-1)^{\frac{m-5}{4}}2}{h}\right)\right\}$$

and

$$H_2 = \left\{ h \ (\mathrm{mod}\ rm) \ \middle| \ \left(\frac{h}{m}\right) = 1, \left(\frac{h}{m}\right)_4 = \left(\frac{(-1)^{\frac{m-5}{4}}}{h}\right)\right\},$$

where $r = 4$ for $m \equiv 1 \pmod 8$ and $r = 1$ for $m \equiv 5 \pmod 8$. The structure of the groups G_1 and G_2 and their respective subgroups H_1 and H_2 are given by

$$G_1 = \langle 2m + 1, 4m + 1, g\rangle \simeq \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{m-1}, \qquad \text{if } m \equiv 1 \pmod 8,$$

$$H_1 = \langle 2m + 1, (4m + 1)g^2\rangle \simeq \mathbf{Z}_2 \times \mathbf{Z}_{\frac{m-1}{2}},$$

$$G_1 = \langle 6m + 1, 6m - 1, g\rangle \simeq \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{m-1}, \qquad \text{if } m \equiv 5 \pmod 8,$$

$$H_1 = \langle 6m + 1, (6m - 1)g^4\rangle \simeq \mathbf{Z}_2 \times \mathbf{Z}_{\frac{m-1}{2}},$$

where g is any element of order $m - 1$ in G_1,

$$G_2 = \langle 2m + 1, g\rangle \simeq \mathbf{Z}_2 \times \mathbf{Z}_{m-1}, \quad \text{if } m \equiv 1 \pmod 8,$$

$$H_2 = \langle (2m + 1)g^2\rangle \simeq \mathbf{Z}_{\frac{m-1}{2}},$$

$$G_2 = \langle g\rangle \simeq \mathbf{Z}_{m-1}, \quad \text{if } m \equiv 5 \pmod 8,$$

$$H_2 = \langle g^4\rangle \simeq \mathbf{Z}_{\frac{m-1}{4}},$$

where g is any element of order $m - 1$ in G_2. The characters of G_j $(j = 1, 2)$ which are trivial on the subgroup H_j form a cyclic group C_j of order 4. A generator χ_j of C_j can be taken as follows:

$$\chi_1(2m + 1) = 1, \chi_1(4m + 1) = -1, \chi_1(g) = i, \qquad \text{if } m \equiv 1 \pmod 8,$$

$$\chi_1(6m + 1) = \chi_1(6m - 1) = 1, \chi_1(g) = i, \qquad \text{if } m \equiv 5 \pmod 8,$$

$$\chi_2(2m + 1) = -1, \chi_2(g) = i, \qquad \text{if } m \equiv 1 \pmod 8,$$

$$\chi_2(g) = i, \qquad \text{if } m \equiv 5 \pmod 8.$$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

The characters χ_j and $\chi_j^3 (j = 1, 2)$ are primitive and so their conductors f_{χ_j} and $f_{\chi_j^3} (j = 1, 2)$ are given by

$$f_{\chi_1} = f_{\chi_1^3} = 8m,$$

$$f_{\chi_2} = f_{\chi_2^3} = \begin{cases} 4m, & \text{if } m \equiv 1 \pmod 8, \\ m, & \text{if } m \equiv 5 \pmod 8). \end{cases}$$

However $\chi_j^2 \quad (j = 1, 2)$ is a non-primitive character which is induced by the primitive character $\left(\dfrac{m}{n}\right)$, so its conductor $f_{\chi_j^2} = m$. Hence, by the conductor-discriminant formula (see for example [**14**, pp. 131-132]), we obtain

$$\text{discriminant of } K_1 = d(K_1) = f_{\chi}f_{\chi_1^2}f_{\chi_1^3} = 2^6 m^3,$$

$$\text{discriminant of } K_2 = d(K_2) = f_{\chi_2}f_{\chi_2^2}f_{\chi_2^3}$$

$$= \begin{cases} 2^4 m^3, & \text{if } m \equiv 1 \pmod 8, \\ m^3, & \text{if } m \equiv 5 \pmod 8, \end{cases}$$

$$\text{conductor of } K_1 = f_1 = \text{LCM}(f_{\chi_1}, f_{\chi_1^2}, f_{\chi_1^3}) = 8m,$$

$$\text{conductor of } K_2 = f_2 = \text{LCM}(f_{\chi_2}, f_{\chi_2^2}, f_{\chi_2^3})$$

$$= \begin{cases} 4m, & \text{if } m \equiv 1 \pmod 8, \\ m, & \text{if } m \equiv 5 \pmod 8). \end{cases}$$

This completes the proof of (5.1). Thus $Q(\zeta_{rm})$ is the smallest cyclotomic field containing $K_j \quad (j = 1, 2)$.

Finally a formula of Hasse [**9**, p. 74] gives

$$h_1 = \frac{h}{128m^2} \left| \sum_{\substack{x=1 \\ (x,8m)=1}}^{8m} x\chi_1(x) \right|^2,$$

and if $m \equiv 1 \pmod 8$

$$h_2 = \frac{h}{32m^2} \left| \sum_{\substack{x=1 \\ (x,4m)=1}}^{4m} x\chi_2(x) \right|^2,$$

and if $m \equiv 5 \pmod 8$, $m > 5$,

$$h_2 = \frac{h}{2m^2} \left| \sum_{x=1}^{m-1}{}' x\chi_2(x) \right|^2,$$

and if $m = 5$,

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

$$h_2 = 1,$$

where h denotes the class number of the real quadratic field $Q(\sqrt{m})$. Using these formulae a program was run to calculate h_1 and h_2 for all primes $m \equiv 1 \pmod 4$ less than 1000. The values of h_1 and h_2 are given in Table 4.

TABLE 4

m	h	h_1	l_1	h_2	l_2
5	1	2	1	1	1
13	1	2	1	1	1
17	1	4	1	4	1
29	1	26	13	1	1
37	1	50	25	1	1
41	1	20	5	4	1
53	1	18	9	1	1
61	1	82	41	1	1
73	1	16	–	40	–
89	1	64	–	8	–
97	1	20	5	52	13
101	1	26	13	5	5
109	1	26	13	17	17
113	1	32	–	16	–
137	1	52	13	36	9
149	1	26	13	9	9
157	1	122	61	5	5
173	1	58	29	5	5
181	1	26	13	25	25
193	1	148	37	20	5
197	1	50	25	5	5
229	3	222	111	51	51
233	1	128	–	40	–
241	1	100	25	68	17
257	3	480	–	96	–
269	1	82	41	13	13
277	1	50	25	17	17
281	1	208	–	40	–
293	1	106	53	9	9
313	1	452	113	20	5
317	1	82	41	13	13
337	1	80	–	256	–
349	1	530	265	5	5
353	1	160	–	80	–
373	1	218	109	5	5
389	1	130	65	41	41
397	1	290	145	13	13
401	5	580	145	1060	265
409	1	68	17	340	85
421	1	90	45	25	25
433	1	500	125	52	13
449	1	100	25	68	17

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

TABLE 4 (continued)

m	h	h_1	l_1	h_2	l_2
457	1	100	25	180	45
461	1	90	45	25	25
509	1	458	229	13	13
521	1	100	25	180	45
541	1	74	37	61	61
557	1	106	53	13	13
569	1	244	61	196	49
577	7	2912	–	448	–
593	1	160	–	80	–
601	1	1024	–	40	–
613	1	730	365	25	25
617	1	208	–	136	–
641	1	388	97	100	25
653	1	442	221	25	25
661	1	794	397	9	9
673	1	596	149	116	29
677	1	226	113	25	25
701	1	370	185	25	25
709	1	298	149	61	61
733	3	438	219	135	135
757	1	194	97	125	125
761	3	540	135	588	147
769	1	1268	317	52	13
773	1	314	157	29	29
797	1	170	85	37	37
809	1	500	125	68	17
821	1	290	145	17	17
829	1	146	73	145	145
853	1	674	337	17	17
857	1	340	85	100	25
877	1	1202	601	37	37
881	1	400	–	128	–
929	1	212	53	244	61
937	1	640	–	136	–
941	1	250	125	41	41
953	1	212	53	100	25
977	1	340	85	244	61
997	1	754	377	25	25

6. Concluding remarks. The methods of this paper can be applied to other systems similar to (1.1) and (1.2).

For example it can be shown that if p is a prime $\equiv$ 1, 7 (mod 16) then there exist integers x, u, v, w such that

$$(6.1) \qquad \begin{cases} p = x^2 + 2u^2 + 2v^2 + 2w^2, \\ 2xw = v^2 - 2uv - u^2. \end{cases}$$

Moreover for $p \equiv 1 \pmod{16}$ we have

$$(6.2) \qquad \left(\frac{2}{p}\right)_4 = (-1)^{w/2}.$$

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

The system (6.1) is contained in the work of Hasse [**10**, p. 236] ($p \equiv 1 \pmod{16}$) and Giudici, Muskat and Robinson [**7**, p. 338] ($p \equiv 1, 7 \pmod{16}$). The result (6.2) is due to Berndt and Evans [**2**, p. 385]. It follows from the work of Muskat and Zee [**15**] that (6.1) has exactly the eight solutions (1.6).

Also, if p is a prime $\equiv 1 \pmod 5$, Dickson [**5**, p. 402] has shown that there are integers x_1, u_1, v_1, w_1 such that

$$(6.3) \quad \begin{cases} 16p = x_1^2 + 50u_1^2 + 50v_1^2 + 125w_1^2, \\ x_1w_1 = v_1^2 - 4u_1v_1 - u_1^2, \end{cases}$$

and that all solutions are given as in (1.6). If in addition $p \equiv 1 \pmod 4$, so that $p \equiv 1 \pmod{20}$, the methods of this paper yield another proof of the theorem of Hudson-Williams [**11**, Theorem 3], namely,

$$(6.4) \quad \left(\frac{5}{p}\right)_4 = \begin{cases} (-1)^{\frac{x_1}{4}+1} & \text{, if } x_1 \equiv 0 \pmod 2, \\ (-1)^{\frac{x_1^2w_1^2+7}{8}} & \text{, if } x_1 \equiv 1 \pmod 2. \end{cases}$$

It is appropriate at this point to show how a solution (x, u, v, w) of (1.2) with $m = 5$, $n = 0$, $l = 1$, that is, of

$$(6.5) \quad \begin{cases} p = x^2 + 5u^2 + 5v^2 + 5w^2, \\ xw = v^2 - uv - u^2, \end{cases}$$

can be constructed from a solution (x_1, u_1, v_1, w_1) of (6.3), and vice-versa.

(i) Let (x, u, v, w) be a solution of (6.5). As

$$x^2 \equiv p \equiv 1 \pmod 5$$

we have $x \equiv \pm 1 \pmod 5$. We consider two cases according as $w \equiv 0 \pmod 5$ or $w \not\equiv 0 \pmod 5$.

(a). $w \equiv 0 \pmod 5$. We have

$$(v - 3u)^2 \equiv v^2 - uv - u^2 \equiv xw \equiv 0 \pmod 5,$$

so

$$v - 3u \equiv 0 \pmod 5,\ u + 3v \equiv 0 \pmod 5.$$

Hence we can define integers x_1, u_1, v_1, w_1, by

$$(6.6) \quad \begin{cases} x_1 = 4x, \\ u_1 = \dfrac{2}{5}(u + 3v), \\ v_1 = \dfrac{2}{5}(v - 3u), \\ w_1 = -\dfrac{4}{5}w. \end{cases}$$

It is easy to check that (x_1, u_1, v_1, w_1) is a solution of (6.3). Note that $x_1 \equiv 0 \pmod 2$ in this case.

(b). $w \not\equiv 0 \pmod 5$. We have

$$(v - 3u)^2 \equiv v^2 - uv - u^2 \equiv xw \not\equiv 0 \pmod 5,$$

so

$$(v - 3u)^2 \equiv \pm 1 \pmod 5,$$

giving

$$w \equiv \pm 1 \pmod 5.$$

Then we have

$$\begin{aligned}
&(-x - 3u + v + w)(-x - u - 3v - w) \\
&\qquad\qquad \times (-x + 3u - v + w)(-x + u + 3v - w) \\
&= ((-x + w)^2 - (3u - v)^2)((-x - w)^2 - (u + 3v)^2) \\
&= (x^2 - 2xw + w^2 - 9u^2 + 6uv - v^2) \\
&\qquad\qquad \times (x^2 + 2xw + w^2 - u^2 - 6uv - 9v^2) \\
&\equiv (2 + 2xw)(2 - 2xw) \pmod 5 \\
&\equiv 4 - 4x^2w^2 \pmod 5 \\
&\equiv 0 \pmod 5,
\end{aligned}$$

so that at least one of

$$-x - 3u + v + w, \ -x - u - 3v - w, \ -x + 3u - v + w, \ -x + u + 3v - w$$

is divisible by 5. Replacing the solution (x, u, v, w) by $(x, v, -u, -w)$, $(x, -u, -v, w)$, or $(x, -v, u, -w)$ as necessary, we may assume without loss of generality that

$$-x - 3u + v + w \equiv 0 \pmod 5.$$

Then we have

$$\begin{aligned}
(-2x + 2u + v)^2 &= 4x^2 + 4u^2 + v^2 - 8xu - 4xv + 4uv \\
&\equiv -x^2 - u^2 + v^2 + 2xu + xv - uv \pmod 5 \\
&\equiv -x^2 - 3xu + xv + xw \pmod 5 \\
&\equiv x(-x - 3u + v + w) \pmod 5 \\
&\equiv 0 \pmod 5,
\end{aligned}$$

so

$$-2x + 2u + v \equiv 0 \pmod 5,$$

giving

$$2x - 2u + 4v \equiv 0 \pmod 5)$$

and

$$x - u - 3v \equiv 0 \pmod 5.$$

Thus we can define integers x_1, u_1, v_1, w_1 by

$$(6.7) \quad \begin{cases} x_1 = x - 5u - 5v - 5w, \\ 5u_1 = x - u - 3v + 5w, \\ 5v_1 = 2x - 2u + 4v, \\ 5w_1 = -x - 3u + v + w, \end{cases}$$

and (x_1, u_1, v_1, w_1) is a solution of (6.3). Note that

$$x_1 \equiv 1 \pmod 2)$$

by the lemma.

(ii) Let (x_1, u_1, v_1, w_1) be a solution of (6.3).

(a). $x_1 \equiv 0 \pmod 2$. Taking the first equation in (6.3) modulo 2 we see that

$$w_1 \equiv 0 \pmod 2.$$

Then taking the first equation modulo 4 we obtain

$$u_1 \equiv v_1 \pmod 2.$$

If $u_1 \equiv v_1 \equiv 1 \pmod 2$ the second equation gives

$$x_1 w_1 \equiv 4 \pmod 8)$$

so $x_1 \equiv w_1 \equiv 2 \pmod 4$. Then

$$\begin{aligned} 16p &= x_1^2 + 50u_1^2 + 50v_1^2 + 125w_1^2 \\ &\equiv 4 + 2 + 2 + 4 \pmod{16} \\ &\equiv 12 \pmod{16}, \end{aligned}$$

which is impossible. Hence we must have

$$u_1 \equiv v_1 \equiv 0 \pmod 2.$$

Setting

$$x_1 = 2x_2,\ u_1 = 2u_2,\ v_1 = 2v_2,\ w_1 = 2w_2,$$

we see that (x_2, u_2, v_2, w_2) is a solution of

$$\begin{cases} 4p = x_2^2 + 50u_2^2 + 50v_2^2 + 125w_2^2, \\ x_2 w_2 = v_2^2 - 4u_2 v_2 - u_2^2. \end{cases}$$

Taking the first equation modulo 2 we obtain

$$x_2 \equiv w_2 \pmod{2}.$$

If $x_2 \equiv w_2 \equiv 1 \pmod{2}$ the first equation gives

$$u_2^2 + v_2^2 \equiv 3 \pmod{4},$$

which is impossible. Hence we must have

$$x_2 \equiv w_2 \equiv 0 \pmod{2}.$$

Then the second equation gives

$$u_2 \equiv v_2 \pmod{2}.$$

We set

$$2x = x_2,\ 2u = -3u_2 - v_2,\ 2v = u_2 - 3v_2,\ 2w = 5w_2,$$

so that (x, u, v, w) is a solution of (6.5).

(b). $x_1 \not\equiv 0 \pmod{2}$. From the first equation in (6.3) we see that w_1 is odd, and then from the second equation that u_1 and v_1 are of opposite parity. Replacing the solution (x_1, u_1, v_1, w_1) by $(x_1, v_1, -u_1, -w_1)$, if necessary, we can suppose that u_1 is odd and v_1 is even.

We first show that

$$(6.8) \qquad w_1 \equiv \begin{cases} \pm 3(u_1 + v_1) \pmod{8}, & \text{if } p \equiv 1 \pmod{4}, \\ \pm(u_1 + v_1) \pmod{8}, & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

From (6.3) we obtain

$$16(p + 1) \equiv x_1^2 + 2u_1^2 + 2v_1^2 - 3w_1^2 \pmod{64}.$$

We consider two cases according as $v_1 \equiv 0 \pmod{4}$ or $v_1 \equiv 2 \pmod{4}$.

For $v_1 \equiv 0 \pmod{4}$ from the second equation in (6.3) taken modulo 8, we obtain

$$x_1 \equiv -w_1 \pmod{8}.$$

Thus

$$\begin{aligned} 16(p + 1) &\equiv (x_1 + w_1)^2 - 2x_1w_1 - 4w_1^2 + 2u_1^2 + 2v_1^2 \\ &\hfill \pmod{64} \\ &\equiv -2x_1w_1 - 4w_1^2 + 2u_1^2 + 2v_1^2 \pmod{64} \\ &\equiv 4u_1^2 + 8u_1v_1 - 4w_1^2 \pmod{64} \\ &\equiv 4(\,(u_1 + v_1)^2 - w_1^2) \pmod{64} \end{aligned}$$

proving (6.8) in this case.

For $v_1 \equiv 2 \pmod{4}$ from the second equation in (6.3) taken modulo 8, we obtain

$$x_1 \equiv 3w_1 \pmod{8}.$$

Thus

$$\begin{aligned} 16(p + 1) &\equiv (x_1 - 3w_1)^2 + 6x_1w_1 - 12w_1^2 + 2u_1^2 + 2v_1^2 \\ &\hfill \pmod{64} \\ &\equiv 6x_1w_1 - 4w_1^2 - 8 + 2u_1^2 + 2v_1^2 \pmod{64} \\ &\equiv 8v_1^2 - 24u_1v_1 - 4u_1^2 - 4w_1^2 - 8 \pmod{64} \\ &\equiv 4(2v_1^2 - 6u_1v_1 - u_1^2 - w_1^2 - 2) \pmod{64} \\ &\equiv 4(v_1^2 + 4 + 2u_1v_1 + u_1^2 - 2 - w_1^2 - 2) \\ &\hfill \pmod{64} \\ &\equiv 4(\,(u_1 + v_1)^2 - w_1^2) \pmod{64} \end{aligned}$$

proving (6.8) in this case.

Next we have

$$\begin{aligned} &(x_1 + 10u_1 + 20v_1 - 25w_1)(x_1 - 10u_1 - 20v_1 - 25w_1) \\ &\equiv (x_1 - 25w_1)^2 - (10u_1 + 20v_1)^2 \pmod{64} \\ &\equiv x_1^2 + 14x_1w_1 - 15w_1^2 + 28u_1^2 - 16u_1v_1 \pmod{64} \\ &\equiv 16p + 16 + 12u_1^2 + 12v_1^2 - 8u_1v_1 - 12w_1^2 \pmod{64} \\ &\equiv 4(4p + 4 + 3u_1^2 + 3v_1^2 - 2u_1v_1 - 3w_1^2) \pmod{64} \\ &\equiv 4(4p + 4 + 3(u_1 + v_1)^2 - 3w_1^2) \pmod{64} \\ &\equiv 0 \pmod{64}, \end{aligned}$$

by (6.8).

Further we have

$$\begin{aligned} &(x_1 + !0u_1 + 20v_1 - 25w_1) - (x_1 - 10u_1 - 20v_1 - 25w_1) \\ &= 20\,u_1 + 40v_1 \equiv 4 \pmod{8}, \end{aligned}$$

so that exactly one of $x_1 + 10u_1 + 20v_1 - 25w_1$ and $x_1 - 10u_1 - 20v_1 - 25w_1$ is divisible by 16. Replacing the solution (x_1, u_1, v_1, w_1) by the solution $(x_1, -u_1, -v_1, w_1)$, if necessary, we may suppose that

(6.9) $$x_1 + 10u_1 + 20v_1 - 25w_1 \equiv 0 \pmod{16}.$$

Then we have

$$\begin{aligned} &(x_1 + 10u_1 + 20v_1 - 25w_1) + (-x_1 - 2u_1 - 4v_1 - 15w_1) \\ &= 8u_1 + 16v_1 - 40w_1 \\ &\equiv 0 \pmod{16}, \end{aligned}$$

so that

(6.10) $$-x_1 - 2u_1 - 4v_1 - 15w_1 \equiv 0 \pmod{16}.$$

From (6.9) we have

$$(6.11) \quad x_1 + 2u_1 - w_1 \equiv 0 \pmod 8.$$

As

$$\begin{cases} x_1 \equiv -w_1 \pmod 8, & \text{if } v_1 \equiv 0 \pmod 4, \\ x_1 \equiv 3w_1 \pmod 8, & \text{if } v_1 \equiv 2 \pmod 4, \end{cases}$$

the congruence (6.11) becomes

$$(6.12) \quad u_1 + v_1 \equiv w_1 \pmod 4.$$

Then we have

$$\begin{aligned} &(x_1 + 10u_1 + 20v_1 - 25w_1) + (-x_1 - 6u_1 + 8v_1 + 5w_1) \\ &= 4u_1 + 28v_1 - 20w_1 \\ &\equiv 4(u_1 + v_1 - w_1) \pmod{16} \\ &\equiv 0 \pmod{16}, \end{aligned}$$

so that

$$(6.13) \quad -x_1 - 6u_1 + 8v_1 + 5w_1 \equiv 0 \pmod{16}.$$

Hence by (6.9), (6.10) and (6.13) we can define integers x, u, v, w by

$$(6.14) \quad \begin{cases} 16x = x_1 + 10u_1 + 20v_1 - 25w_1, \\ 16u = -x_1 - 2u_1 - 4v_1 - 15w_1, \\ 16v = -x_1 - 6u_1 + 8v_1 + 5w_1, \\ 16w = -x_1 + 10u_1 + 5w_1. \end{cases}$$

It is easy to check that (x, u, v, w) is a solution of (6.5).

Finally we deduce (6.4) from our result

$$\left(\frac{5}{p}\right)_4 = (-1)^{x+1}, \quad p \equiv 1 \pmod{20},$$

given in Theorem 3(c), by using the correspondence given above between the solutions of (x, u, v, w) of (6.5) and (x_1, u_1, v_1, w_1) of (6.3).

If $w \equiv 0 \pmod 5$ then by (6.6) $x_1 = 4x$ so

$$\left(\frac{5}{p}\right)_4 = (-1)^{x+1} = (-1)^{\frac{x_1}{4}+1} \quad (x_1 \text{ even})$$

as required.

If $w \not\equiv 0 \pmod 5$ we consider two cases according as x is even or odd.

If x is even, by the lemma and (6.7), we have

$$x_1 \equiv w_1 \equiv 1 \pmod 2, \quad x_1 + 5w_1 \equiv 4 \pmod 8,$$

so that

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press

$$x_1 \equiv -w_1 \pmod{8}.$$

If x is odd, by the lemma and (6.7), we have

$$x_1 \equiv w_1 \equiv 1 \pmod{2}, \quad x_1 + 5w_1 \equiv 0 \pmod{8},$$

so that

$$x_1 \equiv 3w_1 \pmod{8}.$$

Thus we have

$$\left(\frac{5}{p}\right)_4 = (-1)^{x+1} = (-1)^{\frac{x_1^2w_1^2-1}{8}+1}$$
$$= (-1)^{\frac{x_1^2w_1^2+7}{8}} \quad (x_1 \text{ odd})$$

as required. This completes the proof.

References

1. B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi and Jacobsthal*, J. Number Theory *11* (1979), 349-398.
2. ——— *Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer*, Illinois J. Math. *23* (1979), 374-437.
3. E. Brown and C. J. Parry, *The 2-class group of certain biquadratic number fields*, J. reine und angewandte Math. *295* (1977), 61-71.
4. ——— *The 2-class group of biquadratic fields, II*, Pacific J. Math. *78* (1978), 11-26.
5. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. *57* (1935), 391-424.
6. H. Edgar and B. Peterson, *Some contributions to the theory of cyclic quartic extensions of the rationals*, J. Number Theory *12* (1980), 77-83.
7. R. E. Giudici, J. B. Muskat and S. F. Robinson, *On the evaluation of Brewer's character sums*, Trans. Amer. Math. Soc. *171* (1972), 317-347.
8. M.-N. Gras, *Z-bases d'entiers* 1, Θ, Θ^2, Θ^3 *dans les extensions cycliques de degré* 4 *de Q*, Publications Mathématiques de la Faculté des Sciences de Besançon, Années 1979-1980 et 1980-1981, Theorie des Nombres, 14 pp.
9. H. Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, Abh. Deutsch. Akad. Wiss. Berlin, Math. *2* (1948), 1-95.
10. ——— *Der* 2^n*-te Potenzcharakter von* 2 *im Körper der* 2^n*-ten Einheitswurzeln*, Rend. Circ. Mat. Palermo *7* (1958), 185-244.
11. R. H. Hudson and K. S. Williams, *Some new residuacity criteria*, Pacific J. Math. *91* (1980), 135-143.
12. ——— *Extension of a theorem of Cauchy and Jacobi*, to appear in Journal of Number Theory.
13. E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika *5* (1958), 20-29.
14. R. L. Long, *Algebraic number theory* (Marcel Dekker, Inc., New York, 1977).
15. J. B. Muskat and Y.-C. Zee, *On the uniqueness of certain diophantine equations*, Proc. Amer. Math. Soc. *49* (1975), 13-19.
16. Y.-C. Zee, *The Jacobi sums of orders thirteen and sixty and related quadratic decompositions*, Math. Z. *115* (1970), 259-272.

Carleton University,
Ottawa, Ontario

https://doi.org/10.4153/CJM-1985-021-1 Published online by Cambridge University Press