ACTA ARITHMETICA
LXX.3 (1995)

Predictive criteria for the representation of primes by binary quadratic forms

by

Joseph B. Muskat (Ramat-Gan), Blair K. Spearman (Kelowna, B.C.) and Kenneth S. Williams (Ottawa, Ont.)

1. Introduction. Suppose that p is a prime which can be represented by primitive integral binary quadratic forms of distinct nonsquare discriminants d and d^*. Let G denote the genus of forms of discriminant d to which the forms representing p belong. Assume that the parameters in a representation of p by a binary quadratic form of discriminant d^* are known. A criterion which partitions G into subsets and uses the parameters in the above representation to predict which subset contains the form(s) representing p is called a *predictive criterion.*

For example, if p is a prime for which the Legendre symbols $(2/p)$ and $(p/31)$ both have the value 1, then p is represented by positive-definite binary quadratic forms of discriminants -124 and -248. In the case of discriminant -124, p is represented either by the form x^2+31y^2 or by the forms $5x^2\pm 4xy+7y^2$. As $25(5x^2\pm 4xy+7y^2)=(x\mp 12y)^2+31(2x\pm y)^2$, there are integers H $(=1$ or $5)$, M and N such that $H^2p=M^2+31N^2$. The (principal) genus of forms of discriminant -248 representing p consists of the four forms x^2+62y^2, $2x^2+31y^2$, $7x^2\pm 2xy+9y^2$. Given M and N we can predict whether p is represented by one of x^2+62y^2, $2x^2+31y^2$ or by $7x^2\pm 2xy+9y^2$, as follows:

$$\begin{cases} M+N\equiv \pm 1 \pmod 8 \Rightarrow p \text{ is represented by } x^2+62y^2 \text{ or } 2x^2+31y^2,\\ M+N\equiv \pm 3 \pmod 8 \Rightarrow p \text{ is represented by } 7x^2\pm 2xy+9y^2; \end{cases}$$

see [15, p. 276].

The primary purpose of this paper is to show that an elementary technique of Dirichlet [9] yields predictive criteria for positive-definite binary quadratic forms of discriminant $-D$ $(D>0)$ when the Sylow 2-subgroup

Research of the third author supported by Natural Sciences and Engineering Research Council of Canada Grant A-7233.

$H_2(-D)$ of the form class group $H(-D)$ is cyclic of order 2^k, where $k \geq 2$, for a suitable predicting discriminant $-D^*$.

In Section 2 we prove Theorem 1, which characterizes those D for which $H_2(-D)$ is isomorphic to a cyclic group of order 2^k, distinguishing the three possibilities: (a) $k = 0$, (b) $k = 1$, (c) $k \geq 2$.

In Section 3, for each of the twelve cases listed in Theorem 1(c), a suitable discriminant $-D^*$ is defined and predictive criteria are given to determine whether a prime represented by a form in the principal genus of discriminant $-D$ is in fact represented by a form which is a fourth power under composition; see Theorem 2.

In Section 4, for each of the fifty discriminants $-D$ $(D > 0)$ for which $H(-D)$ is cyclic of order 4, a specific formulation of the appropriate predictive criterion from Theorem 2 is presented.

An example in which a predictive criterion is applied successively to a sequence of discriminants is given in Section 5. We then exhibit sequences of discriminants for which the process of making successive predictions requires knowing the parameters in only one representation of p.

The applicability of Dirichlet's technique is not limited to the situation where the Sylow 2-subgroup of $H(-D)$ is cyclic of order ≥ 4. In Section 6 we present a case where the Sylow 2-subgroup has two cyclic factors each of order ≥ 4, and Dirichlet's technique produces a pair of predictive criteria which together determine which one of four cosets of the principal genus contains a form class representing the prime p.

The present research was motivated by the work of the first author in [15]. The focus of this earlier work was restricted to representability of primes by forms of discriminant $-4qr$, where q is either 1 or a prime and r is a prime. The concept of *exclusive prediction*, defined in [15, p. 266], is illustrated by each of the fifty examples in Section 4. In these examples the predictive criterion distinguishes between representability by the principal form, which is the unique fourth power in the form class group, and the other (ambiguous) form in the principal genus, which is not a fourth power. By contrast, in the example given earlier in this introduction, both the forms $x^2 + 62y^2$ and $2x^2 + 31y^2$ are fourth powers under composition. This is associated with the concept of *inclusive prediction* [15, p. 266].

Other approaches to predictive criteria can be found for example in [12]–[14].

Throughout this paper we use the following notation:

Z_m	denotes the cyclic group of order m.
$[a, b, c]$	denotes the form class containing the form $ax^2 + bxy + cy^2$.
$H(-D)$	denotes the form class group of discriminant $-D$ $(D > 0)$ under composition.

$h(-D) = |H(-D)|$ denotes the form class number of discriminant $-D$.

$H_2(-D)$ denotes the Sylow 2-subgroup of $H(-D)$.

$r_2(H(-D))$ denotes the 2-rank of $H(-D)$, that is, the number k in the decomposition $H_2(-D) \simeq Z_{2^{a_1}} \times \ldots \times Z_{2^{a_k}}$, $a_i \geq 1$.

$r_4(H(-D))$ denotes the 4-rank of $H(-D)$, that is, the number of factors $Z_{2^{a_i}}$ in this decomposition having $a_i \geq 2$.

$\left(\frac{m}{n}\right)$ (sometimes written as (m/n)) denotes the Legendre–Jacobi–Kronecker symbol as defined in [10, eqns. (5) and (7)] for arbitrary integers m, n with $n \neq 0$.

$\left(\frac{m}{p}\right)_4$ is the quartic residue symbol modulo a prime $p \equiv 1 \pmod 4$ defined for an integer m satisfying $\left(\frac{m}{p}\right) = 1$ by $\left(\frac{m}{p}\right)_4 = \left(\frac{n}{p}\right)$, where $n^2 \equiv m \pmod p$.

$v_p(a)$ is the exponent of the largest power of the prime p dividing the nonzero integer a, symbolically, $p^{v_p(a)} \parallel a$.

Finally, we recall that a discriminant d is called a *fundamental discriminant* if d/f^2 is not a discriminant for any integer $f > 1$.

2. Characterization of the class groups $H(-D)$ whose 2-part is cyclic. Let D be a positive integer $\equiv 0$ or $3 \pmod 4$. We set

$$D = 2^m p_1^{m_1} \ldots p_s^{m_s}, \tag{2.1}$$

where m is a nonnegative integer, $p_1, \ldots, p_s$ are s (≥ 0) distinct odd primes, and $m_1, \ldots, m_s$ are positive integers. As $D \equiv 0$ or $3 \pmod 4$ we have

$$\begin{cases} m = 0, & \text{in which case} \\ & m_1(p_1-1)/2 + \ldots + m_s(p_s-1)/2 \equiv 1 \pmod 2, \\ \text{or} & \\ m \geq 2. & \end{cases} \tag{2.2}$$

In this section we characterize those class groups $H(-D)$ whose 2-part is (a) trivial, (b) (cyclic) of order 2, and (c) cyclic of order ≥ 4.

THEOREM 1. (a) $H_2(-D) \simeq Z_1$ *if and only if*

(A) $D = 2^m$ $(m = 2, 3, 4)$;
(B) $D = p_1^{m_1}$ $(m_1$ (odd) ≥ 1, $p_1 \equiv 3 \pmod 4)$;
(C) $D = 4p_1^{m_1}$ $(m_1$ (odd) ≥ 1, $p_1 \equiv 3 \pmod 4)$.

(b) $H_2(-D) \simeq Z_2$ *if and only if*

(A) $D = 2^m$ $(m = 5, 6)$;
(B) $D = 4p_1^{m_1}$ $(m_1 \geq 1$, $p_1 \equiv 5 \pmod 8)$;
(C) $D = 4p_1^{m_1}$ $(m_1$ $(even)$ ≥ 2, $p_1 \equiv 3 \pmod 8)$;
(D) $D = 8p_1^{m_1}$ $(m_1 \geq 1$, $p_1 \equiv 3, 5 \pmod 8)$;
(E) $D = 16p_1^{m_1}$ $(m_1$ (odd) ≥ 1, $p_1 \equiv 3 \pmod 4)$;

(F) $D = p_1^{m_1} p_2^{m_2}$ $(m_1\ (\mathit{odd}) \geq 1,\ m_2\ (\mathit{odd}) \geq 1,\ p_1 \equiv 3 \pmod 4,$ $p_2 \equiv 1 \pmod 4,\ (p_1/p_2) = -1);$

(G) $D = p_1^{m_1} p_2^{m_2}$ $(m_1\ (\mathit{odd}) \geq 1,\ m_2\ (\mathit{even}) \geq 2,\ p_1 \equiv 3 \pmod 4,$ $(p_1/p_2) = -1);$

(H) $D = 4p_1^{m_1} p_2^{m_2}$ $(m_1\ (\mathit{odd}) \geq 1,\ m_2\ (\mathit{odd}) \geq 1,\ p_1 \equiv 3 \pmod 4,$ $p_2 \equiv 1 \pmod 4, (p_1/p_2) = -1);$

(I) $D = 4p_1^{m_1} p_2^{m_2}$ $(m_1\ (\mathit{odd}) \geq 1,\ m_2\ (\mathit{even}) \geq 2,\ m_2 \geq 1,$ $p_1 \equiv 3 \pmod 4,\ (p_1/p_2) = -1).$

(c) $H_2(-D) \simeq Z_{2^k}$, *for some* $k \geq 2$, *if and only if*

(A) $D = 2^m$ $(m \geq 7);$

(B) $D = 4p_1^{m_1}$ $(m_1 \geq 1, p_1 \equiv 1 \pmod 8));$

(C) $D = 4p_1^{m_1}$ $(m_1\ (\mathit{even}) \geq 2,\ p_1 \equiv 7 \pmod 8));$

(D) $D = 8p_1^{m_1}$ $(m_1 \geq 1, p_1 \equiv 1 \pmod 8));$

(E) $D = 8p_1^{m_1}$ $(m_1\ (\mathit{odd}) \geq 1,\ p_1 \equiv 7 \pmod 8));$

(F) $D = 8p_1^{m_1}$ $(m_1\ (\mathit{even}) \geq 2,\ p_1 \equiv 7 \pmod 8));$

(G) $D = 16p_1^{m_1}$ $(m_1 \geq 1,\ p_1 \equiv 1 \pmod 4));$

(H) $D = 16p_1^{m_1}$ $(m_1\ (\mathit{even}) \geq 2,\ p_1 \equiv 3 \pmod 4));$

(I) $D = p_1^{m_1} p_2^{m_2}$ $(m_1\ (\mathit{odd}) \geq 1,\ m_2 \geq 1,\ p_1 \equiv 3 \pmod 4,$ $p_2 \equiv 1 \pmod 4,\ (p_1/p_2) = 1);$

(J) $D = p_1^{m_1} p_2^{m_2}$ $(m_1\ (\mathit{odd}) \geq 1,\ m_2\ (\mathit{even}) \geq 2,$ $p_1 \equiv p_2 \equiv 3 \pmod 4,\ (p_1/p_2) = 1);$

(K) $D = 4p_1^{m_1} p_2^{m_2}$ $(m_1\ (\mathit{odd}) \geq 1,\ m_2 \geq 1,\ p_1 \equiv 3 \pmod 4,$ $p_2 \equiv 1 \pmod 4,\ (p_1/p_2) = 1);$

(L) $D = 4p_1^{m_1} p_2^{m_2}$ $(m_1\ (\mathit{odd}) \geq 1,\ m_2\ (\mathit{even}) \geq 2,$ $p_1 \equiv p_2 \equiv 3 \pmod 4,\ (p_1/p_2) = 1).$

In preparation for the proof of Theorem 1 we state some well-known results as Lemmas 2.1–2.3.

Lemma 2.1. *Let* $D \equiv 0, 3 \pmod 4$ *be a positive integer. Let* t *be the number of distinct odd primes dividing* D. *Then*

$$r_2(H(-D)) = \begin{cases} t-1 & \text{if } D \equiv 3 \pmod 4 \text{ or } D \equiv 12 \pmod{16}; \\ t & \text{if } D \equiv 4, 8 \pmod{16} \text{ or } D \equiv 16 \pmod{32}; \\ t+1 & \text{if } D \equiv 0 \pmod{32}. \end{cases}$$

Proof. See for example [8, Proposition 3.11]. This result has its origins in the work of Gauss [11, §§257–258]. ■

Corollary 2.1. *Let* $D \equiv 0, 3 \pmod 4$ *be a positive integer. Then*

$$(2.3)\quad r_2(H(-D)) = 0 \Leftrightarrow D = 2^m\ (m = 2, 3, 4),\ \text{or}\ D = p_1^{m_1}\ \text{or}\ 4p_1^{m_1}\ (p_1^{m_1} \equiv 3 \pmod 4));$$

$$(2.4)\quad r_2(H(-D)) = 1 \Leftrightarrow D = 2^m\ (m \geq 5),\ \text{or}$$

$$\begin{aligned}&D = 4p_1^{m_1}\ (p_1^{m_1} \equiv 1 \pmod 4,\ m_1 \ge 1),\ \textit{or}\\ &D = 8p_1^{m_1}\ \textit{or}\ 16p_1^{m_1}\ (m_1 \ge 1),\ \textit{or}\\ &D = p_1^{m_1}p_2^{m_2}\ \textit{or}\ 4p_1^{m_1}p_2^{m_2}\\ &\qquad (p_1^{m_1}p_2^{m_2} \equiv 3 \pmod 4,\ m_1 \ge 1, m_2 \ge 1).\end{aligned}$$

Proof. We have by Lemma 2.1,

$$\begin{aligned} r_2(H(-D)) = 0 \Leftrightarrow\ & (t=0) \text{ and } (D \equiv 4, 8 \pmod{16} \text{ or } D \equiv 16 \pmod{32})\\ & \text{or}\\ & (t=1) \text{ and } (D \equiv 3 \pmod 4 \text{ or } D \equiv 12 \pmod{16}),\end{aligned}$$

and

$$\begin{aligned} r_2(H(-D)) = 1 \Leftrightarrow\ & (t=0 \text{ and } D \equiv 0 \pmod{32})\\ & \text{or}\\ & (t=1) \text{ and } (D \equiv 4, 8 \pmod{16} \text{ or } D \equiv 16 \pmod{32})\\ & \text{or}\\ & (t=2) \text{ and } (D \equiv 3 \pmod 4 \text{ or } D \equiv 12 \pmod{16}),\end{aligned}$$

from which (2.3) and (2.4) follow. ■

LEMMA 2.2. *Let $-E$ $(E > 0)$ be a fundamental discriminant. Let p and q denote distinct odd primes. Then*

$$(2.5)\quad v_2(h(-E)) = 0 \Leftrightarrow E = 4, 8 \ \textit{or}\ E = p,\ p \equiv 3 \pmod 4;$$

$$\begin{aligned}(2.6)\quad v_2(h(-E)) = 1 \Leftrightarrow\ & E = 4p,\ p \equiv 5 \pmod 8,\ \textit{or}\\ & E = 8p,\ p \equiv \pm 3 \pmod 8,\ \textit{or}\\ & E = pq,\ p \equiv 1 \pmod 4, q \equiv 3 \pmod 4, \left(\frac{p}{q}\right) = -1.\end{aligned}$$

Proof. This result can be found for example in [7, Corollaries (18.4) and (19.6)], or it can be deduced from [4, p. 413 and Theorem 4(1)], [5, Theorems 1 and 2], [6, pp. 225, 226, 262]. ■

LEMMA 2.3. *Let $-E$ $(E > 0)$ be a fundamental discriminant and let f be an integer > 1, so that $D = f^2E$ is a nonfundamental discriminant. Let w denote the number of distinct odd primes which divide f but not E. If $w = 1$ we let q denote the unique odd prime factor of f which does not divide E.*

If $E = 4$ then

$$(2.7)\quad v_2(h(-D)) = 0 \qquad \textit{if}\ v_2(f) = 1,\ w = 0;$$

$$\begin{aligned}(2.8)\quad v_2(h(-D)) = 1 \qquad \textit{if}\ \ & \text{(i) } v_2(f) = 2, w = 0\ \textit{or}\\ & \text{(ii) } v_2(f) = 0,\ w = 1,\ q \equiv \pm 3 \pmod 8;\end{aligned}$$

(2.9) $v_2(h(-D)) \geq 2$ *otherwise.*

If $E \neq 4$ *then*

(2.10) $v_2(h(-D)) = 0$ *if*

(i) $v_2(h(-E)) = 0,\ v_2(f) = 0,\ w = 0$ *or*

(ii) $v_2(h(-E)) = 0,\ v_2(f) = 1,\ v_2(E) = 0,\ w = 0;$

(2.11) $v_2(h(-D)) = 1$ *if*

(i) $v_2(h(-E)) = 1,\ v_2(f) = 0,\ w = 0$ *or*

(ii) $v_2(h(-E)) = 1,\ v_2(f) = 1,\ v_2(E) = 0,\ w = 0$ *or*

(iii) $v_2(h(-E)) = 0,\ v_2(f) = 1,\ v_2(E) \geq 1,\ w = 0$ *or*

(iv) $v_2(h(-E)) = 0,\ v_2(f) = 2,\ v_2(E) = 0,\ w = 0$ *or*

(v) $v_2(h(-E)) = 0,\ v_2(f) = 0,\ w = 1,\ (E/q) = -1$ *or*

(vi) $v_2(h(-E)) = 0,\ v_2(f) = 1,\ v_2(E) = 0,\ w = 1,\ (E/q) = -1;$

(2.12) $v_2(h(-D)) \geq 2$ *otherwise.*

Proof. Gauss [11, §§254–256] proved (see for example [6, p. 217])

$$h(-D) = fh(-E)\prod_{p|f}\left(1 - \frac{(-E/p)}{p}\right)\Big/ u,$$

where p runs through the distinct primes dividing f and

$$u = \begin{cases} 3 & \text{if } E = 3,\\ 2 & \text{if } E = 4,\\ 1 & \text{if } E > 4.\end{cases}$$

As $f = \prod_{p|f} p^{v_p(f)}$ we can express $h(-D)$ in the form

$$\begin{aligned} h(-D) &= h(-E)\prod_{p|f} p^{v_p(f)-1}\prod_{p|f}(p - (-E/p))\Big/ u\\ &= h(-E)\prod_{p|f} p^{v_p(f)-1}\prod_{\substack{p|f\\ p|E}} p \prod_{\substack{p|f\\ p\nmid E}}(p - (-E/p))\Big/ u,\end{aligned}$$

that is,

$$h(-D) = h(-E)\prod_{\substack{p|f\\ p|E}} p^{v_p(f)}\prod_{\substack{p|f\\ p\nmid E}} p^{v_p(f)-1}(p - (-E/p))\Big/ u. \tag{2.13}$$

If $E = 4$ (in which case $h(-E) = 1$ and $u = 2$) we have from (2.13),

$$v_2(h(-D)) = v_2(f) + v_2(R) - 1,$$

where

$$R = \prod_{p|f,\, p\neq 2} (p - (-1/p)).$$

As

$$p - (-1/p) \equiv \begin{cases} 0 \pmod 8 & \text{if } p \equiv \pm 1 \pmod 8, \\ 4 \pmod 8 & \text{if } p \equiv \pm 3 \pmod 8, \end{cases}$$

we deduce

$$v_2(R) \begin{cases} = 0 & \text{if } w = 0 \text{ (this implies } v_2(f) \geq 1), \\ = 2 & \text{if } w = 1,\, q \equiv \pm 3 \pmod 8, \\ \geq 3 & \text{if } w = 1,\ q \equiv \pm 1 \pmod 8 \text{ or } w \geq 2. \end{cases}$$

Hence we have

$$v_2(h(-D)) \begin{cases} = v_2(f) - 1 & \text{if } w = 0, \\ = v_2(f) + 1 & \text{if } w = 1,\, q \equiv \pm 3 \pmod 8, \\ \geq v_2(f) + 2 & \text{if } w = 1,\, q \equiv \pm 1 \pmod 8 \text{ or } w \geq 2. \end{cases}$$

This completes the proof of the lemma in the case $E = 4$.

If $E \neq 4$ we have from (2.13),

$$v_2(h(-D)) = v_2(h(-E)) + (v_2(f) - \lambda) + \sum_{p|f,\, p\nmid E} v_2(p - (-E/p)),$$

where

$$\lambda = \begin{cases} 1 & \text{if } 2 \mid f,\ 2 \nmid E, \\ 0 & \text{otherwise.} \end{cases}$$

If $2 \mid f,\ 2 \nmid E$ then $v_2(2 - (-E/2)) = 0$ so that

$$\sum_{p|f,\, p\nmid E} v_2(p - (-E/p)) = \sum_{\substack{p|f,\, p\nmid E \\ p\neq 2}} v_2(p - (-E/p)).$$

For p an odd prime we have

$$p - (-E/p) \equiv \begin{cases} 0 \pmod 4 & \text{if } (E/p) = 1, \\ 2 \pmod 4 & \text{if } (E/p) = -1, \end{cases}$$

so that

$$\sum_{\substack{p|f,\, p\nmid E \\ p\neq 2}} v_2(p - (-E/p)) \begin{cases} = 0 & \text{if } w = 0, \\ = 1 & \text{if } w = 1,\ (E/q) = -1, \\ \geq 2 & \text{otherwise.} \end{cases}$$

Hence we have

$$\begin{aligned} v_2(h(-D)) = 0 \quad & \text{if } v_2(h(-E)) = v_2(f) - \lambda = w = 0, \\ v_2(h(-D)) = 1 \quad & \text{if } v_2(h(-E)) = 1,\ v_2(f) - \lambda = w = 0, \text{ or} \\ & \quad v_2(h(-E)) = 0,\ v_2(f) - \lambda = 1,\ w = 0, \text{ or} \\ & \quad v_2(h(-E)) = v_2(f) - \lambda = 0,\ w = 1,\ (E/q) = -1, \\ v_2(h(-D)) \geq 2 \quad & \text{otherwise.} \end{aligned}$$

As

$$v_2(f)-\lambda=0 \Leftrightarrow v_2(f)=0 \text{ or } v_2(f)=1,\ v_2(E)=0,$$
$$v_2(f)-\lambda=1 \Leftrightarrow v_2(f)=1,\ v_2(E)\ge 1 \text{ or } v_2(f)=2,\ v_2(E)=0,$$

we obtain the assertion of the lemma when $E\neq 4$. ■

Proof of Theorem 1. We have

$$\begin{aligned} H_2(-D)\simeq Z_1 &\Leftrightarrow r_2(H(-D))=0\\ &\Leftrightarrow D=2^m\ (m=2,3,4),\ \text{or}\\ &\qquad D=p_1^{m_1} \text{ or } 4p_1^{m_1}\ (m_1\ (\text{odd})\ge 1,\\ &\qquad\quad p_1\ (\text{prime})\equiv 3 \pmod 4),\end{aligned}$$

by Corollary 2.1, completing case (a).

In order to complete the proof we must classify all discriminants D with $r_2(H(-D))=1$ according as $H_2(-D)\simeq Z_2$ (equivalently $v_2(h(-D))=1$) or $H_2(-D)\simeq Z_{2^k}$ $(k\ge 2)$ (equivalently $v_2(h(-D))\ge 2$). We examine each of the cases in the second part of Corollary 2.1, which we refine further for convenience. Cases (b), (c) below refer to the sections of the statement of Theorem 1. An asterisk (*) indicates the first part of a case, and a double asterisk (**) indicates the second and final part of the case.

- $D=2^m$, m (even) ≥ 6:

  $E=4,\ f=2^{m/2-1}$.
  $v_2(f)=m/2-1,\ w=0$.
  $v_2(h(-D))=1$ if $m=6$, by (2.8)(i). case (b)(A)*
  $v_2(h(-D))\ge 2$ if $m\ge 8$, by (2.9). case (c)(A)*

- $D=2^m$, m (odd) ≥ 5:

  $E=8,\ f=2^{(m-3)/2}$.
  $v_2(h(-E))=0$, $v_2(f)=(m-3)/2$, $v_2(E)=3$, $w=0$.
  $v_2(h(-D))=1$ if $m=5$, by (2.11)(iii). case (b)(A)**
  $v_2(h(-D))\ge 2$ if $m\ge 7$, by (2.12). case (c)(A)**

- $D=4p_1^{m_1}$, m_1 (odd) ≥ 1, $p_1\equiv 1 \pmod 4$:

  $E=4p_1,\ f=p_1^{(m_1-1)/2}$.
  $v_2(f)=0,\ w=0$.
  $v_2(h(-E))=1$ or ≥ 2 according as $p_1\equiv 5 \pmod 8$ or $p_1\equiv 1 \pmod 8$.
  $v_2(h(-D))=1$ if $p_1\equiv 5 \pmod 8$, by (2.11)(i). case (b)(B)*
  $v_2(h(-D))\ge 2$ if $p_1\equiv 1 \pmod 8$, by (2.12). case (c)(B)*

- $D=4p_1^{m_1}$, m_1 (even) ≥ 2:

  $E=4,\ f=p_1^{m_1/2}$.
  $v_2(f)=0,\ w=1$.

$v_2(h(-D)) = 1$ if $p_1 \equiv \pm 3 \pmod 8$, by (2.8)(ii). case (b)(B)**, (C)
$v_2(h(-D)) \geq 2$ if $p_1 \equiv \pm 1 \pmod 8$, by (2.9). case (c)(B)**, (C)

- $D = 8p_1^{m_1}$, m_1 (even) ≥ 2:

$E = 8$, $f = p_1^{m_1/2}$.
$v_2(h(-E)) = 0$, $v_2(f) = 0$, $w = 1$, $q = p_1$.
$v_2(h(-D)) = 1$ if $p_1 \equiv \pm 3 \pmod 8$, by (2.11)(v). case (b)(D)*
$v_2(h(-D)) \geq 2$ if $p_1 \equiv \pm 1 \pmod 8$, by (2.12). case (c)(D)*, (F)

- $D = 8p_1^{m_1}$, m_1 (odd) ≥ 1:

$E = 8p_1$, $f = p_1^{(m_1-1)/2}$.
$v_2(f) = 0$, $w = 0$.
$v_2(h(-E)) = 1$ or ≥ 2 according as $p_1 \equiv \pm 3 \pmod 8$ or $p_1 \equiv \pm 1 \pmod 8$.
$v_2(h(-D)) = 1$ if $p_1 \equiv \pm 3 \pmod 8$, by (2.11) (i). case (b)(D)**
$v_2(h(-D)) \geq 2$ if $p_1 \equiv \pm 1 \pmod 8$, by (2.12). case (c)(D)**, (E)

- $D = 16p_1^{m_1}$, m_1 (odd) ≥ 1, $p_1 \equiv 3 \pmod 4$:

$E = p_1$, $f = 4p_1^{(m_1-1)/2}$.
$v_2(h(-E)) = 0$, $v_2(f) = 2$, $v_2(E) = 0$, $w = 0$.
$v_2(h(-D)) = 1$, by (2.11)(iv). case (b)(E)

- $D = 16p_1^{m_1}$, m_1 (even) ≥ 2:

$E = 4$, $f = 2p_1^{m_1/2}$.
$v_2(f) = 1$, $w = 1$.
$v_2(h(-D)) \geq 2$, by (2.9). case (c)(G)*, (H)

- $D = 16p_1^{m_1}$, m_1 (odd) ≥ 1, $p_1 \equiv 1 \pmod 4$:

$E = 4p_1$, $f = 2p_1^{(m_1-1)/2}$.
$v_2(h(-E)) \geq 1$, $v_2(f) = 1$, $v_2(E) = 2$, $w = 0$.
$v_2(h(-D)) \geq 2$, by (2.12). case (c)(G)**

- $D = p_1^{m_1}p_2^{m_2}$, m_1 (odd) ≥ 1, m_2 (odd) ≥ 1, $p_1 \equiv 3 \pmod 4$, $p_2 \equiv 1 \pmod 4$:

$E = p_1p_2$, $f = p_1^{(m_1-1)/2}p_2^{(m_2-1)/2}$.
$v_2(h(-E)) \left\{ \begin{array}{ll} = 1, & (p_1/p_2) = -1 \\ \geq 2, & (p_1/p_2) = 1 \end{array} \right\}$, $v_2(f) = 0$, $w = 0$.
$v_2(h(-D)) = 1$ if $(p_1/p_2) = -1$, by (2.11)(i). case (b)(F)
$v_2(h(-D)) \geq 2$ if $(p_1/p_2) = 1$, by (2.12). case (c)(I)*

- $D = p_1^{m_1}p_2^{m_2}$, m_1 (odd) ≥ 1, m_2 (even) ≥ 2, $p_1 \equiv 3 \pmod 4$:

$E = p_1$, $f = p_1^{(m_1-1)/2}p_2^{m_2/2}$.
$v_2(h(-E)) = 0$, $v_2(f) = 0$, $w = 1$, $q = p_2$.

$v_2(h(-D)) = 1$ if $(p_1/p_2) = -1$, by (2.11)(v). case (b)(G)

$v_2(h(-D)) \geq 2$ if $(p_1/p_2) = 1$, by (2.12). case (c)(I)**, (J)

- $D = 4p_1^{m_1}p_2^{m_2}$, m_1 (odd) ≥ 1, m_2 (odd) ≥ 1, $p_1 \equiv 3 \pmod 4$, $p_2 \equiv 1 \pmod 4$:

  $E = p_1p_2$, $f = 2p_1^{(m_1-1)/2}p_2^{(m_2-1)/2}$.

  $v_2(h(-E)) \left\{ \begin{matrix} = 1, & (p_1/p_2) = -1 \\ \geq 2, & (p_1/p_2) = 1 \end{matrix} \right\}$, $v_2(f) = 1$, $v_2(E) = 0$, $w = 0$.

  $v_2(h(-D)) = 1$ if $(p_1/p_2) = -1$, by (2.11)(ii). case (b)(H)

  $v_2(h(-D)) \geq 2$ if $(p_1/p_2) = 1$, by (2.12). case (c)(K)*

- $D = 4p_1^{m_1}p_2^{m_2}$, m_1 (odd) ≥ 1, m_2 (even) ≥ 2, $p_1 \equiv 3 \pmod 4$:

  $E = p_1$, $f = 2p_1^{(m_1-1)/2}p_2^{m_2/2}$.

  $v_2(h(-E)) = 0$, $v_2(f) = 1$, $v_2(E) = 0$, $w = 1$, $q = p_2$.

  $v_2(h(-D)) = 1$ if $(p_1/p_2) = -1$, by (2.11)(vi). case (b)(I)

  $v_2(h(-D)) \geq 2$ if $(p_1/p_2) = 1$, by (2.12). case (c)(K)**, (L)

■

3. Determination of predictive criteria. Throughout this section D is a positive integer $\equiv 0$ or $3 \pmod 4$ such that $H_2(-D) \simeq Z_{2^k}$ for some integer $k \geq 2$. Thus D is one of the twelve types (A), (B), ..., (L) specified in Theorem 1(c). For the discriminant $-D$ there are two generic characters χ_1 and χ_2 as specified below:

$$\begin{array}{lll} \chi_1(r) = (-1/r), & \chi_2(r) = (2/r), & \text{case (A)}, \\ \chi_1(r) = (-1/r), & \chi_2(r) = (r/p_1), & \text{cases (B), (C), (G), (H)}, \\ \chi_1(r) = (-2/r), & \chi_2(r) = (r/p_1), & \text{cases (D), (F)}, \\ \chi_1(r) = (2/r), & \chi_2(r) = (r/p_1), & \text{case (E)}, \\ \chi_1(r) = (r/p_1), & \chi_2(r) = (r/p_2), & \text{cases (I), (J), (K), (L)}. \end{array}$$

Define the positive integer D^* as follows:

$$D^* = \begin{cases} D/2, & \text{cases (A), (E)}, \\ D/p_1, & \text{cases (B), (C), (D), (G), (H)}, \\ D/2p_1, & \text{case (F)}, \\ D/p_2, & \text{cases (I), (K)}, \\ D/p_1p_2, & \text{cases (J), (L)}. \end{cases}$$

It is easily verified that D^* is formed by dividing D by the unique squarefree integer such that $-D^*$ is a discriminant whose generic characters are all included among the generic characters for discriminant $-D$. With χ_1 and χ_2 as specified above, the generic characters for the discriminant $-D^*$ are as follows:

(A) χ_1, χ_2,

(B) χ_1 (if $m_1 = 1$),
χ_1, χ_2 (if $m_1 \geq 2$),

(C) χ_2,

(D) χ_1 (if $m_1 = 1$),
χ_1, χ_2 (if $m_1 \geq 2$),

(E) χ_2,

(F) χ_2,

(G) χ_1 (if $m_1 = 1$),
χ_1, χ_2 (if $m_1 \geq 2$),

(H) χ_1, χ_2,

(I) χ_1 (if $m_2 = 1$),
χ_1, χ_2 (if $m_2 \geq 2$),

(J) χ_2 (if $m_1 = 1$),
χ_1, χ_2 (if $m_1 \geq 2$),

(K) χ_1 (if $m_2 = 1$),
χ_1, χ_2 (if $m_2 \geq 2$),

(L) χ_2 (if $m_1 = 1$),
χ_1, χ_2 (if $m_1 \geq 2$).

Let p be an odd prime such that

$$\chi_1(p) = \chi_2(p) = 1,$$

so that p is represented by a form class C_p (and its inverse C_p^{-1}) in the principal genus of the form class group $H(-D)$. Then, by a well-known theorem of Gauss, C_p is the square of a form class in $H(-D)$, say, $C_p = S_p^2$. Let K be a positive integer coprime with $2Dp$ which is represented primitively by the form class S_p^{-1} of $H(-D)$. Then K^2p is represented primitively by the class $(S_p^{-1})^2 C_p = S_p^{-2} S_p^2 = I =$ principal class of $H(-D)$. Hence there exist integers A and B such that

$$(3.1)\qquad \begin{cases} K^2 p = \begin{cases} A^2 + (D/4)B^2 & \text{if } D \equiv 0 \pmod 4, \\ A^2 + AB + ((D+1)/4)B^2 & \text{if } D \equiv 3 \pmod 4, \end{cases} \\ K > 0,\ (A,B) = 1,\ (K, 2Dp) = 1. \end{cases}$$

Further, as the generic characters for the discriminant $-D^*$ are a subset of those for discriminant $-D$, by a similar argument, there exist integers H, M, N such that

$$(3.2)\qquad \begin{cases} H^2 p = \begin{cases} M^2 + (D^*/4)N^2 & \text{if } D^* \equiv 0 \pmod 4, \\ M^2 + MN + ((D^*+1)/4)N^2 & \text{if } D^* \equiv 3 \pmod 4, \end{cases} \\ H > 0,\ (M,N) = 1,\ (H, 2Dp) = 1. \end{cases}$$

As H (resp. K) is represented primitively by a form class of discriminant $-D^*$ (resp. $-D$) and $(H, 2D) = (K, 2D) = 1$, we have

$$(3.3)\qquad \left(\frac{-D^*}{H}\right) = \left(\frac{-D}{K}\right) = 1.$$

Our purpose is to determine a necessary and sufficient condition for the class C_p to be a fourth power in $H(-D)$ for each of the cases (A)–(L). We do this by extending the techniques employed by the first author in [15], who developed an idea of Dirichlet [9, §2]. Our results are formulated in terms of arithmetic conditions involving the integers M and N in the representation (3.2). We prove

THEOREM 2. *With the above notation the following are necessary and sufficient conditions for the form class C_p to be a fourth power in the form class group $H(-D)$, where $H_2(-D) \simeq Z_{2^k}$ for some $k \geq 2$.*

- Case (A):

$$m = 7 \quad \left(\frac{2}{M+4N}\right) = 1,$$

$$m \geq 8 \quad \left(\frac{2}{M}\right) = 1.$$

- Case (B):

$$m_1 = 1 \quad \left(\frac{M+wN}{p_1}\right) = 1, \ \textit{where } w^2 \equiv -1 \pmod{p_1},$$

$$m_1 \geq 2 \quad \left(\frac{M}{p_1}\right) = 1.$$

- Case (C):

$$(-1)^{(M-1+N)/2}\left(\frac{M}{p_1}\right) = 1.$$

- Case (D):

$$m_1 = 1 \quad \left(\frac{M+wN}{p_1}\right) = 1, \ \textit{where } w^2 \equiv -2 \pmod{p_1},$$

$$m_1 \geq 2 \quad \left(\frac{M}{p_1}\right) = 1.$$

- Case (E):

$$(-1)^{N(p_1+1)/8}\left(\frac{2}{M+N}\right) = 1.$$

- Case (F):

$$(-1)^{N(p_1+1)/8}\left(\frac{-2}{M+N}\right)\left(\frac{M}{p_1}\right) = 1.$$

- Case (G):

$$m_1 = 1 \quad \left(\frac{M+wN}{p_1}\right) = 1, \ \textit{where } w^2 \equiv -4 \pmod{p_1},$$

$$m_1 \geq 2 \quad \left(\frac{M}{p_1}\right) = 1.$$

- Case (H):

$$\left(\frac{-1}{M+2N}\right)\left(\frac{M}{p_1}\right)=1.$$

- Case (I):

$$m_2=1 \quad \left(\frac{M+wN}{p_2}\right)=1,\ \textit{where } w^2-w+\tfrac{1}{4}(1+p_1^{m_1})\equiv 0 \pmod{p_2},$$

$$m_2\ge 2 \quad \left(\frac{4M+2N}{p_2}\right)=1.$$

- Case (J):

$$m_1=1 \quad \left(\frac{M+wN}{p_1}\right)\left(\frac{4M+2N}{p_2}\right)=1,$$

$$\textit{where } w^2-w+\tfrac{1}{4}(1+p_2^{m_2-1})\equiv 0 \pmod{p_1},$$

$$m_1\ge 3 \quad \left(\frac{4M+2N}{p_1p_2}\right)=1.$$

- Case (K):

$$m_2=1 \quad \left(\frac{M+wN}{p_2}\right)=1,\ \textit{where } w^2\equiv -p_1^{m_1} \pmod{p_2},$$

$$m_2\ge 2 \quad \left(\frac{M}{p_2}\right)=1.$$

- Case (L):

$$m_1=1 \quad \left(\frac{M+wN}{p_1}\right)\left(\frac{M}{p_2}\right)=1,\ \textit{where } w^2\equiv -p_2^{m_2-1} \pmod{p_1},$$

$$m_1\ge 3 \quad \left(\frac{M}{p_1p_2}\right)=1.$$

Before proving Theorem 2 we state and prove some lemmas.

LEMMA 3.1. *If x, y, z, m are integers with $m\ne 0$ such that*

$$x^2\equiv y^2+z^2 \pmod{m}$$

then

$$2(x+y)(x+z)\equiv (x+y+z)^2 \pmod{m}.$$

Proof. We have

$$\begin{aligned}2(x+y)(x+z)&=2x^2+2xy+2yz+2zx\\&=2x^2+(x+y+z)^2-(x^2+y^2+z^2)\\&=(x^2-y^2-z^2)+(x+y+z)^2\\&\equiv (x+y+z)^2 \pmod{m}. \ \blacksquare\end{aligned}$$

Not all parts of the next lemma will be used, but they are given for completeness.

Lemma 3.2. *Let X, Y be nonzero integers and m an integer $\equiv 2 \pmod 4$, $3 \pmod 4$ or $5 \pmod 8$. Suppose that $2^a \,\|\, X^2 - mY^2$, $a \ge 1$.*

(i) *If $m \equiv 2 \pmod 4$ then*

$$\begin{cases} 2^{a/2} \,\|\, X,\ 2^{a/2} \mid Y & \text{if } a \text{ is even},\\ 2^{(a+1)/2} \mid X,\ 2^{(a-1)/2} \,\|\, Y & \text{if } a \text{ is odd}.\end{cases}$$

(ii) *If $m \equiv 3 \pmod 4$ then*

$$\begin{cases} 2^{a/2} \,\|\, X,\ 2^{a/2+1} \mid Y \quad \text{or} \quad 2^{a/2+1} \mid X,\ 2^{a/2} \,\|\, Y & \text{if } a \text{ is even},\\ 2^{(a-1)/2} \,\|\, X,\ 2^{(a-1)/2} \,\|\, Y & \text{if } a \text{ is odd}.\end{cases}$$

(iii) *If $m \equiv 5 \pmod 8$ then a is even, and*

$$2^{a/2-1} \,\|\, X,\ 2^{a/2-1} \,\|\, Y,$$

or

$$2^{a/2} \,\|\, X,\ 2^{a/2+1} \mid Y,$$

or

$$2^{a/2+1} \mid X,\ 2^{a/2} \,\|\, Y.$$

Proof. (i) As the exponents of 2 in X^2 and mY^2 are even and odd, respectively, we must have

$$\begin{aligned} &2^a \,\|\, X^2,\ 2^{a+1} \mid mY^2 && \text{if } a \text{ is even},\\ &2^{a+1} \mid X^2,\ 2^a \,\|\, mY^2 && \text{if } a \text{ is odd}.\end{aligned}$$

(ii) If $v_2(X) = v_2(Y)$ then as $-m \equiv 1 \pmod 4$, we have $2^{2v_2(X)+1} \,\|\, X^2 - mY^2$, so that $a = 2v_2(X) + 1$. If $v_2(X) < v_2(Y)$ then $a = 2v_2(X)$. If $v_2(X) > v_2(Y)$ then $a = 2v_2(Y)$.

(iii) If $v_2(X) = v_2(Y)$ then, as $X^2 \equiv Y^2 \equiv 2^{2v_2(X)} \pmod{2^{2v_2(X)+3}}$, we have $X^2 - mY^2 \equiv 2^{2v_2(X)+2} \pmod{2^{2v_2(X)+3}}$, so that $a = 2v_2(X) + 2$. If $v_2(X) < v_2(Y)$ then $a = 2v_2(X)$. If $v_2(X) > v_2(Y)$ then $a = 2v_2(Y)$. ■

Part of the next lemma is used in the proof of Lemma 3.5 below.

Lemma 3.3. *Let m, X, Y be nonzero integers. Suppose that q is an odd prime such that*

$$q^a \,\|\, X^2 - mY^2, \qquad a \ge 0, \ \left(\frac{m}{q}\right) = -1.$$

Then a is even and

$$\begin{aligned} &q^{a/2} \,\|\, X,\ q^{a/2} \,\|\, Y && \text{if } v_q(X) = v_q(Y),\\ &q^{a/2} \,\|\, X,\ q^{a/2+1} \mid Y && \text{if } v_q(X) < v_q(Y),\\ &q^{a/2+1} \mid X,\ q^{a/2} \,\|\, Y && \text{if } v_q(X) > v_q(Y).\end{aligned}$$

Proof. If $v_q(X) = v_q(Y) = k$ (say), then $X = q^k X_1$, $Y = q^k Y_1$, where $q \nmid X_1 Y_1$. Thus $q^{a-2k} \parallel X_1^2 - mY_1^2$. If $a > 2k$ then $(X_1 Y_1^{-1})^2 \equiv m \pmod{q}$, contradicting $(m/q) = -1$. Thus $a = 2k$. If $v_q(X) < v_q(Y)$ then $a = 2v_q(X)$. If $v_q(X) > v_q(Y)$ then $a = 2v_q(Y)$. ■

Lemma 3.4. *Let q be an odd prime, a a positive integer, and m, X, Y nonzero integers satisfying*

$$q^a \parallel X^2 - mqY^2, \qquad q \nmid m.$$

Then

$$\begin{cases} q^{a/2} \parallel X,\ q^{a/2} \mid Y & \text{if } a \text{ is even}, \\ q^{(a+1)/2} \mid X,\ q^{(a-1)/2} \parallel Y & \text{if } a \text{ is odd}. \end{cases}$$

Proof. As the exponents of q in X^2 and qY^2 are even and odd, respectively, we must have

$$\begin{aligned} &q^a \parallel X^2,\ q^{a+1} \mid qY^2 \quad \text{if } a \text{ is even}, \\ &q^{a+1} \mid X^2,\ q^a \parallel qY^2 \quad \text{if } a \text{ is odd}. \ ■ \end{aligned}$$

Lemma 3.5. *Suppose p is a prime and r, s, H, K, M, N, A, B are nonzero integers such that*

$$\begin{aligned} H^2 p &= M^2 + rN^2, \quad (M,N) = 1 \text{ or } 2, \\ K^2 p &= A^2 + rsB^2, \quad (A,B) = 1 \text{ or } 2. \end{aligned}$$

If q is an odd prime satisfying

$$q \nmid r, \qquad \left(\frac{s}{q}\right) = -1,$$

then

(i) *q does not divide both of $HA \pm KM$,*
(ii) *both of $v_q(HA \pm KM)$ are even.*

Proof. (i) Suppose on the contrary that q divides both $HA + KM$ and $HA - KM$. Then, as q is odd, we have $q \mid (HA, KM)$. Thus one of the following must occur:

(a) $q \mid H$, $q \mid K$,
(b) $q \mid H$, $q \mid M$,
(c) $q \mid A$, $q \mid K$,
(d) $q \mid A$, $q \mid M$.

Case (a). We have $M^2 \equiv -rN^2 \pmod{q}$, $A^2 \equiv -rsB^2 \pmod{q}$, $q \nmid M$, $q \nmid N$, $q \nmid A$, $q \nmid B$, so that

$$\left(\frac{-r}{q}\right) = 1, \quad \left(\frac{-rs}{q}\right) = 1,$$

and thus $(s/q) = 1$, contradicting $(s/q) = -1$.

Case (b). From $H^2p = M^2 + rN^2$ we have $q^2 \mid rN^2$, which is impossible as $q \nmid r$ and $(M, N) = 1$ or 2.

Case (c). From $K^2p = A^2 + rsB^2$ we have $q^2 \mid rsB^2$, which is impossible as $q \nmid r$, $q \nmid s$, $(A, B) = 1$ or 2.

Case (d). We have $H^2p \equiv rN^2 \pmod{q}$, $K^2p \equiv rsB^2 \pmod{q}$, $q \nmid N$, $q \nmid H$, $q \neq p$, $q \nmid B$, $q \nmid K$, so that

$$\left(\frac{pr}{q}\right) = 1, \quad \left(\frac{prs}{q}\right) = 1,$$

and thus $(s/q) = 1$, contradicting $(s/q) = -1$.

(ii) By (i), $v_q(HA + KM) = 0$ or $v_q(HA - KM) = 0$. If both are zero we are finished. Otherwise, without loss of generality, we may assume $v_q(HA+KM) = a > 0$, so that $v_q(HA-KM) = 0$. Thus $q^a \parallel H^2A^2 - K^2M^2$. As

$$H^2A^2 - K^2M^2 = H^2(K^2p - rsB^2) - K^2(H^2p - rN^2) = r(K^2N^2 - sH^2B^2),$$

and $q \nmid r$, we deduce $q^a \parallel K^2N^2 - sH^2B^2$. Then, by Lemma 3.3, as $(s/q) = -1$, we conclude that a is even. ∎

Lemma 3.6. *Let p be a prime and A, B, H, K, M, N, r, s nonzero integers such that*

$$H^2p = M^2 + rN^2, \qquad K^2p = A^2 + sB^2.$$

Let q be an odd prime such that

$$q \neq p, \quad q \nmid HK, \quad q \mid rs.$$

Then q does not divide both of $HA \pm KM$.

Proof. Suppose q is an odd prime such that $q \neq p$, $q \nmid HK$, $q \mid rs$, $q \mid (HA + KM, HA - KM)$. Clearly by interchanging the roles of H, M, N, r and K, A, B, s respectively, if necessary, we may suppose that $q \mid r$. Now $q \mid (HA + KM) - (HA - KM) = 2KM$ so that as $q \neq 2$, $q \nmid K$, we have $q \mid M$. Then from $H^2p = M^2 + rN^2$ we see that $q \mid H^2p$, which is impossible as $q \nmid H$ and $q \neq p$. ∎

Lemma 3.7. *Let D, D^* be positive integers with $D \equiv D^* \equiv 3 \pmod{4}$, $D^* \mid D$, and $D/D^* \equiv 5 \pmod{8}$. Suppose that B, C, H, K, L, N are nonzero integers such that H and K are odd and*

$$H^2C^2 - K^2L^2 = D^*(K^2N^2 - (D/D^*)H^2B^2), \tag{3.4}$$

$$B \equiv C \pmod{2}, \quad (B, C) = 1 \text{ or } 2, \tag{3.5}$$

$$L \equiv N \pmod{2}, \quad (L, N) = 1 \text{ or } 2. \tag{3.6}$$

Define the nonnegative integers r and s by

$$2^r \parallel HC+KL, \qquad 2^s \parallel HC-KL. \tag{3.7}$$

Then r and s are both even.

Proof. From (3.4) and (3.7) we see that $2^{r+s} \parallel K^2N^2-(D/D^*)H^2B^2$. By Lemma 3.2(iii), as $D/D^* \equiv 5 \pmod 8$, $r+s$ is even. We assume r and s are both odd and obtain a contradiction. Replacing K by $-K$, if necessary, we may suppose that $r \geq s$. We consider two cases: (i) $r>s$, (ii) $r=s$.

Case (i): $r>s$. From (3.7) we see that $2^s \parallel (HC+KL) \pm (HC-KL)$, so that $2^{s-1} \parallel HC$, $2^{s-1} \parallel KL$. But H and K are both odd, so $2^{s-1} \parallel C$, $2^{s-1} \parallel L$. If $s \geq 3$ then $2^2 \mid C$, $2^2 \mid L$ and so, by (3.5) and (3.6), we have $2 \parallel B$, $2 \parallel N$. Thus $2^4 \parallel K^2N^2-(D/D^*)H^2B^2$ and so, by (3.4), $2^4 \parallel H^2C^2-K^2L^2$, that is, $r+s=4$, contradicting $r>s \geq 3$. If $s=1$ (so that $r \geq 3$) C and L are odd so that, by (3.5) and (3.6), B and N are odd. Thus $2^2 \parallel K^2N^2-(D/D^*)H^2B^2$, and so, by (3.4), $2^2 \parallel H^2C^2-K^2L^2$, that is, $r+s=2$, a contradiction.

Case (ii): $r=s$. From (3.7) we have $2^r \parallel HC \pm KL$ so that, as K,H are both odd, $2^r \mid C$, $2^r \mid L$. If $r \geq 3$, then by (3.5) and (3.6), we see that $2 \parallel B, 2 \parallel N$. Thus $2^4 \parallel K^2N^2-(D/D^*)H^2B^2$, $2^4 \parallel H^2C^2-K^2L^2$, $r+s=4$, $r=s=2$, a contradiction. If $r=1$ then either $2^2 \mid L, 2 \parallel C$ or $2 \parallel L, 2^2 \mid C$. If $2^2 \mid L, 2 \parallel C$ holds then, by (3.6), we have $2 \parallel N$. Then $2^3 \parallel D^*K^2N^2-H^2C^2$, $2^4 \mid K^2L^2$, $2^3 \parallel (D^*K^2N^2-H^2C^2)+K^2L^2 = DH^2B^2$ (by (3.4)), so that $2^3 \parallel B^2$, which is impossible. If $2 \parallel L, 2^2 \mid C$ holds then, by (3.5), $2 \parallel B$. Then $2^3 \parallel DH^2B^2-K^2L^2$, $2^4 \mid H^2C^2$, $2^3 \parallel (DH^2B^2-K^2L^2)+H^2C^2 = D^*K^2N^2$, so that $2^3 \parallel N^2$, which is impossible. ∎

Lemma 3.8. *Let E, E^* be positive integers with $E \equiv E^* \equiv 3 \pmod 4$, $E^* \mid E$, and $E/E^* \equiv 5 \pmod 8$. Suppose that A, B, H, K, M, N are nonzero integers such that H and K are odd and*

$$H^2A^2-K^2M^2 = E^*(K^2N^2-(E/E^*)H^2B^2), \tag{3.8}$$

$$A \not\equiv B \pmod 2, \quad (A,B)=1, \tag{3.9}$$

$$M \not\equiv N \pmod 2, \quad (M,N)=1. \tag{3.10}$$

Define the nonnegative integers r and s by

$$2^r \parallel HA+KM, \qquad 2^s \parallel HA-KM. \tag{3.11}$$

Then r and s are both odd.

Proof. From (3.8) and (3.11) we see that $2^{r+s} \parallel K^2N^2-(E/E^*)H^2B^2$. By Lemma 3.2(iii), $r+s$ is even. We assume r and s are both even and obtain a contradiction. Replacing K by $-K$, if necessary, we may suppose that $r \geq s$. We consider two cases: (i) $r>s$, (ii) $r=s$.

Case (i): $r>s$. If $s=0$ then $HA-KM$ is odd and thus $HA+KM$ is odd, so that $r=0$, contradicting $r>s$. Thus $s \geq 2$. From (3.11) we see that $2^s \parallel (HA+KM) \pm (HA-KM)$, so that, as H and K are odd, $2^{s-1} \parallel A$,

$2^{s-1} \parallel M$. Thus B and N are odd and so $2^2 \parallel K^2N^2 - (E/E^*)H^2B^2$, as $E/E^* \equiv 5 \pmod 8$, that is, $2^2 \parallel H^2A^2 - K^2M^2$. But $2^{s-1} \parallel A$, $2^{s-1} \parallel M$ so $2^{2(s-1)+3} \mid H^2A^2 - K^2M^2$, giving $2(s-1)+3 \le 2$, $2s \le 1$, a contradiction.

Case (ii): $r = s$. If $r = s = 0$ then $HA \pm KM$ are odd, so either A odd, M even or A even, M odd. If A odd, M even, then B even, N odd, so $2 \parallel H^2A^2 - E^*K^2N^2$, $2^2 \mid K^2M^2 - EH^2B^2$, contradicting (3.8). If A even, M odd, then B odd, N even, so $2^2 \mid H^2A^2 - E^*K^2N^2$, $2 \parallel K^2M^2 - EH^2B^2$, contradicting (3.8). Thus $r = s$ (even) ≥ 2. We have $2^r \parallel HA+KM$, $2^r \parallel HA-KM$, so that $2^{2r} \parallel H^2A^2 - K^2M^2$. Furthermore, $2^r \mid A, 2^r \mid M$. By (3.9) and (3.10) both B and N are odd. Thus $2^2 \parallel K^2N^2 - (E/E^*)H^2B^2$, so that $2^2 \parallel H^2A^2 - K^2M^2$, contradicting $r \ge 2$. ∎

We are now ready to prove Theorem 2.

Proof of Theorem 2. We consider each of the 12 cases (A), (B), …, (L) separately.

Case (A): $D = 2^m$, $D^* = 2^{m-1}$, $m \ge 7$. Let p be an odd prime such that $(-1/p) = (2/p) = 1$, that is, $p \equiv 1 \pmod 8$. From (3.2) and (3.1) we have

$$\text{(3.A.1)} \quad H^2p = M^2 + 2^{m-3}N^2, \qquad H > 0,\ (M,N) = 1,\ (H,2p) = 1,$$

$$\text{(3.A.2)} \quad K^2p = A^2 + 2^{m-2}B^2, \qquad K > 0,\ (A,B) = 1,\ (K,2p) = 1.$$

By (3.3) we have $(-D/K) = (-2^m/K) = 1$ so that

$$\text{(3.A.3)} \qquad \left(\frac{-1}{K}\right) = \left(\frac{2}{K}\right)^m.$$

Eliminating p from (3.A.1) and (3.A.2) yields

$$\text{(3.A.4)} \qquad (HA+KM)(HA-KM) = 2^{m-3}(K^2N^2 - 2H^2B^2).$$

As H, A, K, M are odd, exactly one of $HA \pm KM$ is divisible by 2 but not by 4. We choose the sign of A so that $2 \parallel HA+KM$. Then, from (3.A.4), we see that $2^{m-4} \mid HA-KM$. We factor $(HA+KM)/2$ into primes as follows:

$$\text{(3.A.5)} \qquad (HA+KM)/2 = \varepsilon \prod_{(2/q_i)=1} q_i^{e_i} \prod_{(2/r_j)=-1} r_j^{f_j},$$

where $\varepsilon = \pm 1$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. By Lemma 3.5(ii) with $s = 2$, each f_j in (3.A.5) is even. We conclude that

$$\text{(3.A.6)} \qquad (HA+KM)/2 \equiv \pm 1 \pmod 8.$$

Next, by (3.A.4) and Lemma 3.1 (with $m = 2^5$), we have

$$\begin{cases} \frac{1}{2}(HA+KM)(KM+4KN) \equiv \left(\frac{1}{2}(HA+KM)+2KN\right)^2 \pmod 8 & \text{if } m = 7, \\ \frac{1}{2}(HA+KM)(KM) \equiv \left(\frac{1}{2}(HA+KM)\right)^2 \pmod 8 & \text{if } m \ge 8, \end{cases}$$

so that appealing to (3.A.6) we have

$$\begin{cases} K(M+4N) \equiv \pm 1 \pmod 8 & \text{if } m = 7, \\ KM \equiv \pm 1 \pmod 8 & \text{if } m \ge 8, \end{cases}$$

and thus

$$\left(\frac{2}{K}\right) = \begin{cases} \left(\dfrac{2}{M+4N}\right) & \text{if } m = 7, \\ \left(\dfrac{2}{M}\right) & \text{if } m \ge 8. \end{cases} \tag{3.A.7}$$

Finally, recalling that K is odd and represented by the form class S_p^{-1} of discriminant D, we have

$$\begin{aligned} &C_p \text{ is a fourth power in } H(-D) \\ &\quad\Leftrightarrow S_p \text{ is a square in } H(-D) \ (\text{as } H_2(-D) \simeq Z_{2^k}, k \ge 2) \\ &\quad\Leftrightarrow S_p^{-1} \text{ is a square in } H(-D) \\ &\quad\Leftrightarrow \left(\frac{-1}{K}\right) = \left(\frac{2}{K}\right) = 1 \\ &\quad\Leftrightarrow \left(\frac{2}{K}\right) = 1 \qquad\qquad (\text{by } (3.A.3)) \\ &\quad\Leftrightarrow \begin{cases} \left(\dfrac{2}{M+4N}\right) = 1 & \text{if } m = 7, \\ \left(\dfrac{2}{M}\right) = 1 & \text{if } m \ge 8 \qquad (\text{by } (3.A.7)). \end{cases} \end{aligned}$$

Case (B): $D = 4p_1^{m_1}$, $D^* = 4p_1^{m_1-1}$, $m_1 \ge 1$, $p_1 \equiv 1 \pmod 8$. Let p be an odd prime satisfying $(-1/p) = (p/p_1) = 1$, so that $p \equiv 1 \pmod 4$ and $p \ne p_1$. From (3.2) and (3.1) we have

$$H^2 p = M^2 + p_1^{m_1-1} N^2, \qquad H > 0,\ (M,N) = 1,\ (H, 2pp_1) = 1, \tag{3.B.1}$$

$$K^2 p = A^2 + p_1^{m_1} B^2, \qquad K > 0,\ (A,B) = 1,\ (K, 2pp_1) = 1. \tag{3.B.2}$$

By (3.3) we have $(-D/K) = (-4p_1^{m_1}/K) = 1$, so that by the law of quadratic reciprocity

$$\left(\frac{-1}{K}\right) = \left(\frac{p_1}{K}\right)^{m_1} = \left(\frac{K}{p_1}\right)^{m_1}. \tag{3.B.3}$$

From (3.B.1) and (3.B.2), we obtain

$$(HA + KM)(HA - KM) = p_1^{m_1-1}(K^2N^2 - p_1H^2B^2). \tag{3.B.4}$$

By Lemma 3.6, p_1 does not divide both of $HA \pm KM$. Choose the sign of A so that $p_1 \nmid HA + KM$. Define odd integers R and S by

$$R = (HA + KM)/2^r, \qquad S = (HA - KM)/2^s p_1^{\alpha}, \tag{3.B.5}$$

where $p_1^\alpha \parallel HA-KM$. Note that $p_1 \nmid RS$ and, by (3.B.4), $\alpha \ge m_1 - 1$. We factor R into primes as follows:

$$R = \varepsilon \prod_{(p_1/q_i)=1} q_i^{e_i} \prod_{(p_1/r_j)=-1} r_j^{f_j}, \tag{3.B.6}$$

where $\varepsilon = \pm 1$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. By Lemma 3.5(ii) each f_j is even. Then from (3.B.6), by the law of quadratic reciprocity, we obtain

$$\begin{aligned}\left(\frac{R}{p_1}\right) &= \left(\frac{\varepsilon}{p_1}\right) \prod_{(p_1/q_i)=1} \left(\frac{q_i}{p_1}\right)^{e_i} \prod_{(p_1/r_j)=-1} \left(\frac{r_j}{p_1}\right)^{f_j} \\ &= \prod_{(p_1/q_i)=1} \left(\frac{p_1}{q_i}\right)^{e_i} = 1.\end{aligned} \tag{3.B.7}$$

By Lemma 3.1 and (3.B.4) we have

$$\begin{cases} 2(HA+KM)(KM+wKN) & \\ \quad \equiv (HA+KM+wKN)^2 \pmod{p_1} & \text{if } m_1 = 1, \\ 2(HA+KM)KM \equiv (HA+KM)^2 \pmod{p_1} & \text{if } m_1 \ge 2, \end{cases} \tag{3.B.8}$$

where $w^2 \equiv -1 \pmod{p_1}$. From (3.B.8) we see that

$$\begin{cases} \left(\frac{2}{p_1}\right)\left(\frac{HA+KM}{p_1}\right)\left(\frac{K}{p_1}\right)\left(\frac{M+wN}{p_1}\right) = 1 & \text{if } m_1 = 1, \\ \left(\frac{2}{p_1}\right)\left(\frac{HA+KM}{p_1}\right)\left(\frac{K}{p_1}\right)\left(\frac{M}{p_1}\right) = 1 & \text{if } m_1 \ge 2. \end{cases}$$

Thus, as $(2/p_1) = 1$ and $(HA+KM/p_1) = (2^r R/p_1) = 1$ (by (3.B.5) and (3.B.7)), we obtain

$$\left(\frac{K}{p_1}\right) = \begin{cases} \left(\frac{M+wN}{p_1}\right) & \text{if } m_1 = 1, \\ \left(\frac{M}{p_1}\right) & \text{if } m_1 \ge 2. \end{cases} \tag{3.B.9}$$

Finally,

C_p is a fourth power in $H(-D)$

$\Leftrightarrow \left(\frac{-1}{K}\right) = \left(\frac{K}{p_1}\right) = 1$

$\Leftrightarrow \left(\frac{K}{p_1}\right) = 1 \quad$ (by (3.B.3))

$$\Leftrightarrow \begin{cases} \left(\dfrac{M+wN}{p_1}\right)=1 & \\ & \text{if } m_1=1, \text{ where } w^2\equiv -1 \pmod{p_1}, \\ \left(\dfrac{M}{p_1}\right)=1 & \text{if } m_1\geq 2 \end{cases} \qquad \text{(by (3.B.9))}.$$

We remark that when $m_1 = 1$ it is possible for p_1 to divide M so that the symbol (M/p_1) cannot be used for the criterion in this case. We note that the value of the Legendre symbol $(M+wN/p_1)$ is independent of the choice of solution $\pm w$ of $w^2 \equiv -1 \pmod{p_1}$, as

$$\left(\frac{M+wN}{p_1}\right)\left(\frac{M-wN}{p_1}\right)=\left(\frac{M^2-w^2N^2}{p_1}\right)=\left(\frac{M^2+N^2}{p_1}\right)$$
$$=\left(\frac{H^2p}{p_1}\right)=1.$$

Case (C): $D=4p_1^{m_1}$, $D^*=4p_1^{m_1-1}$, m_1 (even) ≥ 2, $p_1\equiv 7 \pmod 8$. Let p be an odd prime satisfying $(-1/p)=(p/p_1)=1$, so that $p\equiv 1 \pmod 4$ and $p\neq p_1$. From (3.2) and (3.1) we have

(3.C.1) $H^2p=M^2+p_1^{m_1-1}N^2,\qquad H>0,\ (M,N)=1,\ (H,2pp_1)=1,$

(3.C.2) $K^2p=A^2+p_1^{m_1}B^2,\qquad K>0,\ (A,B)=1,\ (K,2pp_1)=1.$

From (3.3) we have $(-D/K)=(-4p_1^{m_1}/K)=1$ so that

(3.C.3) $$\left(\frac{-1}{K}\right)=1,$$

and hence

(3.C.4) $$K\equiv 1 \pmod 4.$$

Reducing (3.C.1) and (3.C.2) modulo 8, we obtain

(3.C.5) $$\begin{cases} A\equiv (p-1)/2 \pmod 4,\ B\equiv 1 \pmod 2 \text{ or} \\ A\equiv 1 \pmod 2,\ B\equiv (p-1)/2 \pmod 4, \\ M\equiv 1 \pmod 2,\ N\equiv (p-1)/2 \pmod 4. \end{cases}$$

Replacing M by $-M$ if necessary, we may suppose that

(3.C.6) $$M\equiv 1 \pmod 4.$$

From (3.C.1) and (3.C.2) we obtain

(3.C.7) $$(HA+KM)(HA-KM)=p_1^{m_1-1}(K^2N^2-p_1H^2B^2).$$

By Lemma 3.6, p_1 does not divide both of $HA\pm KM$. Choose the sign of A so that $p_1 \nmid HA+KM$, and define the odd integers R and S by

(3.C.8) $$R=(HA+KM)/2^r,\qquad S=(HA-KM)/2^sp_1^{\alpha},$$

where $p_1^\alpha \parallel HA - KM$. Clearly $p_1 \nmid RS$. Note that

$$\text{(3.C.9)} \qquad \begin{cases} \alpha \geq m_1 - 1, \\ r = s = 0 & \text{if } A \text{ is even,} \\ \min(r, s) = 1 & \text{if } A \text{ is odd.} \end{cases}$$

We show that when A is odd

$$\text{(3.C.10)} \qquad \begin{cases} p \equiv 1 \pmod 8 & \text{if } r + s \geq 4, \\ p \equiv 5 \pmod 8 & \text{if } r + s = 3. \end{cases}$$

This is clear from (3.C.5) as

$$\begin{aligned} p \equiv 1 \pmod 8 &\Rightarrow B \equiv N \equiv 0 \pmod 4 \Rightarrow 2^4 \mid K^2N^2 - p_1H^2B^2 \\ &\Rightarrow 2^4 \mid (HA + KM)(HA - KM) \Rightarrow r + s \geq 4, \\ p \equiv 5 \pmod 8 &\Rightarrow B \equiv N \equiv 2 \pmod 4 \Rightarrow 2 \parallel (N/2)^2 + (B/2)^2 \\ &\Rightarrow 2 \parallel K^2(N/2)^2 - p_1H^2(B/2)^2 \Rightarrow 2^3 \parallel K^2N_2 - p_1H^2B^2 \\ &\Rightarrow 2^3 \parallel (HA + KM)(HA - KM) \Rightarrow r + s = 3. \end{aligned}$$

Next we show that

$$\text{(3.C.11)} \qquad \left(\frac{R}{p_1}\right)\left(\frac{S}{p_1}\right) = (-1)^{\alpha+1}.$$

From (3.C.7) and (3.C.8) we see that $p_1^\alpha \parallel H^2A^2 - K^2M^2 = p_1^{m_1-1}(K^2N^2 - p_1H^2B^2)$, so that $p_1^{\alpha-m_1+1} \parallel K^2N^2 - p_1H^2B^2$. Then, by Lemma 3.4, we observe that

$$\begin{cases} p_1^{(\alpha-m_1+1)/2} \parallel N,\ p_1^{(\alpha-m_1+1)/2} \mid B & \text{if } \alpha \text{ is odd,} \\ p_1^{(\alpha-m_1+2)/2} \mid N,\ p_1^{(\alpha-m_1)/2} \parallel B & \text{if } \alpha \text{ is even.} \end{cases}$$

Define integers N_1 and B_1 by

$$\begin{cases} N = p_1^{(\alpha-m_1+1)/2}N_1,\ B = p_1^{(\alpha-m_1+1)/2}B_1 & \text{if } \alpha \text{ is odd,} \\ N = p_1^{(\alpha-m_1+2)/2}N_1,\ B = p_1^{(\alpha-m_1)/2}B_1 & \text{if } \alpha \text{ is even,} \end{cases}$$

where $p_1 \nmid N_1$ (α odd) and $p_1 \nmid B$ (α even). Hence

$$\begin{aligned} 2^{r+s}RS &= (H^2A^2 - K^2M^2)/p_1^\alpha = (K^2N^2 - p_1H^2B^2)/p_1^{\alpha-m_1+1} \\ &= \begin{cases} K^2N_1^2 - p_1H^2B_1^2 & \text{if } \alpha \text{ is odd,} \\ p_1K^2N_1^2 - H^2B_1^2 & \text{if } \alpha \text{ is even,} \end{cases} \end{aligned}$$

so that, as $(2/p_1) = 1$,

$$\left(\frac{RS}{p_1}\right) = \begin{cases} \left(\dfrac{K^2N_1^2}{p_1}\right) = 1 & \text{if } \alpha \text{ is odd,} \\ \left(\dfrac{-H^2B_1^2}{p_1}\right) = -1 & \text{if } \alpha \text{ is even,} \end{cases}$$

completing the proof of (3.C.11).

Now factor R and S into primes:

$$\text{(3.C.12)} \qquad \begin{cases} R = \varepsilon \displaystyle\prod_{(p_1/q_i)=1} q_i^{e_i} \prod_{(p_1/r_j)=-1} r_j^{f_j}, \\ S = \varepsilon' \displaystyle\prod_{(p_1/q_i)=1} q_i^{g_i} \prod_{(p_1/r_j)=-1} r_j^{h_j}, \end{cases}$$

where $\varepsilon, \varepsilon' = \pm 1$, e_i, f_j, g_i, h_j are nonnegative integers, and q_i, r_j are distinct odd primes. By Lemma 3.5(ii) for each j both f_j and h_j are even. Hence, appealing to the law of quadratic reciprocity, we have

$$\begin{aligned} \left(\frac{R}{p_1}\right) &= \left(\frac{\varepsilon}{p_1}\right) \prod_{(p_1/q_i)=1} \left(\frac{q_i}{p_1}\right)^{e_i} \prod_{(p_1/r_j)=-1} \left(\frac{r_j}{p_1}\right)^{f_j} \\ &= \varepsilon \prod_{(p_1/q_i)=1} \left(\left(\frac{-1}{q_i}\right)\left(\frac{p_1}{q_i}\right)\right)^{e_i}, \end{aligned}$$

that is

$$\text{(3.C.13)} \qquad \left(\frac{R}{p_1}\right) = \varepsilon(-1)^E, \qquad \text{where } E = \sum_{\substack{(p_1/q_i)=1 \\ q_i \equiv 3 \pmod 4}} e_i.$$

Next, taking the first equation in (3.C.12) modulo 4, we have

$$R \equiv \varepsilon \prod_{\substack{(p_1/q_i)=1 \\ q_i \equiv 3 \pmod 4}} (-1)^{e_i} \equiv \varepsilon(-1)^E \pmod 4,$$

so that

$$\text{(3.C.14)} \qquad \varepsilon(-1)^E = (-1)^{(R-1)/2}.$$

Thus, from (3.C.13) and (3.C.14), we obtain

$$\text{(3.C.15)} \qquad \left(\frac{R}{p_1}\right) = (-1)^{(R-1)/2}.$$

Similarly we derive

$$\text{(3.C.16)} \qquad \left(\frac{S}{p_1}\right) = (-1)^{(S-1)/2}.$$

The next step is to show that

$$\text{(3.C.17)} \qquad \left(\frac{R}{p_1}\right) = (-1)^{N/2}.$$

We consider three cases.

Case (i): A even. We have

$$\begin{aligned} R-1 &\equiv HA+KM-1 && \text{(by (3.C.8) and (3.C.9))} \\ &\equiv A && \text{(by (3.C.1), (3.C.4) and (3.C.6))} \\ &\equiv N \pmod 4 && \text{(by (3.C.5))}, \end{aligned}$$

so that by (3.C.15) we obtain

$$\left(\frac{R}{p_1}\right) = (-1)^{(R-1)/2} = (-1)^{N/2}.$$

Case (ii): A odd, $r=1$. We have

$$\begin{aligned} R-1 &= \tfrac{1}{2}(HA+KM)-1 \\ &= KM + 2^{s-1}p_1^{\alpha}S - 1 && \text{(by (3.C.8))} \\ &\equiv 2^{s-1}p_1^{\alpha}S && \text{(by (3.C.4) and (3.C.6))} \\ &\equiv \begin{cases} 0 \equiv N \pmod 4 & \text{if } p \equiv 1 \pmod 8 \\ 2 \equiv N \pmod 4 & \text{if } p \equiv 5 \pmod 8 \end{cases} && \text{(by (3.C.10) and (3.C.5))}, \end{aligned}$$

so that by (3.C.15) we obtain

$$\left(\frac{R}{p_1}\right) = (-1)^{(R-1)/2} = (-1)^{N/2}.$$

Case (iii): A odd, $s=1$. We have

$$\begin{aligned} S = (HA-KM)/2p_1^{\alpha} &= (2^{r-1}R-KM)/p_1^{\alpha} && \text{(by (3.C.8))} \\ &\equiv (-1)^{\alpha}(2^{r-1}R-1) && \text{(by (3.C.4) and (3.C.6))} \\ &\equiv \begin{cases} (-1)^{\alpha+1} & \text{if } p \equiv 1 \pmod 8 \\ (-1)^{\alpha} & \text{if } p \equiv 5 \pmod 8 \end{cases} && \text{(by (3.C.10))} \\ &\equiv 2\alpha + (p+5)/2 \pmod 4, \end{aligned}$$

that is

$$(S-1)/2 \equiv \alpha + (p+3)/4 \pmod 2,$$

so that, by (3.C.5), (3.C.11) and (3.C.16), we obtain

$$\begin{aligned} \left(\frac{R}{p_1}\right) &= (-1)^{\alpha+1}\left(\frac{S}{p_1}\right) = (-1)^{\alpha+1+(S-1)/2} \\ &= (-1)^{\alpha+1+\alpha+(p+3)/4} = (-1)^{(p-1)/4} = (-1)^{N/2}. \end{aligned}$$

This completes the proof of (3.C.17).

Writing (3.C.7) in the form

$$(HA+KM)^2 - 2(HA+KM)KM = p_1^{m_1-1}(K^2N^2 - p_1H^2B^2),$$

and appealing to (3.C.8), we see that

$$2^{2r}R^2 - 2^{r+1}RKM \equiv 0 \pmod{p_1},$$

so that

$$\left(\frac{RKM}{p_1}\right) = \left(\frac{2^{r+1}RKM}{p_1}\right) = \left(\frac{2^r R}{p_1}\right)^2 = 1,$$

which implies by (3.C.17),

$$\text{(3.C.18)} \qquad \left(\frac{K}{p_1}\right) = \left(\frac{R}{p_1}\right)\left(\frac{M}{p_1}\right) = (-1)^{N/2}\left(\frac{M}{p_1}\right).$$

Finally,

C_p is a fourth power in $H(-D)$

$$\begin{aligned} &\Leftrightarrow \left(\frac{-1}{K}\right) = \left(\frac{K}{p_1}\right) = 1 \\ &\Leftrightarrow \left(\frac{K}{p_1}\right) = 1 \qquad\qquad \text{(by (3.C.3))} \\ &\Leftrightarrow (-1)^{N/2}\left(\frac{M}{p_1}\right) = 1 \qquad \text{(by (3.C.18)).} \end{aligned}$$

We have shown that if $M \equiv 1 \pmod 4$ then

$$\text{(3.C.19)} \qquad C_p \text{ is a fourth power in } H(-D) \Leftrightarrow (-1)^{N/2}\left(\frac{M}{p_1}\right) = 1.$$

Clearly, if $M \equiv 3 \pmod 4$, (3.C.19) becomes (as $(-M/p_1) = -(M/p_1)$)

$$\text{(3.C.20)} \qquad C_p \text{ is a fourth power in } H(-D) \Leftrightarrow -(-1)^{N/2}\left(\frac{M}{p_1}\right) = 1.$$

Putting (3.C.19) and (3.C.20) together, we obtain

C_p is a fourth power in $H(-D)$

$$\begin{aligned} &\Leftrightarrow (-1)^{(M-1+N)/2}\left(\frac{M}{p_1}\right) = 1 \\ &\Leftrightarrow (-1)^{N/2}\left(\frac{p_1}{M}\right) = 1 \end{aligned}$$

without any restriction on M.

Case (D): $D = 8p_1^{m_1}$, $D^* = 8p_1^{m_1-1}$, $m_1 \geq 1$, $p_1 \equiv 1 \pmod 8$. Let p be an odd prime such that $(-2/p) = (p/p_1) = 1$, so that $p \equiv 1, 3 \pmod 8$ and $p \neq p_1$. From (3.2) and (3.1) we have

$$\text{(3.D.1)} \quad H^2 p = M^2 + 2p_1^{m_1-1}N^2, \qquad H > 0,\ (M,N) = 1,\ (H, 2pp_1) = 1,$$

$$\text{(3.D.2)} \quad K^2 p = A^2 + 2p_1^{m_1}B^2, \qquad K > 0,\ (A,B) = 1,\ (K, 2pp_1) = 1.$$

By (3.3) we have $(-D/K) = (-8p_1^{m_1}/K) = 1$, so that, by the law of quadratic reciprocity, we have

$$\left(\frac{-2}{K}\right) = \left(\frac{K}{p_1}\right)^{m_1}. \tag{3.D.3}$$

Next, from (3.D.1) and (3.D.2), we obtain

$$(HA+KM)(HA-KM) = 2p_1^{m_1-1}(K^2N^2 - p_1H^2B^2). \tag{3.D.4}$$

The rest of the proof proceeds almost exactly as the proof of Case (B), immediately following (3.B.4), except that in the equivalent to (3.B.8) w is chosen so that $w^2 \equiv -2 \pmod{p_1}$, and at the end we use $(-2/K)$.

Case (E): $D = 8p_1^{m_1}$, $D^* = 4p_1^{m_1}$, m_1 (odd) ≥ 1, $p_1 \equiv 7 \pmod 8$. Let p be an odd prime such that $(2/p) = (p/p_1) = 1$, so that $p \equiv 1, 7 \pmod 8$ and $p \neq p_1$. From (3.2) and (3.1) we have

$$H^2p = M^2 + p_1^{m_1}N^2, \qquad H > 0,\ (M,N) = 1,\ (H, 2pp_1) = 1, \tag{3.E.1}$$

$$K^2p = A^2 + 2p_1^{m_1}B^2, \qquad K > 0,\ (A,B) = 1,\ (K, 2pp_1) = 1. \tag{3.E.2}$$

From (3.3) we have $(-D/K) = (-8p_1^{m_1}/K) = 1$ so that (appealing to the law of quadratic reciprocity)

$$\left(\frac{2}{K}\right) = \left(\frac{-p_1}{K}\right) = \left(\frac{K}{p_1}\right). \tag{3.E.3}$$

Reducing (3.E.1) and (3.E.2) modulo 8, we see that A is odd and

$$\begin{cases} B \equiv 0 \pmod 2,\ M \equiv 1 \pmod 2,\ N \equiv 0 \pmod 4 & \text{if } p \equiv 1 \pmod 8, \\ B \equiv 1 \pmod 2,\ M \equiv 0 \pmod 4,\ N \equiv 1 \pmod 2 & \text{if } p \equiv 7 \pmod 8. \end{cases} \tag{3.E.4}$$

From (3.E.1) and (3.E.2) we obtain

$$(HA+KM)(HA-KM) = p_1^{m_1}(K^2N^2 - 2H^2B^2). \tag{3.E.5}$$

If $p \equiv 1 \pmod 8$ exactly one of $HA \pm KM$ is congruent to 2 (mod 4); choose the sign of A so that $2 \parallel HA+KM$. Thus $2^\alpha \parallel HA-KM$ for some integer $\alpha \geq 2$. If $p \equiv 7 \pmod 8$ both of $HA \pm KM$ are odd.

We define the odd integers R and S by

$$\begin{cases} R = (HA+KM)/2,\ S = (HA-KM)/2^\alpha & \text{if } p \equiv 1 \pmod 8, \\ R = HA+KM,\ S = HA-KM & \text{if } p \equiv 7 \pmod 8. \end{cases} \tag{3.E.6}$$

Factor R into primes:

$$R = \varepsilon p_1^r \prod_{(2/q_i)=1} q_i^{e_i} \prod_{(2/r_j)=-1} r_j^{f_j}, \tag{3.E.7}$$

where $\varepsilon = \pm 1$, $r \geq 0$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes all different from p_1. By Lemma 3.5(ii) each f_j is even. Hence, from

(3.E.7) modulo 8, we obtain $R \equiv \pm 1 \pmod 8$ so that by (3.E.6),

$$\text{(3.E.8)} \qquad \begin{cases} HA + KM \equiv 2\delta \pmod{16} & \text{if } p \equiv 1 \pmod 8, \\ HA + KM \equiv \delta \pmod 8 & \text{if } p \equiv 7 \pmod 8, \end{cases}$$

where $\delta = \pm 1$. We show next that

$$\text{(3.E.9)} \qquad \left(\frac{2}{K}\right) = \left(\frac{2}{M+N}\right)(-1)^{N(p_1+1)/8}$$

by adapting the method used in the proof of [15, Theorem 2] but without constraining the odd integers among A, B, H, K, M and N to be congruent to $1 \pmod 4$.

We treat the case $p \equiv 1 \pmod 8$ first. By (3.E.1), (3.E.2) and (3.E.4) we may express

$$A = 4a + \varepsilon_A, \quad B = 2b, \quad H = 4h + \varepsilon_H, \quad K = 4k + \varepsilon_K,$$
$$M = 4m + \varepsilon_M, \quad N = 4n,$$

where ε_A, ε_H, ε_K, ε_M take only the values ±1. Note that

$$\varepsilon_A^2 = 1, \quad \varepsilon_A \equiv 1 \pmod 2, \quad a^2 \equiv a \pmod 2, \quad A^2 \equiv 8a + 1 \pmod{16},$$

and similarly for the others. Then, from (3.E.8) we obtain

$$\text{(3.E.10)} \quad 4(\varepsilon_H a + \varepsilon_A h + \varepsilon_M k + \varepsilon_K m) + (\varepsilon_A\varepsilon_H + \varepsilon_K\varepsilon_M) \equiv 2\delta \pmod{16}.$$

Taking (3.E.10) modulo 4, we see that

$$\text{(3.E.11)} \qquad \varepsilon_A\varepsilon_H = \varepsilon_K\varepsilon_M = \theta \quad \text{(say)}.$$

Then, taking (3.E.10) modulo 8 and dividing by 2, we obtain (as $4\varepsilon_H a \equiv 4a \pmod 8, \ldots$)

$$\delta \equiv \theta + 2(a + h + k + m) \pmod 4,$$

so that

$$\text{(3.E.12)} \qquad \delta = \theta(-1)^{a+h+k+m}.$$

Thus, from (3.E.10), (3.E.11) and (3.E.12), we have

$$\varepsilon_H a + \varepsilon_A h + \varepsilon_M k + \varepsilon_K m \equiv \theta((-1)^{a+h+k+m} - 1)/2 \pmod 4,$$

so that, as $\varepsilon_H = \theta\varepsilon_A$, $\varepsilon_A = \theta\varepsilon_H$, $\varepsilon_M = \theta\varepsilon_K$, $\varepsilon_K = \theta\varepsilon_M$, we have

$$\text{(3.E.13)} \quad \varepsilon_A a + \varepsilon_H h + \varepsilon_K k + \varepsilon_M m \equiv ((-1)^{a+h+k+m} - 1)/2 \pmod 4.$$

Next we take (3.E.5) modulo 32 and divide by 8 to obtain

$$\text{(3.E.14)} \quad 2(a+h+k+m) + (\varepsilon_A a + \varepsilon_H h - \varepsilon_K k - \varepsilon_M m) \equiv 2n + b^2 \pmod 4.$$

Taking (3.E.14) modulo 2, we deduce

$$\text{(3.E.15)} \qquad a + h + k + m \equiv b \pmod 2.$$

Then, from (3.E.13)–(3.E.15), we obtain

$$2b + 2(k + m) \equiv 2n + b^2 - ((-1)^b - 1)/2 \pmod 4.$$

But $2b \equiv b^2 - ((-1)^b - 1)/2 \pmod 4$ for any integer b so that $k + m \equiv n \pmod 2$. Thus

$$\left(\frac{2}{K}\right) = (-1)^{(K^2-1)/8} = (-1)^k = (-1)^{m+n} = \left(\frac{2}{M+N}\right),$$

which proves (3.E.9) in this case as N is even.

Now we treat the case $p \equiv 7 \pmod 8$. By (3.E.4) we may express

$$A = 4a \pm 1, \quad B = 4b \pm 1, \quad H = 4h \pm 1, \quad K = 4k \pm 1,$$
$$M = 4m, \quad N = 4n \pm 1,$$

so that $A^2 \equiv 8a + 1 \pmod{16}, \ldots$. From (3.E.8) modulo 8 we obtain

(3.E.16) $$a + h + m \equiv 0 \pmod 2.$$

Next, from (3.E.5) modulo 16, we deduce

(3.E.17) $$k + n \equiv a + h + (p_1 + 1)/8 \pmod 2.$$

Eliminating $a + h$ from (3.E.16) and (3.E.17) yields

$$k \equiv m + n + (p_1 + 1)/8 \pmod 2.$$

Thus

$$\left(\frac{2}{K}\right) = (-1)^k = (-1)^{m+n+(p_1+1)/8} = \left(\frac{2}{M+N}\right)(-1)^{(p_1+1)/8},$$

which proves (3.E.9) in this case as N is odd.

Finally,

C_p is a fourth power in $H(-D)$

$$\Leftrightarrow \left(\frac{2}{K}\right) = \left(\frac{K}{p_1}\right) = 1$$

$$\Leftrightarrow \left(\frac{2}{K}\right) = 1 \qquad \text{(by (3.E.3))}$$

$$\Leftrightarrow \left(\frac{2}{M+N}\right)(-1)^{N(p_1+1)/8} = 1 \qquad \text{(by (3.E.9))}.$$

Case (F): $D = 8p_1^{m_1}$, $D^* = 4p_1^{m_1-1}$, m_1 (even) ≥ 2, $p_1 \equiv 7 \pmod 8$. Let p be an odd prime such that $(-2/p) = (p/p_1) = 1$, so that $p \equiv 1, 3 \pmod 8$ and $p \neq p_1$. From (3.2) and (3.1) we have

(3.F.1) $$H^2 p = M^2 + p_1^{m_1-1} N^2, \qquad H > 0,\ (M, N) = 1,\ (H, 2pp_1) = 1,$$

(3.F.2) $$K^2 p = A^2 + 2p_1^{m_1} B^2, \qquad K > 0,\ (A, B) = 1,\ (K, 2pp_1) = 1.$$

From (3.3) we have $(-D/K) = (-8p_1^{m_1}/K) = 1$, that is,

(3.F.3) $$\left(\frac{-2}{K}\right) = 1, \qquad K \equiv 1, 3 \pmod 8.$$

Reducing (3.F.1) and (3.F.2) modulo 8, we obtain

$$A \equiv 1 \pmod 2, \tag{3.F.4}$$

and

$$\begin{cases} B \equiv 0 \pmod 2,\ M \equiv 1 \pmod 2,\ N \equiv 0 \pmod 4 \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } p \equiv 1 \pmod 8, \\ B \equiv 1 \pmod 2,\ M \equiv 2 \pmod 4,\ N \equiv 1 \pmod 2 \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{if } p \equiv 3 \pmod 8). \end{cases} \tag{3.F.5}$$

Replacing (M, N) by $(-M, -N)$ if necessary, we may suppose that

$$M + N \equiv 1 \pmod 4). \tag{3.F.6}$$

From (3.F.1) and (3.F.2) we obtain

$$(HA + KM)(HA - KM) = p_1^{m_1-1}(K^2N^2 - 2p_1H^2B^2). \tag{3.F.7}$$

By Lemma 3.6, p_1 does not divide both of $HA \pm KM$. Choose the sign of A so that $p_1 \nmid HA + KM$. Define odd integers R and S by

$$R = (HA + KM)/2^r, \qquad S = (HA - KM)/2^s p_1^\alpha, \tag{3.F.8}$$

where $p_1^\alpha \parallel HA - KM$. Clearly, $p_1 \nmid RS$. We note that

$$\begin{cases} \alpha \geq m_1 - 1 \geq 1, \\ \min(r, s) = 1,\ r + s \geq 3 & \text{if } p \equiv 1 \pmod 8), \\ r = s = 0 & \text{if } p \equiv 3 \pmod 8). \end{cases} \tag{3.F.9}$$

We first show that

$$\left(\frac{R}{p_1}\right)\left(\frac{S}{p_1}\right) = (-1)^{\alpha+1}. \tag{3.F.10}$$

From (3.F.7), (3.F.8) and (3.F.9), we see that

$$p_1^{\alpha-m_1+1} \parallel K^2N^2 - 2p_1H^2B^2.$$

Thus, by Lemma 3.4, we have

$$\begin{cases} p_1^{(\alpha-m_1+1)/2} \parallel N,\ p_1^{(\alpha-m_1+1)/2} \mid B & \text{if } \alpha \text{ is odd}, \\ p_1^{(\alpha-m_1+2)/2} \mid N,\ p_1^{(\alpha-m_1)/2} \parallel B & \text{if } \alpha \text{ is even}. \end{cases}$$

Define integers N_1 and B_1 by

$$\begin{cases} N = p_1^{(\alpha-m_1+1)/2} N_1,\ B = p_1^{(\alpha-m_1+1)/2} B_1 & \text{if } \alpha \text{ is odd}, \\ N = p_1^{(\alpha-m_1+2)/2} N_1,\ B = p_1^{(\alpha-m_1)/2} B_1 & \text{if } \alpha \text{ is even}, \end{cases}$$

so that

$$p_1 \nmid N_1 \ (\alpha \text{ odd}), \qquad p_1 \nmid B_1 \ (\alpha \text{ even}).$$

Hence

$$2^{r+s}RS = \begin{cases} K^2N_1^2 - 2p_1H^2B_1^2 & \text{if } \alpha \text{ is odd}, \\ p_1K^2N_1^2 - 2H^2B_1^2 & \text{if } \alpha \text{ is even}, \end{cases}$$

so that (recalling $(2/p_1)=1$)

$$\left(\frac{R}{p_1}\right)\left(\frac{S}{p_1}\right)=\begin{cases}\left(\dfrac{K^2N_1^2}{p_1}\right)=1 & \text{if } \alpha \text{ is odd,}\\ \left(\dfrac{-2H^2B_1^2}{p_1}\right)=-1 & \text{if } \alpha \text{ is even,}\end{cases}$$

proving (3.F.10).

We next show that

$$\left(\frac{R}{p_1}\right)=\left(\frac{-2}{R}\right),\qquad \left(\frac{S}{p_1}\right)=\left(\frac{-2}{S}\right). \tag{3.F.11}$$

We factor R into primes as follows:

$$R=\varepsilon\prod_{(2p_1/q_i)=1} q_i^{e_i}\prod_{(2p_1/r_j)=-1} r_j^{f_j}, \tag{3.F.12}$$

where $\varepsilon=\pm1$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. By Lemma 3.5(ii) each f_j is even. It is convenient to define

$$E_k=\sum_{\substack{(2p_1/q_i)=1\\ q_i\equiv k\,(\mathrm{mod}\,8)}} e_i,\qquad k=1,3,5,7. \tag{3.F.13}$$

From (3.F.12) we have

$$\begin{aligned}\left(\frac{R}{p_1}\right)&=\left(\frac{\varepsilon}{p_1}\right)\prod_{(2p_1/q_i)=1}\left(\frac{q_i}{p_1}\right)^{e_i} && \text{(as the } f_j \text{ are even)}\\ &=\varepsilon\prod_{(2p_1/q_i)=1}\left(\frac{-p_1}{q_i}\right)^{e_i} && \text{(by the law of quadratic reciprocity)}\\ &=\varepsilon\prod_{(2p_1/q_i)=1}\left(\frac{-2}{q_i}\right)^{e_i}\\ &=\varepsilon\prod_{\substack{(2p_1/q_i)=1\\ q_i\equiv 5,7\,(\mathrm{mod}\,8)}}(-1)^{e_i},\end{aligned}$$

that is, by (3.F.13),

$$\left(\frac{R}{p_1}\right)=\varepsilon(-1)^{E_5+E_7}. \tag{3.F.14}$$

Now taking (3.F.12) modulo 4, we obtain, as each f_j is even,

$$R\equiv\varepsilon\prod_{(2p_1/q_i)=1}q_i^{e_i}\equiv\varepsilon\prod_{\substack{(2p_1/q_i)=1\\ q_i\equiv 3\,(\mathrm{mod}\,4)}}(-1)^{e_i}\equiv\varepsilon(-1)^{E_3+E_7}\pmod 4,$$

that is,

$$\left(\frac{-1}{R}\right) = \varepsilon(-1)^{E_3+E_7},$$

so

$$\varepsilon = \left(\frac{-1}{R}\right)(-1)^{E_3+E_7}. \tag{3.F.15}$$

Substituting (3.F.15) in (3.F.14), we obtain

$$\left(\frac{R}{p_1}\right) = \left(\frac{-1}{R}\right)(-1)^{E_3+E_5}. \tag{3.F.16}$$

Further, taking (3.F.12) modulo 8, we deduce

$$\begin{aligned} R &\equiv \varepsilon \prod_{\substack{(2p_1/q_i)=1\\ q_i\equiv 3 \pmod 8}} 3^{e_i} \prod_{\substack{(2p_1/q_i)=1\\ q_i\equiv 5 \pmod 8}} 5^{e_i} \prod_{\substack{(2p_1/q_i)=1\\ q_i\equiv 7 \pmod 8}} 7^{e_i} \\ &\equiv \varepsilon 3^{E_3} 5^{E_5} 7^{E_7} \\ &\equiv \varepsilon(-5)^{E_3} 5^{E_5}(-1)^{E_7} \\ &\equiv \varepsilon(-1)^{E_3+E_7} 5^{E_3+E_5} \pmod 8, \end{aligned}$$

that is, by (3.F.15),

$$R \equiv \left(\frac{-1}{R}\right) 5^{E_3+E_5} \pmod 8. \tag{3.F.17}$$

Hence, from (3.F.17), we have

$$\left(\frac{2}{R}\right) = \left(\frac{2}{5}\right)^{E_3+E_5} = (-1)^{E_3+E_5}. \tag{3.F.18}$$

Then, from (3.F.16) and (3.F.18), we deduce

$$\left(\frac{R}{p_1}\right) = \left(\frac{-1}{R}\right)\left(\frac{2}{R}\right) = \left(\frac{-2}{R}\right),$$

as asserted in (3.F.11). The proof of $(S/p_1) = (-2/S)$ is similar.

The next step is to show that

$$\left(\frac{-2}{R}\right) = (-1)^{N(p_1+1)/8}\left(\frac{2}{M+N}\right). \tag{3.F.19}$$

We consider two cases according as $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.

Case 1: $p \equiv 1 \pmod 8$. We set (recalling (3.F.1)–(3.F.6))

$$A = 4a + \varepsilon_A, \quad B = 2b, \quad H = 4h + \varepsilon_H, \quad K = 4k + (-1)^k,$$
$$M = 4m + 1, \quad N = 4n,$$

where $\varepsilon_A = \pm 1$, $\varepsilon_H = \pm 1$. Substituting these in (3.F.7), reducing modulo 32, and dividing by 8, we obtain

$$2(a+h+k+m+n)+(\varepsilon_A a+\varepsilon_H h-(-1)^k k-m) \equiv -b^2 \pmod{4}. \tag{3.F.20}$$

Taking (3.F.20) modulo 2 we have

$$b \equiv a+h+k+m \pmod{2}. \tag{3.F.21}$$

Next, substituting the above values for $A, B, \ldots$ into the first equation in (3.F.8) when $r = 1$ and into the second equation in (3.F.8) when $s = 1$, we obtain, modulo 16,

$$\begin{cases} 4(\varepsilon_H a+\varepsilon_A h)+4(-1)^k m+4k+(\varepsilon_A\varepsilon_H+(-1)^k) \\ \qquad \equiv 2R \pmod{16} & \text{if } r=1, \\ 4(\varepsilon_H a+\varepsilon_A h)-4(-1)^k m-4k+(\varepsilon_A\varepsilon_H+(-1)^{k+1}) \\ \qquad \equiv 2p_1^\alpha S \pmod{16} & \text{if } s=1. \end{cases} \tag{3.F.22}$$

Looking at (3.F.22) modulo 4, we deduce

$$\begin{cases} \varepsilon_A\varepsilon_H+(-1)^k \equiv 2 \pmod{4} & \text{if } r=1, \\ \varepsilon_A\varepsilon_H-(-1)^k \equiv 2 \pmod{4} & \text{if } s=1, \end{cases}$$

that is,

$$\varepsilon_A = \begin{cases} (-1)^k\varepsilon_H & \text{if } r=1, \\ (-1)^{k+1}\varepsilon_H & \text{if } s=1. \end{cases} \tag{3.F.23}$$

Substituting (3.F.23) in (3.F.22), and dividing by 2, we obtain

$$\begin{cases} R \equiv 2\varepsilon_H(a+(-1)^k h)+2(-1)^k m+2k+(-1)^k \pmod{8} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } r=1, \\ (-1)^\alpha S \equiv 2\varepsilon_H(a+(-1)^{k+1}h)+2(-1)^{k+1}m-2k \\ \qquad\qquad +(-1)^{k+1} \pmod{8} & \text{if } s=1. \end{cases} \tag{3.F.24}$$

Taking (3.F.24) modulo 4, we have

$$\begin{cases} R \equiv 2(a+h+m)+1 \pmod{4} & \text{if } r=1, \\ (-1)^\alpha S \equiv 2(a+h+m)-1 \pmod{4} & \text{if } s=1, \end{cases} \tag{3.F.25}$$

as $2k+(-1)^k \equiv 1 \pmod{4}$ for all integers k. Then, using (3.F.21) and (3.F.23), we may rewrite (3.F.20) as

$$\begin{cases} \varepsilon_H(a+(-1)^k h) \\ \qquad \equiv (-1)^k m+k+2(b+n)-(-1)^k b^2 \pmod{4} & \text{if } r=1, \\ \varepsilon_H(a+(-1)^{k+1}h) \\ \qquad \equiv (-1)^{k+1}m-k+2(b+n)+(-1)^k b^2 \pmod{4} & \text{if } s=1. \end{cases} \tag{3.F.26}$$

Substituting (3.F.26) into (3.F.24) gives

$$\begin{cases} R \equiv 4(b+k+m+n)-2(-1)^k b^2+(-1)^k \pmod{8} & \text{if } r=1, \\ (-1)^\alpha S \equiv 4(b+k+m+n)+2(-1)^k b^2+(-1)^{k+1} \pmod{8} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } s=1. \end{cases} \tag{3.F.27}$$

Now, from (3.F.21) and (3.F.25), we have

$$\text{(3.F.28)}\qquad \begin{cases} R \equiv 2(b+k)+1 \pmod 4 & \text{if } r=1,\\ (-1)^\alpha S \equiv 2(b+k)-1 \pmod 4 & \text{if } s=1. \end{cases}$$

Applying (3.F.28) to the right side of (3.F.27), we obtain

$$\begin{cases} R \equiv 2(R-1)+4(m+n)-2(-1)^k b^2+(-1)^k \pmod 8 & \text{if } r=1,\\ (-1)^\alpha S \equiv 2((-1)^\alpha S+1)+4(m+n)+2(-1)^k b^2+(-1)^{k+1} \pmod 8 & \\ & \text{if } s=1. \end{cases}$$

By rearranging and then squaring, we obtain

$$\begin{cases} R^2-4R+4-8(m+n) \equiv 1 \pmod{16} & \text{if } r=1,\\ S^2+4(-1)^\alpha S+4-8(m+n) \equiv 1 \pmod{16} & \text{if } s=1, \end{cases}$$

as $(2b^2-1)^2 = 4b^2(b^2-1)+1 \equiv 1 \pmod{16}$. Hence

$$\begin{cases} (R^2-1)-4(R-1) \equiv 8(m+n) \pmod{16} & \text{if } r=1,\\ (S^2-1)-4(S-1) \equiv 8(m+n)+8(\alpha+1) \pmod{16} & \text{if } s=1. \end{cases}$$

Thus if $r=1$ we have

$$\begin{aligned}\left(\frac{-2}{R}\right) &= (-1)^{(R-1)/2+(R^2-1)/8} = (-1)^{m+n}\\ &= (-1)^{((M+N)^2-1)/8} = \left(\frac{2}{M+N}\right),\end{aligned}$$

and if $s=1$ we have

$$\begin{aligned}\left(\frac{-2}{S}\right) &= (-1)^{(S-1)/2+(S^2-1)/8} = (-1)^{m+n+\alpha+1}\\ &= (-1)^{((M+N)^2-1)/8}(-1)^{\alpha+1} = \left(\frac{2}{M+N}\right)\left(\frac{-2}{R}\right)\left(\frac{-2}{S}\right)\\ &\qquad \text{(by (3.F.10) and (3.F.11))}\end{aligned}$$

so that in both cases

$$\left(\frac{-2}{R}\right) = \left(\frac{2}{M+N}\right).$$

This completes the proof of (3.F.19) when $p \equiv 1 \pmod 8$ as N is even in this case.

Case 2: $p \equiv 3 \pmod 8$. We set (recalling (3.F.1)–(3.F.6))

$$\begin{gathered} A = 4a+\varepsilon_A, \quad B = 4b+\varepsilon_B, \quad H = 4h+\varepsilon_H,\\ K = 4k+(-1)^k, \quad M = 4m+2, \quad N = 4n-1, \end{gathered}$$

where $\varepsilon_A = \pm 1$, $\varepsilon_B = \pm 1$, $\varepsilon_H = \pm 1$. Taking $R = HA+KM$ modulo 4, we obtain

$$\text{(3.F.29)}\qquad \varepsilon_A \varepsilon_H = (-1)^{(R+1)/2}.$$

Then, taking $R = HA + KM$ modulo 8, and appealing to (3.F.29), we deduce

$$\left(\frac{-2}{R}\right) = (-1)^{a+h+k+m}. \tag{3.F.30}$$

From (3.F.7) modulo 16 we have

$$a + h + k \equiv n + (p_1 + 1)/8 \pmod 2. \tag{3.F.31}$$

Then, from (3.F.30) and (3.F.31), we obtain

$$\left(\frac{-2}{R}\right) = (-1)^{m+n+(p_1+1)/8} = \left(\frac{2}{M+N}\right)(-1)^{(p_1+1)/8},$$

which is (3.F.19) as N is odd in this case. This completes the proof of (3.F.19).

Now, by (3.F.7) and (3.F.8), we have

$$\begin{aligned} 2^{2r}R^2 - 2^{r+1}RKM &= (HA + KM)^2 - 2(HA + KM)KM \\ &= (HA + KM)(HA - KM) \\ &= p_1^{m_1-1}(K^2N^2 - 2p_1H^2B^2) \\ &\equiv 0 \pmod{p_1} \quad (\text{as } m_1 \geq 2), \end{aligned}$$

so that

$$\left(\frac{2}{p_1}\right)^{r+1}\left(\frac{R}{p_1}\right)\left(\frac{K}{p_1}\right)\left(\frac{M}{p_1}\right) = 1. \tag{3.F.32}$$

Finally,

C_p is a fourth power in $H(-D)$

$$\begin{aligned} &\Leftrightarrow \left(\frac{-2}{K}\right) = \left(\frac{K}{p_1}\right) = 1 \\ &\Leftrightarrow \left(\frac{K}{p_1}\right) = 1 && \text{(by (3.F.3))} \\ &\Leftrightarrow \left(\frac{R}{p_1}\right)\left(\frac{M}{p_1}\right) = 1 && \text{(by (3.F.32))} \\ &\Leftrightarrow \left(\frac{-2}{R}\right)\left(\frac{M}{p_1}\right) = 1 && \text{(by (3.F.11))}, \end{aligned}$$

that is, *under the restriction* (3.F.6),

(3.F.33) C_p is a fourth power in $H(-D)$

$$\Leftrightarrow (-1)^{N(p_1+1)/8}\left(\frac{2}{M+N}\right)\left(\frac{M}{p_1}\right) = 1 \quad \text{(by (3.F.19))}.$$

In order to remove this restriction, the necessary and sufficient condition (3.F.33) must include the additional factor

$$\left(\frac{-1}{M+N}\right) = \begin{cases} 1 & \text{if } M+N \equiv 1 \pmod 4, \\ -1 & \text{if } M+N \equiv 3 \pmod 4, \end{cases}$$

so that the condition can now be written

$$(-1)^{N(p_1+1)/8}\left(\frac{-2}{M+N}\right)\left(\frac{M}{p_1}\right) = 1.$$

Case (G): $D = 16p_1^{m_1}$, $D^* = 16p_1^{m_1-1}$, $m_1 \ge 1$, $p_1 \equiv 1 \pmod 4$. Let p be an odd prime satisfying $(-1/p) = (p/p_1) = 1$, so that $p \equiv 1 \pmod 4$ and $p \ne p_1$. From (3.2) and (3.1) we have

(3.G.1) $H^2p = M^2 + 4p_1^{m_1-1}N^2, \qquad H > 0,\ (M,N) = 1,\ (H, 2pp_1) = 1,$

(3.G.2) $K^2p = A^2 + 4p_1^{m_1}B^2, \qquad K > 0,\ (A,B) = 1, (K, 2pp_1) = 1.$

By (3.3) we have $(-D/K) = (-16p_1^{m_1}/K) = 1$, so that by the law of quadratic reciprocity

(3.G.3) $$\left(\frac{-1}{K}\right) = \left(\frac{p_1}{K}\right)^{m_1} = \left(\frac{K}{p_1}\right)^{m_1}.$$

Reducing (3.G.1) and (3.G.2) modulo 8, we obtain

(3.G.4) $$A \equiv M \equiv 1 \pmod 2, \qquad B \equiv N \equiv (p-1)/4 \pmod 2.$$

From (3.G.1) and (3.G.2) we obtain

(3.G.5) $$(HA + KM)(HA - KM) = 4p_1^{m_1-1}(K^2N^2 - p_1H^2B^2).$$

By Lemma 3.6, p_1 does not divide both of $HA \pm KM$. Choose the sign of A so that $p_1 \nmid HA + KM$. Define odd integers R and S by

(3.G.6) $$R = (HA + KM)/2^r, \qquad S = (HA - KM)/2^s p_1^{\alpha},$$

where $p_1^{\alpha} \parallel HA - KM$. Clearly $p_1 \nmid RS$, $\alpha \ge m_1 - 1$, and appealing to (3.G.4) we see that

(3.G.7) $$\min(r,s) = 1, \qquad r + s \ge 4.$$

From (3.G.5) and (3.G.6) we see that $2^{r+s-2} \parallel K^2N^2 - p_1H^2B^2$. Thus, by Lemma 3.2(iii), we have

(3.G.8) $$r + s \equiv 0 \pmod 2 \quad \text{if } p_1 \equiv 5 \pmod 8.$$

We factor R into primes:

(3.G.9) $$R = \varepsilon \prod_{(p_1/q_i)=1} q_i^{e_i} \prod_{(p_1/r_j)=-1} r_j^{f_j},$$

where $\varepsilon = \pm 1$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. By Lemma 3.5(ii) each f_j is even. From (3.G.9) we have by the law of quadratic reciprocity

$$\left(\frac{R}{p_1}\right)=1. \tag{3.G.10}$$

By Lemma 3.1 we have

$$\begin{cases} 2(HA+KM)(KM+wKN) \\ \qquad \equiv (HA+KM+wKN)^2 \pmod{p_1} & \text{if } m_1=1, \\ 2(HA+KM)KM \equiv (HA+KM)^2 \pmod{p_1} & \text{if } m_1\ge 2, \end{cases} \tag{3.G.11}$$

where $w^2\equiv -4 \pmod{p_1}$. Thus by (3.G.6) and (3.G.11), we have

$$\begin{cases} \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{R}{p_1}\right)\left(\frac{K}{p_1}\right)\left(\frac{M+wN}{p_1}\right)=1 & \text{if } m_1=1, \\ \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{R}{p_1}\right)\left(\frac{K}{p_1}\right)\left(\frac{M}{p_1}\right)=1 & \text{if } m_1\ge 2. \end{cases} \tag{3.G.12}$$

If $p_1\equiv 1 \pmod 8$ then $(2/p_1)=1$. If $p_1\equiv 5 \pmod 8$ then by (3.G.7) and (3.G.8), r is odd so that $(2/p_1)^{r+1}=(-1)^{r+1}=1$. Hence, by (3.G.10) and (3.G.12), we have

$$\left(\frac{K}{p_1}\right)=\begin{cases} \left(\frac{M+wN}{p_1}\right) & \text{if } m_1=1, \\ \left(\frac{M}{p_1}\right) & \text{if } m_1\ge 2. \end{cases} \tag{3.G.13}$$

Finally,

C_p is a fourth power in $H(-D)$

$$\Leftrightarrow \left(\frac{-1}{K}\right)=\left(\frac{K}{p_1}\right)=1$$

$$\Leftrightarrow \left(\frac{K}{p_1}\right)=1 \qquad \text{(by (3.G.3))}$$

$$\Leftrightarrow \begin{cases} \left(\frac{M+wN}{p_1}\right)=1 \\ \qquad\qquad \text{if } m_1=1, \text{ where } w^2\equiv -4 \pmod{p_1} \\ \left(\frac{M}{p_1}\right)=1 \quad \text{if } m_1\ge 2 \end{cases} \qquad \text{(by (3.G.13))}.$$

Case (H): $D=16p_1^{m_1}$, $D^*=16p_1^{m_1-1}$, m_1 (even) ≥ 2, $p_1\equiv 3 \pmod 4$. Let p be an odd prime such that $(-1/p)=(p/p_1)=1$, so that $p\equiv 1 \pmod 4$ and $p\ne p_1$. From (3.2) and (3.1) we have

$$H^2p=M^2+4p_1^{m_1-1}N^2, \qquad H>0,\ (M,N)=1,\ (H,2pp_1)=1, \tag{3.H.1}$$

$$K^2p=A^2+4p_1^{m_1}B^2, \qquad K>0,\ (A,B)=1,\ (K,2pp_1)=1. \tag{3.H.2}$$

From (3.3) we have $(-D/K) = (-16p_1^{m_1}/K) = 1$, so that

$$\left(\frac{-1}{K}\right) = 1, \quad K \equiv 1 \pmod 4. \tag{3.H.3}$$

Reducing (3.H.1) and (3.H.2) modulo 8, we obtain

$$A \equiv M \equiv 1 \pmod 2, \quad B \equiv N \equiv (p-1)/4 \pmod 2. \tag{3.H.4}$$

From (3.H.1) and (3.H.2) we obtain

$$(HA+KM)(HA-KM) = 4p_1^{m_1-1}(K^2N^2 - p_1H^2B^2). \tag{3.H.5}$$

By Lemma 3.6, p_1 does not divide both of $HA \pm KM$. We choose the sign of A so that $p_1 \nmid HA+KM$, and define odd integers R and S by

$$R = (HA+KM)/2^r, \quad S = (HA-KM)/2^s p_1^{\alpha}, \tag{3.H.6}$$

where $p_1^{\alpha} \parallel HA-KM$. Clearly $p_1 \nmid RS$. We note that

$$\begin{cases} \alpha \geq m_1 - 1 \geq 1, \\ \min(r,s) = 1, \\ p \equiv 1 \pmod 8 & \text{if } r+s \geq 4, \\ p \equiv 5 \pmod 8 & \text{if } r+s = 3. \end{cases} \tag{3.H.7}$$

Proceeding exactly as in the proof of (3.C.11), we obtain

$$\left(\frac{2}{p_1}\right)^{r+s} \left(\frac{R}{p_1}\right)\left(\frac{S}{p_1}\right) = (-1)^{\alpha+1},$$

that is,

$$\left(\frac{R}{p_1}\right)\left(\frac{S}{p_1}\right) = \left(\frac{2}{p_1}\right)^{r+s} (-1)^{\alpha+1}. \tag{3.H.8}$$

Next, factoring R and S into primes and proceeding as in case (C) ((3.C.12)–(3.C.16)), we obtain

$$\left(\frac{R}{p_1}\right) = (-1)^{(R-1)/2}, \quad \left(\frac{S}{p_1}\right) = (-1)^{(S-1)/2}. \tag{3.H.9}$$

From (3.H.8) and (3.H.9) we deduce

$$(R-1)/2 + (S-1)/2 \equiv (r+s)(p_1^2-1)/8 + (\alpha+1) \pmod 2. \tag{3.H.10}$$

Our next task is to show that

$$(M-1)/2 + N \equiv (R-1)/2 + (r+1)(p_1^2-1)/8 \pmod 2. \tag{3.H.11}$$

From (3.H.7) either $r = 1$ or $s = 1$. We treat the case $r = 1$ first. In this case $s \geq 2$ by (3.H.7). Working modulo 4 we have

$$\begin{aligned}
R &= KM + p_1^\alpha 2^{s-1} S && \text{(by (3.H.6))}\\
&\equiv M + p_1^\alpha 2^{s-1} S && \text{(by (3.H.3))}\\
&\equiv M + \begin{cases} 2 & \text{if } s = 2\\ 0 & \text{if } s \geq 3\end{cases} && \text{(as } p_1, S \text{ are odd)}\\
&\equiv \begin{cases} M+2 & \text{if } p \equiv 5 \pmod 8\\ M & \text{if } p \equiv 1 \pmod 8\end{cases} && \text{(by (3.H.7))}\\
&\equiv M + 2N \pmod 4 && \text{(by (3.H.4)),}
\end{aligned}$$

so that

$$(M-1)/2 + N \equiv (R-1)/2 \pmod 2,$$

proving (3.H.11) in this case. We now turn to the case $s = 1$. In this case $r \geq 2$ by (3.H.7). Working modulo 4 we have

$$\begin{aligned}
2\alpha + S &\equiv (-1)^\alpha S && \text{(as } S \equiv 1 \pmod 2\text{))}\\
&\equiv p_1^\alpha S && \text{(as } p_1 \equiv 3 \pmod 4\text{))}\\
&\equiv (HA - KM)/2 && \text{(by (3.H.6))}\\
&\equiv 2^{r-1}R - KM && \text{(by (3.H.6))}\\
&\equiv 2^{r-1}R - M && \text{(by (3.H.3))}\\
&\equiv 2^{r-1} + M + 2 && \text{(as } R \text{ and } M \text{ are odd)}\\
&\equiv \begin{cases} M+2 & \text{if } r \geq 3 \Leftrightarrow p \equiv 1 \pmod 8\\ M & \text{if } r = 2 \Leftrightarrow p \equiv 5 \pmod 8\end{cases} && \text{(by (3.H.7))}\\
&\equiv M + 2N - 2 \pmod 4 && \text{(by (3.H.4)),}
\end{aligned}$$

so that

$$(M-1)/2 + N \equiv (S-1)/2 + (\alpha + 1) \pmod 2.$$

Appealing to (3.H.10) we obtain

$$(M-1)/2 + N \equiv (R-1)/2 + (r+1)(p_1^2 - 1)/8 \pmod 2$$

as required.

From (3.H.5) and (3.H.6) we have

$$\begin{aligned}
2^{2r}R^2 - 2^{r+1}RKM &= (HA + KM)^2 - 2(HA + KM)KM\\
&= (HA + KM)(HA - KM)\\
&= 4p_1^{m_1 - 1}(K^2N^2 - p_1H^2B^2)\\
&\equiv 0 \pmod{p_1} \quad \text{(as } m_1 \geq 2\text{),}
\end{aligned}$$

so that

$$\left(\frac{2^{r+1}RKM}{p_1}\right) = \left(\frac{2^{2r}R^2}{p_1}\right) = 1,$$

giving

$$\begin{aligned}\left(\frac{K}{p_1}\right) &= \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{R}{p_1}\right)\left(\frac{M}{p_1}\right)\\ &= (-1)^{(r+1)(p_1^2-1)/8+(R-1)/2}\left(\frac{M}{p_1}\right) \qquad \text{(by (3.H.9))},\end{aligned}$$

that is,

(3.H.12) $$\left(\frac{K}{p_1}\right) = (-1)^{(M-1)/2+N}\left(\frac{M}{p_1}\right) \qquad \text{(by (3.H.11))}.$$

Finally,

C_p is a fourth power in $H(-D)$

$$\begin{aligned}&\Leftrightarrow \left(\frac{-1}{K}\right) = \left(\frac{K}{p_1}\right) = 1\\ &\Leftrightarrow \left(\frac{K}{p_1}\right) = 1 && \text{(by (3.H.3))}\\ &\Leftrightarrow (-1)^{(M-1)/2+N}\left(\frac{M}{p_1}\right) = 1 && \text{(by (3.H.12))}\\ &\Leftrightarrow \left(\frac{-1}{M+2N}\right)\left(\frac{M}{p_1}\right) = 1.\end{aligned}$$

Case (I): $D = p_1^{m_1}p_2^{m_2}$, $D^* = p_1^{m_1}p_2^{m_2-1}$, m_1 (odd) ≥ 1, $m_2 \geq 1$, $p_1 \equiv 3 \pmod 4$, $p_2 \equiv 1 \pmod 4$, $(p_1/p_2) = 1$. Let p be an odd prime such that $(p/p_1) = (p/p_2) = 1$, so that $p \neq p_1, p_2$. From (3.2) and (3.1) we have

(3.I.1) $$H^2p = M^2 + MN + \tfrac{1}{4}(1 + p_1^{m_1}p_2^{m_2-1})N^2, \qquad H > 0,\ (M,N) = 1,\ (H, 2pp_1p_2) = 1,$$

(3.I.2) $$K^2p = A^2 + AB + \tfrac{1}{4}(1 + p_1^{m_1}p_2^{m_2})B^2, \qquad K > 0,\ (A,B) = 1,\ (K, 2pp_1p_2) = 1.$$

From (3.3) we have $(-D/K) = (-p_1^{m_1}p_2^{m_2}/K) = 1$, so that, by the law of quadratic reciprocity,

(3.I.3) $$\left(\frac{K}{p_1}\right) = \left(\frac{K}{p_2}\right)^{m_2}.$$

We set

(3.I.4) $$C = 2A + B, \qquad L = 2M + N.$$

Using (3.I.4) in (3.I.1) and (3.I.2), we obtain

(3.I.5) $$4H^2p = L^2 + p_1^{m_1}p_2^{m_2-1}N^2,$$

(3.I.6) $$4K^2p = C^2 + p_1^{m_1}p_2^{m_2}B^2.$$

We note that

$$(3.I.7)\quad (L,N)=(2M+N,N)=(2M,N)=(2,N)=\begin{cases}1 & \text{if } N \text{ is odd,}\\ 2 & \text{if } N \text{ is even,}\end{cases}$$

$$(3.I.8)\quad (C,B)=(2A+B,B)=(2A,B)=(2,B)=\begin{cases}1 & \text{if } B \text{ is odd,}\\ 2 & \text{if } B \text{ is even.}\end{cases}$$

From (3.I.5) and (3.I.6) we obtain

$$(3.I.9)\qquad (HC+KL)(HC-KL)=p_1^{m_1}p_2^{m_2-1}(K^2N^2-p_2H^2B^2).$$

Lemma 3.6 implies that neither p_1 nor p_2 divides both of $HC \pm KL$. By changing the sign of C if necessary, we may suppose that $p_1 \nmid HC+KL$. We define odd integers R and S by

$$(3.I.10)\qquad R=(HC+KL)/2^r p_2^{\beta},\qquad S=(HC-KL)/2^s p_1^{\alpha} p_2^{\gamma},$$

where $p_1^{\alpha} \parallel HC-KL,\ p_2^{\beta} \parallel HC+KL,\ p_2^{\gamma} \parallel HC-KL$. We note that

$$(3.I.11)\qquad \begin{cases} p_1 \nmid RS,\ p_2 \nmid RS,\\ \alpha \ge m_1 \ge 1,\ \beta+\gamma \ge m_2-1 \ge 0,\\ \min(\beta,\gamma)=0.\end{cases}$$

Next we factor R into primes:

$$(3.I.12)\qquad R=\varepsilon \prod_{(p_2/q_i)=1} q_i^{e_i} \prod_{(p_2/r_j)=-1} r_j^{f_j},$$

where $\varepsilon=\pm 1$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. From (3.I.5)–(3.I.8), (3.I.10) and Lemma 3.5(ii) we see that each f_j is even. Then, from (3.I.12), we have

$$(3.I.13)\qquad \left(\frac{R}{p_2}\right)=\left(\frac{\varepsilon}{p_2}\right)\prod_{(p_2/q_i)=1}\left(\frac{q_i}{p_2}\right)^{e_i}=1,$$

by the law of quadratic reciprocity. Similarly we have

$$(3.I.14)\qquad \left(\frac{S}{p_2}\right)=1.$$

Next, by Lemma 3.1 and (3.I.9), we have

$$(3.I.15)\quad 2(KL\pm HC)(KL+\theta KN)\equiv (KL\pm HC+\theta KN)^2 \pmod{p_2},$$

where θ is a solution of the congruence

$$(3.I.16)\qquad \theta^2 \equiv -p_1^{m_1}p_2^{m_2-1} \pmod{p_2}.$$

Note that we may take $\theta = 0$ when $m_2 \geq 2$. The congruence (3.I.16) is solvable when $m_2 = 1$ as

$$\left(\frac{-p_1^{m_1}}{p_2}\right) = \left(\frac{p_1}{p_2}\right)^{m_1} = 1.$$

From (3.I.15) we have, as $(-1/p_2) = 1$,

$$\left(\frac{2}{p_2}\right)\left(\frac{HC \pm KL}{p_2}\right)\left(\frac{K}{p_2}\right)\left(\frac{L+\theta N}{p_2}\right) = 1. \tag{3.I.17}$$

Recall from (3.I.11) that either $\beta = 0$ or $\gamma = 0$. Taking the + sign in (3.I.17) when $\beta = 0$ and the − sign when $\gamma = 0$, and appealing to (3.I.10), we obtain

$$\begin{cases} \left(\frac{2}{p_2}\right)^{r+1}\left(\frac{R}{p_2}\right)\left(\frac{K}{p_2}\right)\left(\frac{L+\theta N}{p_2}\right) = 1 & \text{if } \beta = 0, \\ \left(\frac{2}{p_2}\right)^{s+1}\left(\frac{p_1}{p_2}\right)^{\alpha}\left(\frac{S}{p_2}\right)\left(\frac{K}{p_2}\right)\left(\frac{L+\theta N}{p_2}\right) = 1 & \text{if } \gamma = 0. \end{cases} \tag{3.I.18}$$

Thus, by (3.I.13), (3.I.14) and (3.I.18), we have

$$\left(\frac{K}{p_2}\right) = \begin{cases} \left(\frac{2}{p_2}\right)^{r+1}\left(\frac{L+\theta N}{p_2}\right) & \text{if } \beta = 0, \\ \left(\frac{2}{p_2}\right)^{s+1}\left(\frac{L+\theta N}{p_2}\right) & \text{if } \gamma = 0. \end{cases} \tag{3.I.19}$$

If $p_2 \equiv 1 \pmod 8$ then $(2/p_2)^{r+1} = (2/p_2)^{s+1} = (2/p_2)$. If $p_2 \equiv 5 \pmod 8$, by Lemma 3.7, r and s are both even so $(2/p_2)^{r+1} = (2/p_2)^{s+1} = (2/p_2)$. Hence (3.I.19) reduces to

$$\left(\frac{K}{p_2}\right) = \left(\frac{2}{p_2}\right)\left(\frac{L+\theta N}{p_2}\right). \tag{3.I.20}$$

Now set $w \equiv (1+\theta)/2 \pmod{p_2}$ so that

$$L + \theta N = 2M + (1+\theta)N \equiv 2(M + wN) \pmod{p_2}, \tag{3.I.21}$$

and w is a solution of the congruence

$$w^2 - w + \tfrac{1}{4}(1 + p_1^{m_1} p_2^{m_2 - 1}) \equiv 0 \pmod{p_2}.$$

Note $2w \equiv 1 \pmod{p_2}$ if $m_2 \geq 2$.

Hence, by (3.I.20) and (3.I.21), we have

$$\left(\frac{K}{p_2}\right) = \left(\frac{M+wN}{p_2}\right). \tag{3.I.22}$$

Finally,

C_p is a fourth power

$$\Leftrightarrow \left(\frac{K}{p_1}\right) = \left(\frac{K}{p_2}\right) = 1$$

$$\Leftrightarrow \left(\frac{K}{p_2}\right) = 1 \qquad \text{(by (3.I.3))}$$

$$\Leftrightarrow \left(\frac{M+wN}{p_2}\right) = 1 \qquad \text{(by (3.I.22))}$$

$$\Leftrightarrow \begin{cases} \left(\dfrac{M+wN}{p_2}\right) = 1 & \text{if } m_2 = 1, \\ \qquad\qquad \text{where } w^2 - w + \frac{1}{4}(1+p_1^{m_1}) \equiv 0 \pmod{p_2}, \\ \left(\dfrac{4M+2N}{p_2}\right) = 1 & \text{if } m_2 \geq 2. \end{cases}$$

Case (J): $D = p_1^{m_1}p_2^{m_2}$, $D^* = p_1^{m_1-1}p_2^{m_2-1}$, m_1 (odd) ≥ 1, m_2 (even) ≥ 2, $p_1 \equiv p_2 \equiv 3 \pmod 4$, $(p_1/p_2) = 1$. Let p be an odd prime such that $(p/p_1) = (p/p_2) = 1$, so that $p \neq p_1, p_2$. From (3.2) and (3.1) we have

(3.J.1) $$H^2p = M^2 + MN + \tfrac{1}{4}(1 + p_1^{m_1-1}p_2^{m_2-1})N^2, \quad H > 0,\ (M,N) = 1,\ (H, 2pp_1p_2) = 1,$$

(3.J.2) $$K^2p = A^2 + AB + \tfrac{1}{4}(1 + p_1^{m_1}p_2^{m_2})B^2, \quad K > 0,\ (A,B) = 1,\ (K, 2pp_1p_2) = 1.$$

From (3.3) we have $(-D/K) = (-p_1^{m_1}p_2^{m_2}/K) = 1$, so that by the law of quadratic reciprocity, we have

(3.J.3) $$\left(\frac{K}{p_1}\right) = \left(\frac{-p_1}{K}\right) = 1.$$

We set

(3.J.4) $$C = 2A + B, \qquad L = 2M + N.$$

Making use of (3.J.4), equations (3.J.1) and (3.J.2) become

(3.J.5) $$4H^2p = L^2 + p_1^{m_1-1}p_2^{m_2-1}N^2,$$

(3.J.6) $$4K^2p = C^2 + p_1^{m_1}p_2^{m_2}B^2.$$

As in case (I) we have

(3.J.7) $$(L,N) = \begin{cases} 1 & \text{if } N \text{ is odd,} \\ 2 & \text{if } N \text{ is even,} \end{cases}$$

(3.J.8) $$(C,B) = \begin{cases} 1 & \text{if } B \text{ is odd,} \\ 2 & \text{if } B \text{ is even.} \end{cases}$$

From (3.J.5) and (3.J.6) we obtain

$$(3.J.9)\qquad (HC+KL)(HC-KL)=p_1^{m_1-1}p_2^{m_2-1}(K^2N^2-p_1p_2H^2B^2).$$

By Lemma 3.6 neither p_1 nor p_2 divides both of $HC\pm KL$. By changing the sign of C if necessary, we may suppose that $p_2\nmid HC+KL$. We define odd integers R and S by

$$(3.J.10)\qquad R=(HC+KL)/2^r p_1^{\beta},\qquad S=(HC-KL)/2^s p_2^{\alpha}p_1^{\gamma},$$

where $p_2^{\alpha}\parallel HC-KL,\ p_1^{\beta}\parallel HC+KL,\ p_1^{\gamma}\parallel HC-KL$. We note that

$$(3.J.11)\qquad \begin{cases} p_1\nmid RS,\ p_2\nmid RS,\\ \alpha\ge m_2-1\ge 1,\ \beta+\gamma\ge m_1-1\ge 0,\\ \min(\beta,\gamma)=0.\end{cases}$$

Next we factor R into primes:

$$(3.J.12)\qquad R=\varepsilon\prod_{(p_1p_2/q_i)=1} q_i^{e_i}\prod_{(p_1p_2/r_j)=-1} r_j^{f_j},$$

where $\varepsilon=\pm1$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. By (3.J.5)–(3.J.8), (3.J.10), (3.J.12), and Lemma 3.5(ii), we see that each f_j in (3.J.12) is even. Hence

$$(3.J.13)\qquad \begin{aligned} \left(\frac{R}{p_1}\right)&=\left(\frac{\varepsilon}{p_1}\right)\prod_{(p_1p_2/q_i)=1}\left(\frac{q_i}{p_1}\right)^{e_i},\\ \left(\frac{R}{p_2}\right)&=\left(\frac{\varepsilon}{p_2}\right)\prod_{(p_1p_2/q_i)=1}\left(\frac{q_i}{p_2}\right)^{e_i}.\end{aligned}$$

By the law of quadratic reciprocity, we have

$$(p_1p_2/q_i)=1\Rightarrow(q_i/p_1p_2)=1\Rightarrow(q_i/p_1)=(q_i/p_2),$$

and, as $(\varepsilon/p_1)=(\varepsilon/p_2)=\varepsilon$, we deduce from (3.J.13) that

$$(3.J.14)\qquad \left(\frac{R}{p_1}\right)=\left(\frac{R}{p_2}\right).$$

Similarly we have

$$(3.J.15)\qquad \left(\frac{S}{p_1}\right)=\left(\frac{S}{p_2}\right).$$

From (3.J.9) and (3.J.10) we see that $p_2^{\alpha-m_2+1}\parallel K^2N^2-p_1p_2H^2B^2$. By Lemma 3.4 we observe that

$$\begin{cases} p_2^{(\alpha-m_2+1)/2}\parallel N,\ p_2^{(\alpha-m_2+1)/2}\mid B & \text{if } \alpha \text{ is odd},\\ p_2^{(\alpha-m_2+2)/2}\mid N,\ p_2^{(\alpha-m_2)/2}\parallel B & \text{if } \alpha \text{ is even}.\end{cases}$$

Define integers N_1 and B_1 by

$$\begin{cases} N_1 = N/p_2^{(\alpha-m_2+1)/2},\ B_1 = B/p_2^{(\alpha-m_2+1)/2} & \text{if } \alpha \text{ is odd,} \\ N_1 = N/p_2^{(\alpha-m_2+2)/2},\ B_1 = B/p_2^{(\alpha-m_2)/2} & \text{if } \alpha \text{ is even,} \end{cases}$$

so that $p_2 \nmid N_1$ (α odd) and $p_2 \nmid B_1$ (α even). Hence, by (3.J.10) and (3.J.9), we have

$$\begin{aligned} 2^{r+s} p_1^{\beta+\gamma} RS &= (H^2C^2 - K^2L^2)/p_2^{\alpha} \\ &= p_1^{m_1-1}(K^2N^2 - p_1p_2H^2B^2)/p_2^{\alpha-m_2+1} \\ &= \begin{cases} p_1^{m_1-1}(K^2N_1^2 - p_1p_2H^2B_1^2) & \text{if } \alpha \text{ is odd,} \\ p_1^{m_1-1}(p_2K^2N_1^2 - p_1H^2B_1^2) & \text{if } \alpha \text{ is even,} \end{cases} \end{aligned}$$

so that, as $(p_1/p_2) = 1$,

$$\left(\frac{2}{p_2}\right)^{r+s} \left(\frac{R}{p_2}\right)\left(\frac{S}{p_2}\right) = \begin{Bmatrix} +1 \text{ if } \alpha \text{ is odd} \\ -1 \text{ if } \alpha \text{ is even} \end{Bmatrix} = (-1)^{\alpha+1},$$

that is,

$$\left(\frac{R}{p_2}\right)\left(\frac{S}{p_2}\right) = \left(\frac{2}{p_2}\right)^{r+s}(-1)^{\alpha+1}. \tag{3.J.16}$$

A similar calculation, with the roles of p_1 and p_2 reversed (note that $(p_2/p_1) = -1$), shows that

$$\left(\frac{R}{p_1}\right)\left(\frac{S}{p_1}\right) = \left(\frac{2}{p_1}\right)^{r+s}(-1)^{\alpha+1}. \tag{3.J.17}$$

From (3.J.14)–(3.J.17) we obtain $(2/p_1)^{r+s} = (2/p_2)^{r+s}$, so that

$$\left(\frac{2}{p_1p_2}\right)^{r} = \left(\frac{2}{p_1p_2}\right)^{s}.$$

If $p_1p_2 \equiv 1 \pmod 8$ then $(2/p_1p_2) = 1$. If $p_1p_2 \equiv 5 \pmod 8$ then, by Lemma 3.7, r and s are both even. Thus in both cases we have

$$\left(\frac{2}{p_1p_2}\right)^{r} = \left(\frac{2}{p_1p_2}\right)^{s} = 1. \tag{3.J.18}$$

Now let θ be a solution of

$$\theta^2 \equiv -p_1^{m_1-1}p_2^{m_2-1} \pmod{p_1}. \tag{3.J.19}$$

If $m_1 \geq 3$ we see from (3.J.19) that we can take $\theta = 0$. If $m_1 = 1$ the congruence is solvable as $(-p_2^{m_2-1}/p_1) = (-p_2/p_1) = (p_1/p_2) = +1$. Then, by Lemma 3.1, we have

$$2(KL \pm HC)(KL + \theta KN) \equiv (KL \pm HC + \theta KN)^2 \pmod{p_1},$$

and thus

$$\left(\frac{2}{p_1}\right)\left(\frac{KL \pm HC}{p_1}\right)\left(\frac{K}{p_1}\right)\left(\frac{L+\theta N}{p_1}\right) = 1.$$

Recall from (3.J.11) that either $\beta = 0$ or $\gamma = 0$. Taking the + sign when $\beta = 0$ and the − sign when $\gamma = 0$, we obtain, appealing to (3.J.3) and (3.J.10),

$$\begin{cases} \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{R}{p_1}\right)\left(\frac{L+\theta N}{p_1}\right) = 1 & \text{if } \beta = 0, \\ \left(\frac{2}{p_1}\right)^{s+1}\left(\frac{-1}{p_1}\right)\left(\frac{p_2}{p_1}\right)^{\alpha}\left(\frac{S}{p_1}\right)\left(\frac{L+\theta N}{p_1}\right) = 1 & \text{if } \gamma = 0. \end{cases}$$

Hence, as $(-1/p_1) = -1$ and $(p_2/p_1) = (-p_1/p_2) = -1$, we have

$$\begin{cases} \left(\frac{R}{p_1}\right) = \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{L+\theta N}{p_1}\right) & \text{if } \beta = 0, \\ \left(\frac{S}{p_1}\right) = (-1)^{\alpha+1}\left(\frac{2}{p_1}\right)^{s+1}\left(\frac{L+\theta N}{p_1}\right) & \text{if } \gamma = 0. \end{cases}$$

Appealing to (3.J.17) when $\gamma = 0$, we see that

$$\left(\frac{R}{p_1}\right) = \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{L+\theta N}{p_1}\right) \tag{3.J.20}$$

in both cases. Then, from (3.J.14) and (3.J.20), we obtain

$$\left(\frac{R}{p_2}\right) = \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{L+\theta N}{p_1}\right). \tag{3.J.21}$$

Next we observe that

$$\begin{aligned} &(HC+KL)^2 - 2(HC+KL)KL \\ &\qquad = (HC+KL)(HC-KL) \\ &\qquad = p_1^{m_1-1}p_2^{m_2-1}(K^2N^2 - p_1p_2H^2B^2) && \text{(by (3.J.9))} \\ &\qquad \equiv 0 \pmod{p_2} && \text{(as } m_2 \geq 2\text{)}, \end{aligned}$$

so that

$$\left(\frac{2}{p_2}\right)\left(\frac{HC+KL}{p_2}\right)\left(\frac{K}{p_2}\right)\left(\frac{L}{p_2}\right) = 1.$$

From (3.J.10) we deduce (as $(p_1/p_2) = 1$)

$$\left(\frac{2}{p_2}\right)^{r+1}\left(\frac{R}{p_2}\right)\left(\frac{K}{p_2}\right)\left(\frac{L}{p_2}\right) = 1. \tag{3.J.22}$$

Then, from (3.J.21) and (3.J.22), we have

$$\left(\frac{2}{p_1p_2}\right)^{r+1}\left(\frac{K}{p_2}\right)\left(\frac{L}{p_2}\right)\left(\frac{L+\theta N}{p_1}\right)=1,$$

that is, by (3.J.18),

$$\left(\frac{K}{p_2}\right)=\left(\frac{2}{p_1p_2}\right)\left(\frac{L}{p_2}\right)\left(\frac{L+\theta N}{p_1}\right).$$

Now set $w\equiv(\theta+1)/2 \pmod{p_1}$ so that w is a solution of the congruence

$$\text{(3.J.23)}\qquad w^2-w+\tfrac{1}{4}(1+p_1^{m_1-1}p_2^{m_2-1})\equiv 0 \pmod{p_1}.$$

Then we have

$$\left(\frac{L+\theta N}{p_1}\right)=\left(\frac{2M+(1+\theta)N}{p_1}\right)=\left(\frac{2M+2wN}{p_1}\right)=\left(\frac{2}{p_1}\right)\left(\frac{M+wN}{p_1}\right)$$

and

$$\text{(3.J.24)}\qquad \left(\frac{K}{p_2}\right)=\left(\frac{2}{p_2}\right)\left(\frac{L}{p_2}\right)\left(\frac{M+wN}{p_1}\right).$$

Finally, noting from (3.J.23) that $2w\equiv 1 \pmod{p_1}$ when $m_1\ge 3$, we have

C_p is a fourth power in $H(-D)$

$$\Leftrightarrow \left(\frac{K}{p_1}\right)=\left(\frac{K}{p_2}\right)=1$$

$$\Leftrightarrow \left(\frac{K}{p_2}\right)=1 \qquad \text{(by (3.J.3))}$$

$$\Leftrightarrow \left(\frac{2}{p_2}\right)\left(\frac{L}{p_2}\right)\left(\frac{M+wN}{p_1}\right)=1 \qquad \text{(by (3.J.24))}$$

$$\Leftrightarrow \begin{cases} \left(\dfrac{M+wN}{p_1}\right)\left(\dfrac{4M+2N}{p_2}\right)=1 \\ \qquad\qquad \text{if } m_1=1, \text{ where } w^2-w+\frac{1}{4}(1+p_2^{m_2-1})\equiv 0 \pmod{p_1}, \\ \left(\dfrac{4M+2N}{p_1p_2}\right)=1 \ \text{ if } m_1\ge 3 \qquad\qquad \text{(by (3.J.4)).} \end{cases}$$

Case (K): $D=4p_1^{m_1}p_2^{m_2}$, $D^*=4p_1^{m_1}p_2^{m_2-1}$, m_1 (odd) ≥ 1, $m_2\ge 1$, $p_1\equiv 3 \pmod 4$, $p_2\equiv 1 \pmod 4$, $(p_1/p_2)=1$. Let p be an odd prime such that $(p/p_1)=(p/p_2)=1$, so that $p\ne p_1,p_2$. From (3.2) and (3.1) we have

$$\text{(3.K.1)}\qquad H^2p=M^2+p_1^{m_1}p_2^{m_2-1}N^2,\ H>0,\ (M,N)=1,\ (H,2pp_1p_2)=1,$$

$$\text{(3.K.2)}\qquad K^2p=A^2+p_1^{m_1}p_2^{m_2}B^2,\qquad K>0,\ (A,B)=1,\ (K,2pp_1p_2)=1.$$

From (3.3) we have $(-D/K) = (-4p_1^{m_1}p_2^{m_2}/K) = 1$, so that, by the law of quadratic reciprocity, we have

$$\left(\frac{K}{p_1}\right) = \left(\frac{K}{p_2}\right)^{m_2}. \tag{3.K.3}$$

From (3.K.1) and (3.K.2) we obtain

$$(HA + KM)(HA - KM) = p_1^{m_1}p_2^{m_2-1}(K^2N^2 - p_2H^2B^2). \tag{3.K.4}$$

By Lemma 3.6 neither p_1 nor p_2 divides both of $HA \pm KM$. By changing the sign of A if necessary, we may suppose that $p_2 \nmid HA + KM$. We define odd integers R and S by

$$R = (HA + KM)/2^r p_1^{\beta}, \qquad S = (HA - KM)/2^s p_2^{\alpha} p_1^{\gamma}, \tag{3.K.5}$$

where $p_2^{\alpha} \parallel HA - KM$, $p_1^{\beta} \parallel HA + KM$, $p_1^{\gamma} \parallel HA - KM$. We note from (3.K.4) and (3.K.5) that

$$\begin{cases} p_1 \nmid RS, \ p_2 \nmid RS, \\ \alpha \geq m_2 - 1 \geq 0, \ \beta + \gamma \geq m_1 \geq 1, \\ \min(\beta, \gamma) = 0. \end{cases}$$

Next we factor R into primes:

$$R = \varepsilon \prod_{(p_2/q_i)=1} q_i^{e_i} \prod_{(p_2/r_j)=-1} r_j^{f_j}, \tag{3.K.6}$$

where $\varepsilon = \pm 1$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. By (3.K.1), (3.K.2), (3.K.5), (3.K.6) and Lemma 3.5(ii) we see that each f_j in (3.K.6) is even. Hence, by the law of quadratic reciprocity, we have

$$\left(\frac{R}{p_2}\right) = \left(\frac{\varepsilon}{p_2}\right) \prod_{(p_2/q_i)=1} \left(\frac{q_i}{p_2}\right)^{e_i} = 1. \tag{3.K.7}$$

Now, by Lemma 3.1, we have

$$2(KM + HA)(KM + wKN) \equiv (KM + HA + wKN)^2 \pmod{p_2}, \tag{3.K.8}$$

where

$$w^2 \equiv -p_1^{m_1}p_2^{m_2-1} \pmod{p_2}. \tag{3.K.9}$$

Note from (3.K.9) that we may take $w = 0$ when $m_2 \geq 2$. When $m_2 = 1$, the congruence for w is solvable as $(-p_1^{m_1}/p_2) = (-p_1/p_2) = (p_1/p_2) = 1$. Then, from (3.K.5) and (3.K.8), we obtain

$$\left(\frac{2}{p_2}\right)^{r+1} \left(\frac{p_1}{p_2}\right)^{\beta} \left(\frac{R}{p_2}\right) \left(\frac{K}{p_2}\right) \left(\frac{M + wN}{p_2}\right) = 1. \tag{3.K.10}$$

Thus, as $(p_1/p_2) = (R/p_2) = 1$ (see (3.K.7)), we deduce from (3.K.10) that

$$\text{(3.K.11)} \qquad \left(\frac{K}{p_2}\right) = \left(\frac{2}{p_2}\right)^{r+1}\left(\frac{M+wN}{p_2}\right).$$

If $p_2 \equiv 1 \pmod 8$ then $(2/p_2) = 1$. If $p_2 \equiv 5 \pmod 8$ then, by Lemma 3.8 with $E = p_1^{m_1}p_2^{m_2} \equiv 3 \pmod 4$, $E^* = p_1^{m_1}p_2^{m_2-1} \equiv 3 \pmod 4$, $E/E^* = p_2 \equiv 5 \pmod 8$, r is odd so that $(2/p_2)^{r+1} = 1$. Hence (3.K.11) becomes

$$\text{(3.K.12)} \qquad \left(\frac{K}{p_2}\right) = \left(\frac{M+wN}{p_2}\right).$$

Finally,

C_p is a fourth power in $H(-D)$

$$\Leftrightarrow \left(\frac{K}{p_1}\right) = \left(\frac{K}{p_2}\right) = 1$$

$$\Leftrightarrow \left(\frac{K}{p_2}\right) = 1 \qquad \text{(by (3.K.3))}$$

$$\Leftrightarrow \left(\frac{M+wN}{p_2}\right) = 1 \qquad \text{(by (3.K.12))}$$

$$\Leftrightarrow \begin{cases} \left(\dfrac{M+wN}{p_2}\right) = 1 & \text{if } m_2 = 1, \text{ where } w^2 \equiv -p_1^{m_1} \pmod{p_2}, \\ \left(\dfrac{M}{p_2}\right) = 1 & \text{if } m_2 \geq 2 \end{cases} \qquad \text{(by (3.K.9))}.$$

Case (L): $D = 4p_1^{m_1}p_2^{m_2}$, $D^* = 4p_1^{m_1-1}p_2^{m_2-1}$, m_1 (odd) ≥ 1, m_2 (even) ≥ 2, $p_1 \equiv p_2 \equiv 3 \pmod 4$, $(p_1/p_2) = 1$. Let p be an odd prime such that $(p/p_1) = (p/p_2) = 1$, so that $p \neq p_1, p_2$. From (3.2) and (3.1), we have

$$\text{(3.L.1)} \quad H^2p = M^2 + p_1^{m_1-1}p_2^{m_2-1}N^2,\ H > 0,\ (M,N) = 1,\ (H, 2pp_1p_2) = 1,$$

$$\text{(3.L.2)} \quad K^2p = A^2 + p_1^{m_1}p_2^{m_2}B^2,\ K > 0,\ (A,B) = 1,\ (K, 2pp_1p_2) = 1.$$

From (3.3) we have $(-D/K) = (-4p_1^{m_1}p_2^{m_2}/K) = 1$, so that, by the law of quadratic reciprocity, we have

$$\text{(3.L.3)} \qquad \left(\frac{K}{p_1}\right) = 1.$$

From (3.L.1) and (3.L.2) we have

$$\text{(3.L.4)} \quad (HA + KM)(HA - KM) = p_1^{m_1-1}p_2^{m_2-1}(K^2N^2 - p_1p_2H^2B^2).$$

By Lemma 3.6 neither p_1 nor p_2 divides both of $HA \pm KM$. By changing the sign of A if necessary, we may suppose that $p_2 \nmid HA + KM$. We define odd integers R and S by

$$R = (HA + KM)/2^r p_1^{\alpha}, \qquad S = (HA - KM)/2^s p_1^{\beta} p_2^{\gamma}, \tag{3.L.5}$$

where $p_1^{\alpha} \parallel HA + KM$, $p_1^{\beta} \parallel HA - KM$, $p_2^{\gamma} \parallel HA - KM$. We observe that

$$\begin{cases} p_1 \nmid RS,\ p_2 \nmid RS, \\ \alpha + \beta \geq m_1 - 1 \geq 0,\ \gamma \geq m_2 - 1 \geq 1, \\ \min(\alpha, \beta) = 0. \end{cases} \tag{3.L.6}$$

Proceeding as in Case (J) (proof of (3.J.16)) with roles of p_1 and p_2 reversed, we obtain

$$\left(\frac{R}{p_1}\right)\left(\frac{S}{p_1}\right) = \left(\frac{2}{p_1}\right)^{r+s} (-1)^{\gamma+1}. \tag{3.L.7}$$

Next we factor R into primes:

$$R = \varepsilon \prod_{(p_1p_2/q_i)=1} q_i^{e_i} \prod_{(p_1p_2/r_j)=-1} r_j^{f_j}, \tag{3.L.8}$$

where $\varepsilon = \pm 1$, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. By Lemma 3.5(ii) each f_j is even. Hence from (3.L.8) we have

$$\left(\frac{R}{p_1}\right) = \left(\frac{\varepsilon}{p_1}\right) \prod_{(p_1p_2/q_i)=1} \left(\frac{q_i}{p_1}\right)^{e_i}, \qquad \left(\frac{R}{p_2}\right) = \left(\frac{\varepsilon}{p_2}\right) \prod_{(p_1p_2/q_i)=1} \left(\frac{q_i}{p_2}\right)^{e_i}.$$

As

$$\left(\frac{p_1p_2}{q_i}\right) = 1 \Rightarrow \left(\frac{-p_1}{q_i}\right) = \left(\frac{-p_2}{q_i}\right) \Rightarrow \left(\frac{q_i}{p_1}\right) = \left(\frac{q_i}{p_2}\right)$$

and

$$\left(\frac{\varepsilon}{p_1}\right) = \left(\frac{\varepsilon}{p_2}\right) = \varepsilon,$$

we deduce that

$$\left(\frac{R}{p_1}\right) = \left(\frac{R}{p_2}\right). \tag{3.L.9}$$

Next, by Lemma 3.1, we have

$$2(KM \pm HA)(KM + wKN) \equiv (KM \pm HA + wKN)^2 \pmod{p_1}, \tag{3.L.10}$$

where w is a solution of the congruence

$$w^2 \equiv -p_1^{m_1-1} p_2^{m_2-1} \pmod{p_1}. \tag{3.L.11}$$

Note that we may take $w = 0$ when $m_1 \geq 3$. When $m_1 = 1$ the congruence (3.L.11) is solvable as

$$\left(\frac{-p_2^{m_2-1}}{p_1}\right) = \left(\frac{-p_2}{p_1}\right) = \left(\frac{p_1}{p_2}\right) = 1.$$

From (3.L.10) we obtain

$$\left(\frac{2}{p_1}\right)\left(\frac{KM \pm HA}{p_1}\right)\left(\frac{K}{p_1}\right)\left(\frac{M+wN}{p_1}\right) = 1.$$

Recall by (3.L.6) that either $\alpha = 0$ or $\beta = 0$. Taking the + sign in the above equation if $\alpha = 0$ and the $-$ sign if $\beta = 0$, we derive, using (3.L.3) and (3.L.5),

$$\text{(3.L.12)}\qquad \begin{cases} \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{R}{p_1}\right) = \left(\frac{M+wN}{p_1}\right) & \text{if } \alpha = 0, \\ -\left(\frac{2}{p_1}\right)^{s+1}\left(\frac{p_2}{p_1}\right)^{\gamma}\left(\frac{S}{p_1}\right) = \left(\frac{M+wN}{p_1}\right) & \text{if } \beta = 0. \end{cases}$$

Appealing to (3.L.7) in the case $\beta = 0$, we see from (3.L.12) that in both cases we have

$$\text{(3.L.13)}\qquad \left(\frac{R}{p_1}\right) = \left(\frac{2}{p_1}\right)^{r+1}\left(\frac{M+wN}{p_1}\right).$$

Further, by (3.L.4), we have (as $m_2 \ge 2$)

$$2(HA+KM)KM \equiv (HA+KM)^2 \pmod{p_2},$$

so that

$$\left(\frac{2}{p_2}\right)\left(\frac{HA+KM}{p_2}\right)\left(\frac{K}{p_2}\right)\left(\frac{M}{p_2}\right) = 1.$$

Then, appealing to (3.L.5), we obtain

$$\left(\frac{2}{p_2}\right)^{r+1}\left(\frac{p_1}{p_2}\right)^{\alpha}\left(\frac{R}{p_2}\right)\left(\frac{K}{p_2}\right)\left(\frac{M}{p_2}\right) = 1,$$

so that (as $(p_1/p_2) = 1$ and $(R/p_1) = (R/p_2)$, see (3.L.9)) we have

$$\left(\frac{K}{p_2}\right) = \left(\frac{2}{p_2}\right)^{r+1}\left(\frac{M}{p_2}\right)\left(\frac{R}{p_1}\right),$$

and thus by (3.L.13),

$$\left(\frac{K}{p_2}\right) = \left(\frac{2}{p_1p_2}\right)^{r+1}\left(\frac{M}{p_2}\right)\left(\frac{M+wN}{p_1}\right).$$

If $p_1p_2 \equiv 1 \pmod 8$ then $(2/p_1p_2) = 1$. If $p_1p_2 \equiv 5 \pmod 8$ then, by Lemma 3.8 with $E = p_1^{m_1}p_2^{m_2} \equiv 3 \pmod 4$, $E^* = p_1^{m_1-1}p_2^{m_2-1} \equiv 3 \pmod 4$, $E/E^* = p_1p_2 \equiv 5 \pmod 8$, r is odd, so that $(2/p_1p_2)^{r+1} = 1$. Hence we have

$$\text{(3.L.14)}\qquad \left(\frac{K}{p_2}\right) = \left(\frac{M+wN}{p_1}\right)\left(\frac{M}{p_2}\right).$$

Finally,

$$\begin{aligned}
&C_p \text{ is a fourth power in } H(-D)\\
&\Leftrightarrow \left(\frac{K}{p_1}\right) = \left(\frac{K}{p_2}\right) = 1\\
&\Leftrightarrow \left(\frac{K}{p_2}\right) = 1 \qquad\qquad\qquad \text{(by (3.L.3))}\\
&\Leftrightarrow \left(\frac{M+wN}{p_1}\right)\left(\frac{M}{p_2}\right) = 1 \quad \text{(by (3.L.14))}\\
&\Leftrightarrow \begin{cases} \left(\dfrac{M+wN}{p_1}\right)\left(\dfrac{M}{p_2}\right) = 1, & \text{if } m_1 = 1, \text{ where } w^2 \equiv -p_2^{m_2-1} \pmod{p_1},\\ \left(\dfrac{M}{p_1p_2}\right) = 1 & \text{if } m_1 \geq 3 \qquad\qquad \text{(by (3.L.14)).} \ \blacksquare \end{cases}
\end{aligned}$$

4. Predictive criteria when $H(-D) \simeq Z_4$. The class number 4 problem for imaginary quadratic fields was solved by Steven Arno [1]. It can be deduced from this work that there are exactly fifty values of D (> 0) for which $H(-D) \simeq Z_4$. For these values of D, we tabulate (pp. 266–269) the predictive criteria given by Theorem 2 with specific numerical values for H and w. For some discriminants the criterion can be simplified, for example by removing a quadratic residue from a Legendre symbol or by writing the product of two Jacobi symbols as one. For example the latter is possible when $D = 63$, as

$$\begin{aligned}
\left(\frac{M+3N}{7}\right)\left(\frac{4M+2N}{3}\right) &= \left(\frac{M-4N}{7}\right)\left(\frac{M-4N}{3}\right)\\
&= \left(\frac{M-4N}{21}\right).
\end{aligned}$$

For these fifty values of D the predictive criterion determines which form class represents the prime p as the principal genus contains exactly two form classes. For most of these, the predictive criterion is already known, and a reference is given.

The fifty discriminants in the table include representatives of all cases except (F). We conclude this section with an example illustrating case (F).

Example. $D = 392$, $D^* = 28$. Here $h(-392) = 8$, $h(-28) = 1$. The principal genus of discriminant -392 contains the four form classes $[1, 0, 98]$, $[2, 0, 49]$, $[9, \pm 2, 11]$, of which the first two are fourth powers and the other two are not (see the table on p. 270).

D	D^*	p	Representation of p with $(M,N)=1$	Predictive criterion	Case	Ref.
39	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{13}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+10Y^2 \Leftrightarrow \left(\frac{M+4N}{13}\right)=1$	I	[13]
55	11	$\left(\frac{p}{5}\right)=\left(\frac{p}{11}\right)=1$	$p=M^2+MN+3N^2$	$p=X^2+XY+14Y^2 \Leftrightarrow \left(\frac{M+2N}{5}\right)=1$	I	[13]
56	28	$\left(\frac{2}{p}\right)=\left(\frac{p}{7}\right)=1$	$p=M^2+7N^2$	$p=X^2+14Y^2 \Leftrightarrow \left(\frac{2}{M+3N}\right)=1$	E	[15], [13]
63	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{7}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+16Y^2 \Leftrightarrow \left(\frac{M-4N}{21}\right)=1$	J	
68	4	$\left(\frac{-1}{p}\right)=\left(\frac{p}{17}\right)=1$	$p=M^2+N^2$	$p=X^2+17Y^2 \Leftrightarrow \left(\frac{M+4N}{17}\right)=1$	B	[3]
80	16	$\left(\frac{-1}{p}\right)=\left(\frac{p}{5}\right)=1$	$p=M^2+4N^2$	$p=X^2+20Y^2 \Leftrightarrow \left(\frac{M+N}{5}\right)=1$	G	[16]
128	64	$\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=1$	$p=M^2+16N^2$	$p=X^2+32Y^2 \Leftrightarrow \left(\frac{2}{M+4N}\right)=1$	A	[2]
136	8	$\left(\frac{-2}{p}\right)=\left(\frac{p}{17}\right)=1$	$p=M^2+2N^2$	$p=X^2+34Y^2 \Leftrightarrow \left(\frac{M+7N}{17}\right)=1$	D	[15], [13]
144	48	$\left(\frac{-1}{p}\right)=\left(\frac{p}{3}\right)=1$	$p=M^2+12N^2$	$p=X^2+36Y^2 \Leftrightarrow \left(\frac{-1}{M+2N}\right)\left(\frac{M}{3}\right)=1$	H	
155	31	$\left(\frac{p}{5}\right)=\left(\frac{p}{31}\right)=1$	$H^2p=M^2+MN+8N^2$ $H=1,7$	$p=X^2+XY+39Y^2 \Leftrightarrow \left(\frac{M+2N}{5}\right)=1$	I	[13]
156	12	$\left(\frac{p}{3}\right)=\left(\frac{p}{13}\right)=1$	$p=M^2+3N^2$	$p=X^2+39Y^2 \Leftrightarrow \left(\frac{M+6N}{13}\right)=1$	K	[15]
171	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{19}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+43Y^2 \Leftrightarrow \left(\frac{M+8N}{57}\right)=1$	J	
184	92	$\left(\frac{2}{p}\right)=\left(\frac{p}{23}\right)=1$	$H^2p=M^2+23N^2$ $H=1,3$	$p=X^2+46Y^2 \Leftrightarrow \left(\frac{2}{M+3N}\right)=1$	E	[15] [13]
196	28	$\left(\frac{-1}{p}\right)=\left(\frac{p}{7}\right)=1$	$p=M^2+7N^2$	$p=X^2+49Y^2 \Leftrightarrow (-1)^{(M-1+N)/2}\left(\frac{M}{7}\right)=1$	C	

D	D^*	p	Representation of p with $(M,N)=1$	Predictive criterion	Case	Ref.
203	7	$\left(\frac{p}{7}\right)=\left(\frac{p}{29}\right)=1$	$p=M^2+MN+2N^2$	$p=X^2+XY+51Y^2 \Leftrightarrow \left(\frac{M+8N}{29}\right)=1$	I	[13]
208	16	$\left(\frac{-1}{p}\right)=\left(\frac{p}{13}\right)=1$	$p=M^2+4N^2$	$p=X^2+52Y^2 \Leftrightarrow \left(\frac{M+3N}{13}\right)=1$	G	
219	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{73}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+55Y^2 \Leftrightarrow \left(\frac{M+9N}{73}\right)=1$	I	[13]
220	44	$\left(\frac{p}{5}\right)=\left(\frac{p}{11}\right)=1$	$H^2p=M^2+11N^2$ $H=1,3$	$p=X^2+55Y^2 \Leftrightarrow \left(\frac{M+2N}{5}\right)=1$	K	[15]
252	12	$\left(\frac{p}{3}\right)=\left(\frac{p}{7}\right)=1$	$p=M^2+3N^2$	$p=X^2+63Y^2 \Leftrightarrow \left(\frac{M+9N}{21}\right)=1$	L	
256	128	$\left(\frac{-1}{p}\right)=\left(\frac{2}{p}\right)=1$	$H^2p=M^2+32N^2$ $H=1,3$	$p=X^2+64Y^2 \Leftrightarrow \left(\frac{2}{M}\right)=1$	A	
259	7	$\left(\frac{p}{7}\right)=\left(\frac{p}{37}\right)=1$	$p=M^2+MN+2N^2$	$p=X^2+XY+65Y^2 \Leftrightarrow \left(\frac{M+9N}{37}\right)=1$	I	[13]
275	55	$\left(\frac{p}{5}\right)=\left(\frac{p}{11}\right)=1$	$H^2p=M^2+MN+14N^2$ $H=1,7$	$p=X^2+XY+69Y^2 \Leftrightarrow \left(\frac{M-2N}{5}\right)=1$	I	[13]
291	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{97}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+73Y^2 \Leftrightarrow \left(\frac{M+36N}{97}\right)=1$	I	[13]
292	4	$\left(\frac{-1}{p}\right)=\left(\frac{p}{73}\right)=1$	$p=M^2+N^2$	$p=X^2+73Y^2 \Leftrightarrow \left(\frac{M+27N}{73}\right)=1$	B	[13]
323	19	$\left(\frac{p}{17}\right)=\left(\frac{p}{19}\right)=1$	$p=M^2+MN+5N^2$	$p=X^2+XY+81Y^2 \Leftrightarrow \left(\frac{M+4N}{17}\right)=1$	I	[13]
328	8	$\left(\frac{-2}{p}\right)=\left(\frac{p}{41}\right)=1$	$p=M^2+2N^2$	$p=X^2+82Y^2 \Leftrightarrow \left(\frac{M+11N}{41}\right)=1$	D	[15], [13]
355	71	$\left(\frac{p}{5}\right)=\left(\frac{p}{71}\right)=1$	$H^2p=M^2+MN+18N^2$ $H=1,3,9,27$	$p=X^2+XY+89Y^2 \Leftrightarrow \left(\frac{M+2N}{5}\right)=1$	I	[13]

D	D^*	p	Representation of p with $(M,N)=1$	Predictive criterion	Case	Ref.
363	11	$\left(\frac{p}{3}\right)=\left(\frac{p}{11}\right)=1$	$p=M^2+MN+3N^2$	$p=X^2+XY+91Y^2 \Leftrightarrow \left(\frac{M+6N}{33}\right)=1$	J	
387	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{43}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+97Y^2 \Leftrightarrow \left(\frac{M+50N}{129}\right)=1$	J	
388	4	$\left(\frac{-1}{p}\right)=\left(\frac{p}{97}\right)=1$	$p=M^2+N^2$	$p=X^2+97Y^2 \Leftrightarrow \left(\frac{M+22N}{97}\right)=1$	B	[13]
400	80	$\left(\frac{-1}{p}\right)=\left(\frac{p}{5}\right)=1$	$H^2p=M^2+20N^2$ $H=1,3$	$p=X^2+100Y^2 \Leftrightarrow \left(\frac{M}{5}\right)=1$	G	
475	95	$\left(\frac{p}{5}\right)=\left(\frac{p}{19}\right)=1$	$H^2p=M^2+MN+24N^2$ $H=1,3,9$	$p=X^2+XY+119Y^2 \Leftrightarrow \left(\frac{M-2N}{5}\right)=1$	I	[13]
507	39	$\left(\frac{p}{3}\right)=\left(\frac{p}{13}\right)=1$	$H^2p=M^2+MN+10N^2$ $H=1,5$	$p=X^2+XY+127Y^2 \Leftrightarrow \left(\frac{M-6N}{13}\right)=1$	I	[13]
568	284	$\left(\frac{2}{p}\right)=\left(\frac{p}{71}\right)=1$	$H^2p=M^2+71N^2$ $H=1,3,5,9$	$p=X^2+142Y^2 \Leftrightarrow \left(\frac{2}{M+3N}\right)=1$	E	[15] [13]
592	16	$\left(\frac{-1}{p}\right)=\left(\frac{p}{37}\right)=1$	$p=M^2+4N^2$	$p=X^2+148Y^2 \Leftrightarrow \left(\frac{M+12N}{37}\right)=1$	G	
603	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{67}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+151Y^2 \Leftrightarrow \left(\frac{M-37N}{201}\right)=1$	J	
667	23	$\left(\frac{p}{23}\right)=\left(\frac{p}{29}\right)=1$	$H^2p=M^2+MN+6N^2$ $H=1,3$	$p=X^2+XY+167\ Y^2 \Leftrightarrow \left(\frac{M+11N}{29}\right)=1$	I	[13]
723	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{241}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+181Y^2 \Leftrightarrow \left(\frac{M+16N}{241}\right)=1$	I	[13]
763	7	$\left(\frac{p}{7}\right)=\left(\frac{p}{109}\right)=1$	$p=M^2+MN+2N^2$	$p=X^2+XY+191Y^2 \Leftrightarrow \left(\frac{M+30N}{109}\right)=1$	I	[13]

D	D^*	p	Representation of p with $(M,N)=1$	Predictive criterion	Case	Ref.
772	4	$\left(\frac{-1}{p}\right)=\left(\frac{p}{193}\right)=1$	$p=M^2+N^2$	$p=X^2+193Y^2 \Leftrightarrow \left(\frac{M+81N}{193}\right)=1$	B	[13]
955	191	$\left(\frac{p}{5}\right)=\left(\frac{p}{191}\right)=1$	$H^2p=M^2+MN+48N^2$ $H=1,3,9,13,17,27,39$	$p=X^2+XY+239Y^2 \Leftrightarrow \left(\frac{M+2N}{5}\right)=1$	I	[13]
1003	59	$\left(\frac{p}{17}\right)=\left(\frac{p}{59}\right)=1$	$H^2p=M^2+MN+15N^2$ $H=1,3$	$p=X^2+XY+251Y^2 \Leftrightarrow \left(\frac{M+2N}{17}\right)=1$	I	[13]
1027	79	$\left(\frac{p}{13}\right)=\left(\frac{p}{79}\right)=1$	$H^2p=M^2+MN+20N^2$ $H=1,5,11$	$p=X^2+XY+257Y^2 \Leftrightarrow \left(\frac{M+3N}{13}\right)=1$	I	[13]
1227	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{409}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+307Y^2 \Leftrightarrow \left(\frac{M+54N}{409}\right)=1$	I	[13]
1243	11	$\left(\frac{p}{11}\right)=\left(\frac{p}{113}\right)=1$	$p=M^2+MN+3N^2$	$p=X^2+XY+311Y^2 \Leftrightarrow \left(\frac{M+11N}{113}\right)=1$	I	[13]
1387	19	$\left(\frac{p}{19}\right)=\left(\frac{p}{73}\right)=1$	$p=M^2+MN+5N^2$	$p=X^2+XY+347Y^2 \Leftrightarrow \left(\frac{M+23N}{73}\right)=1$	I	[13]
1411	83	$\left(\frac{p}{17}\right)=\left(\frac{p}{83}\right)=1$	$H^2p=M^2+MN+21N^2$ $H=1,3$	$p=X^2+XY+353Y^2 \Leftrightarrow \left(\frac{M+6N}{17}\right)=1$	I	[13]
1467	3	$\left(\frac{p}{3}\right)=\left(\frac{p}{163}\right)=1$	$p=M^2+MN+N^2$	$p=X^2+XY+367Y^2 \Leftrightarrow \left(\frac{M+59N}{489}\right)=1$	J	
1507	11	$\left(\frac{p}{11}\right)=\left(\frac{p}{137}\right)=1$	$p=M^2+MN+3N^2$	$p=X^2+XY+377Y^2 \Leftrightarrow \left(\frac{M+59N}{137}\right)=1$	I	[13]
1555	311	$\left(\frac{p}{5}\right)=\left(\frac{p}{311}\right)=1$	$H^2p=M^2+MN+78N^2$ $H=1,3,7,9,13,21,39,53,63$	$p=X^2+XY+389Y^2 \Leftrightarrow \left(\frac{M+2N}{5}\right)=1$	I	[13]

$p = M^2 + 7N^2$			$(-1)^N\left(\frac{-2}{M+N}\right)\left(\frac{M}{7}\right)$	Representation of p by a form of discriminant -392
p	M	N		
11	2	1	-1	$11 = 9 \cdot 0^2 + 2 \cdot 0 \cdot 1 + 11 \cdot 1^2$
43	6	1	-1	$43 = 9 \cdot 2^2 + 2 \cdot 2(-1) + 11(-1)^2$
67	2	3	$+1$	$67 = 2 \cdot 3^2 + 49 \cdot 1^2$
107	10	1	$+1$	$107 = 3^2 + 98 \cdot 1^2$

5. Successive predictions. If the pair of discriminants (D, D^*) meets the conditions of one of the six cases (A), (B), (D), (G), (I), (K) studied in Theorem 2, then the pair $(\lambda D, D)$ (where $\lambda = D/D^*$) also satisfies the conditions of the same case. For these six cases we can apply Theorem 2 t times to determine whether or not a form class in the principal genus of $H(-\lambda^t d)$ representing p is a fourth power.

For example consider case (G) with $p_1 = 5$, and take $p = 29$. We use Theorem 2 three times to determine whether a form class in $H(-16 \cdot 5^3) = H(-2000)$ representing 29 is a fourth power or not. From $29 = 5^2 + 4 \cdot 1^2$, $((5 + 1 \cdot 1)/5) = 1$ ($w = 1$ is a solution of $w^2 \equiv -4 \pmod 5$), we see that 29 is represented by the form $x^2 + 20y^2$, as the form class $[1, 0, 20]$ is the only fourth power in $H(-16 \cdot 5) = H(-80)$. Indeed $29 = 3^2 + 20 \cdot 1^2$. Now $(3/5) = -1$, so that 29 is represented by the form $4x^2 + 25y^2$, as the form class $[4, 0, 25]$ is the only square which is not a fourth power in $H(-16 \cdot 5^2) = H(-400)$. Indeed, $29 = 4 \cdot 1^2 + 25 \cdot 1^2$. In order to continue we must determine a positive integer H coprime with $2 \cdot 5 \cdot 29$ such that $29H^2$ is represented by the form $x^2 + 100y^2$. As $[8, \pm 4, 13]$ are the two form classes in the non-principal genus of $H(-400)$, a suitable choice is $H = 13$. We find $13^2 \cdot 29 = 1^2 + 100 \cdot 7^2$. Now $(1/5) = 1$, so that 29 is represented by one or two of the forms $x^2 + 500y^2$, $21x^2 \pm 10xy + 25y^2$, $24x^2 \pm 20xy + 25y^2$, as the form classes corresponding to these forms are precisely those which are fourth powers in $H(-16 \cdot 5^3) = H(-2000)$. However, Theorem 2 does not tell us which of these forms actually represent 29.

Once it has been determined, by Theorem 2 or otherwise, whether a form class in the principal genus of discriminant $-D$ representing p is a fourth power or not, Theorem 3 tells us how to determine directly whether a form class in the principal genus of discriminant $-\lambda^t D$ representing p is a fourth power or not, without determining the sequence of representations of p needed to apply Theorem 2.

THEOREM 3. *Let p be an odd prime such that $\chi_1(p) = \chi_2(p) = 1$, where χ_1, χ_2 are defined at the beginning of Section* 3. *Let (D, D^*) be a pair of discriminants as defined in cases* (A), (B), (D), (G), (I), (K) *of Theorem* 2. *Set $\lambda = D/D^*$. For $t = 0, 1, 2, \ldots$ let $C_p(t)$ denote a form class of $H(-\lambda^t D)$*

which represents p. Define the character

$$\Psi_p(t)=\begin{cases}1 & \textit{if } C_p(t) \textit{ is a fourth power in } H(-\lambda^t D),\\ -1 & \textit{if } C_p(t) \textit{ is a square but not a}\\ & \textit{fourth power in } H(-\lambda^t D).\end{cases}$$

Then

$$\frac{\Psi_p(t)}{\Psi_p(0)}=\begin{cases}(-1)^{t(p-1)/8} & \textit{in case } \text{(A)}, \textit{ where } m\ge 7,\\ \left(\dfrac{p}{p_1}\right)_4^t & \textit{in cases } \text{(B), (D), (G)}, \textit{ where } m_1\ge 1,\\ \left(\dfrac{p}{p_2}\right)_4^t & \textit{in cases } \text{(I), (K)}, \textit{ where } m_2\ge 1.\end{cases}$$

Proof. Case (A). Let $D=2^m$, $m\ge 7$, and let t denote a positive integer. As $(-1/p)=(2/p)=1$, applying (3.2) with discriminant $-2^{t+m-1}=-2^{t-1}D$ shows that there are integers H, M, N such that

$$H^2p=M^2+2^{t+m-3}N^2,\qquad H>0,\ (M,N)=1,\ (H,2p)=1. \tag{5.1}$$

By (3.3) we have $(-2^{t+m-1}/H)=1$ so that

$$\left(\frac{-1}{H}\right)=\left(\frac{2}{H}\right)^{t+m-1}. \tag{5.2}$$

Reducing (5.1) modulo 16, we obtain, as $t+m-3>m-3\ge 4$,

$$H^2p\equiv M^2 \pmod{16}. \tag{5.3}$$

By Theorem 2 (Case (A)),

$C_p(t)$ is a fourth power in $H(-2^tD)$
$\Leftrightarrow$ $(2/M)=1$
$\Leftrightarrow$ $M\equiv\pm1 \pmod 8$
$\Leftrightarrow$ $M^2\equiv 1 \pmod{16}$
$\Leftrightarrow$ $H^2p\equiv 1 \pmod{16}$ (by (5.3))
$\Leftrightarrow$ $H\equiv\pm1 \pmod 8$, $p\equiv 1 \pmod{16}$ or
$H\equiv\pm3 \pmod 8$, $p\equiv 9 \pmod{16}$
$\Leftrightarrow$ $(2/H)=1$, $p\equiv 1 \pmod{16}$ or $(2/H)=-1$, $p\equiv 9 \pmod{16}$
$\Leftrightarrow$ (by (5.2)) H is represented by a square in $H(-2^{t-1}D)$ if $p\equiv 1 \pmod{16}$, or H is not represented by a square in $H(-2^{t-1}D)$ if $p\equiv 9 \pmod{16}$
$\Leftrightarrow$ p is represented by a fourth power in $H(-2^{t-1}D)$ if $p\equiv 1 \pmod{16}$, or p is represented by a square which is not a fourth power in $H(-2^{t-1}D)$ if $p\equiv 9 \pmod{16}$
$\Leftrightarrow$ $C_p(t-1)$ is a fourth power in $H(-2^{t-1}D)$ if $p\equiv 1 \pmod{16}$, or $C_p(t-1)$ is a square but not a fourth power in $H(-2^{t-1}D)$ if $p\equiv 9 \pmod{16}$,

and thus

$$\begin{aligned}\Psi_p(t)=1 \Leftrightarrow \Psi_p(t-1)&=1,\ p\equiv 1 \pmod{16} \text{ or}\\ \Psi_p(t-1)&=-1,\ p\equiv 9 \pmod{16}\\ \Leftrightarrow \Psi_p(t-1)&=(-1)^{(p-1)/8}.\end{aligned}$$

Hence we have

$$\Psi_p(t)=(-1)^{(p-1)/8}\Psi_p(t-1) \qquad (t\ge 1)$$

and so

$$\Psi_p(t)=(-1)^{t(p-1)/8}\Psi_p(0) \qquad (t\ge 0).$$

Cases (B), (D), (G). Let $D=2^\mu p_1^{m_1}$, where $m_1\ge 1$,

$$\mu=\begin{cases}2, & \text{case (B)},\\ 3, & \text{case (D)},\\ 4, & \text{case (G)},\end{cases}$$

and

$$\begin{cases}p_1 \text{ (prime)} \equiv 1 \pmod 8, & \text{cases (B), (D)},\\ p_1 \text{ (prime)} \equiv 1 \pmod 4, & \text{case (G)}.\end{cases}$$

Here

$$\chi_1(r)=\left(\frac{-2^\mu}{r}\right), \qquad \chi_2(r)=\left(\frac{r}{p_1}\right).$$

Let t denote a positive integer. As $\chi_1(p)=\chi_2(p)=1$, from (3.2) with discriminant $-p_1^{t-1}D$, there exist integers H, M, N such that

(5.4) $$H^2p=M^2+(p_1^{t-1}D/4)N^2, \qquad H>0,\ (M,N)=1,\ (H,2pp_1)=1.$$

By (3.3) and the law of quadratic reciprocity, we have

$$\begin{aligned}1=\left(\frac{-p_1^{t-1}D}{H}\right)&=\left(\frac{-2^\mu p_1^{t+m_1-1}}{H}\right)\\ &=\chi_1(H)\left(\frac{p_1}{H}\right)^{t+m_1-1}=\chi_1(H)\left(\frac{H}{p_1}\right)^{t+m_1-1},\end{aligned}$$

that is,

(5.5) $$\chi_1(H)=\chi_2(H)^{t+m_1-1}.$$

From (5.4) we have

$$H^2p\equiv M^2 \pmod{p_1},$$

so that

(5.6) $$\left(\frac{H}{p_1}\right)\left(\frac{p}{p_1}\right)_4=\left(\frac{M}{p_1}\right).$$

By Theorem 2 (cases (B), (D), (G)),

$C_p(t)$ is a fourth power in $H(-p_1^tD)$

$\Leftrightarrow \left(\dfrac{M}{p_1}\right) = 1$

$\Leftrightarrow \left(\dfrac{H}{p_1}\right)\left(\dfrac{p}{p_1}\right)_4 = 1 \quad$ (by (5.6))

$\Leftrightarrow \left(\dfrac{p}{p_1}\right)_4 = 1$, $\chi_2(H) = 1$ or $\left(\dfrac{p}{p_1}\right)_4 = -1$, $\chi_2(H) = -1$

$\Leftrightarrow$ (by (5.5)) H is represented by a square in $H(-p_1^{t-1}D)$ if $(p/p_1)_4 = 1$, or H is not represented by a square in $H(-p_1^{t-1}D)$ if $(p/p_1)_4 = -1$

$\Leftrightarrow$ p is represented by a fourth power in $H(-p_1^{t-1}D)$ if $(p/p_1)_4 = 1$, or p is represented by a square which is not a fourth power in $H(-p_1^{t-1}D)$ if $(p/p_1)_4 = -1$

$\Leftrightarrow$ $C_p(t-1)$ is a fourth power in $H(-p_1^{t-1}D)$ if $(p/p_1)_4 = 1$, or $C_p(t-1)$ is a square but not a fourth power in $H(-p_1^{t-1}D)$ if $(p/p_1)_4 = -1$,

and thus

$$\begin{aligned}\Psi_p(t) = 1 \Leftrightarrow \Psi_p(t-1) = 1,\ &\left(\frac{p}{p_1}\right)_4 = 1 \text{ or}\\ \Psi_p(t-1) = -1,\ &\left(\frac{p}{p_1}\right)_4 = -1\\ \Leftrightarrow \Psi_p(t-1) = &\left(\frac{p}{p_1}\right)_4.\end{aligned}$$

Hence we have

$$\Psi_p(t) = \left(\frac{p}{p_1}\right)_4 \Psi_p(t-1) \quad (t \ge 1)$$

and so

$$\Psi_p(t) = \left(\frac{p}{p_1}\right)_4^t \Psi_p(0) \quad (t \ge 0).$$

Case (I). Let $D = p_1^{m_1}p_2^{m_2}$, m_1 (odd) ≥ 1, $m_2 \ge 1$, $p_1 \equiv 3 \pmod 4$, $p_2 \equiv 1 \pmod 4$, $(p_1/p_2) = 1$. Let t denote a positive integer. As $(p/p_1) = (p/p_2) = 1$, from (3.2) with discriminant $-p_2^{t-1}D$, there exist integers H, M, N such that

$$(5.7) \qquad H^2p = M^2 + MN + \tfrac{1}{4}(1 + p_1^{m_1}p_2^{t+m_2-1})N^2, \\ H > 0,\ (M,N) = 1, (H, 2pp_1p_2) = 1.$$

By (3.3) we have

$$1 = \left(\frac{-p_2^{t-1}D}{H}\right) = \left(\frac{-p_1^{m_1}p_2^{t+m_2-1}}{H}\right) = \left(\frac{-p_1p_2^{t+m_2-1}}{H}\right)$$

$$= \left(\frac{-p_1}{H}\right)\left(\frac{p_2}{H}\right)^{t+m_2-1} = \left(\frac{H}{p_1}\right)\left(\frac{H}{p_2}\right)^{t+m_2-1},$$

so that

$$\left(\frac{H}{p_1}\right) = \left(\frac{H}{p_2}\right)^{t+m_2-1}.$$

From (5.7) we have

$$16H^2p = (4M+2N)^2 + 4p_1^{m_1}p_2^{t+m_2-1}N^2.$$

Hence $2^4H^2p \equiv (4M+2N)^2 \pmod{p_2}$ so that

$$\left(\frac{H}{p_2}\right)\left(\frac{p}{p_2}\right)_4 = \left(\frac{4M+2N}{p_2}\right).$$

The rest of the proof now proceeds as in the previous cases.

Case (K). Let $D = 4p_1^{m_1}p_2^{m_2}$, m_1 (odd) ≥ 1, $m_2 \geq 1$, $p_1 \equiv 3 \pmod 4$, $p_2 \equiv 1 \pmod 4$, $(p_1/p_2) = 1$. Let t denote a positive integer. As $(p/p_1) = (p/p_2) = 1$, from (3.2) with discriminant $-p_2^{t-1}D$, there exist integers H, M, N such that

(5.8) $H^2p = M^2 + (p_2^{t-1}D/4)N^2, \qquad H > 0,\ (M,N) = 1,\ (H, 2pp_1p_2) = 1.$

Appealing to (3.3), we obtain as in Case (I),

$$\left(\frac{H}{p_1}\right) = \left(\frac{H}{p_2}\right)^{t+m_2-1}.$$

From (5.8) we have $H^2p \equiv M^2 \pmod{p_2}$ so that

$$\left(\frac{H}{p_2}\right)\left(\frac{p}{p_2}\right)_4 = \left(\frac{M}{p_2}\right).$$

The rest of the proof now proceeds as in the previous cases. ∎

Returning to the example discussed at the beginning of this section, as 29 is represented by the principal form of discriminant -80 $(29 = 3^2 + 20 \cdot 1^2)$, $\Psi_{29}(0) = 1$. Then, by Theorem 3, for $t \geq 0$ we have

$$\Psi_{29}(t) = \left(\frac{29}{5}\right)_4^t \Psi_{29}(0) = (-1)^t.$$

Thus 29 is represented by a form class in $H(-5^t \cdot 80)$ which is a fourth power if t is even and a square but not a fourth power if t is odd.

6. Double prediction. We have applied Dirichlet's technique to determine predictive criteria when $H_2(-D) \simeq Z_{2^k}$, $k \geq 2$. However the method is also applicable to certain types of discriminants $-D$ for which the 2-rank of $H(-D)$ is 2 or more.

We illustrate this for the following two types of discriminants $-D$:

$$D = 4tqr, \qquad q \text{ and } r \text{ (primes)} \equiv 1 \pmod 8, \ (q/r) = 1, \ t = 1 \text{ or } 2.$$

By Lemma 2.1 the 2-rank of $H(-D)$ is 2. Further, by the Rédei–Reichardt theorem [17], the 4-rank of $H(-D)$ is also 2. Thus

$$H(-4tqr) = G_1 \times G_2 \times G_3,$$

where G_1 and G_2 are cyclic subgroups of $H(-4tqr)$ of orders 2^k $(k \geq 2)$ and 2^l $(l \geq 2)$, respectively, and G_3 is a subgroup of $H(-4tqr)$ of odd order. Let U and V be generators of G_1 and G_2 respectively. The subgroup $H^2(-4tqr)$ in $H(-4tqr)$ is the principal genus. The four genera of $H(-4tqr)$ are the cosets $H^2(-4tqr)$, $UH^2(-4tqr)$, $VH^2(-4tqr)$, $UVH^2(-4tqr)$. We order the generic characters of $H(-4tqr)$ as follows: $(*/q)$, $(*/r)$, $(-t/*)$. Let $FH^2(-4tqr)$ be the genus among $UH^2(-4tqr)$, $VH^2(-4tqr)$, $UVH^2(-4tqr)$ with character values $+--$. Let $GH^2(-4tqr)$ be the genus with character values $-+-$. Thus the 4 genera are $H^2(-4tqr)$, $FH^2(-4tqr)$, $GH^2(-4tqr)$, $FGH^2(-4tqr)$ with character values $+++$, $+--$, $-+-$, $--+$ respectively.

Let $H^4(-4tqr)$ denote the subgroup of fourth powers in $H^2(-4tqr)$. We have the coset decomposition $H^2(-4tqr) = H^4(-4tqr) \cup F^2H^4(-4tqr) \cup G^2H^4(-4tqr) \cup F^2G^2H^4(-4tqr)$.

By the law of quadratic reciprocity, we have $(-r/q) = (-q/r) = 1$, and therefore $(-tr/q) = (-tq/r) = 1$. Hence we may define integers w_q and w_r such that

$$w_q^2 \equiv -tr \pmod q, \qquad w_r^2 \equiv -tq \pmod r.$$

Theorem 4. *Let t, q, r, F, G, w_q, w_r be as defined above. Let p be a prime satisfying*

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

so that there are integers H, M, N, H', M', N' with

$$(6.1) \quad H^2p = M^2 + tqN^2, \qquad H > 0, \ (M,N) = 1, \ (H, 2pqr) = 1,$$

$$(6.2) \quad H'^2p = M'^2 + trN'^2, \qquad H' > 0, \ (M',N') = 1, \ (H', 2pqr) = 1.$$

Then p is represented by form class(*es*) *from*

$$\begin{cases} H^4(-4tqr) \Leftrightarrow (M' + w_qN'/q) = (M + w_rN/r) = 1, \\ F^2H^4(-4tqr) \Leftrightarrow (M' + w_qN'/q) = 1, \ (M + w_rN/r) = -1, \\ G^2H^4(-4tqr) \Leftrightarrow (M' + w_qN'/q) = -1, \ (M + w_rN/r) = 1, \\ F^2G^2H^4(-4tqr) \Leftrightarrow (M' + w_qN'/q) = (M + w_rN/r) = -1. \end{cases}$$

Proof. As $(p/q) = (p/r) = (-t/p) = 1$, p is represented by a form class C_p (and its inverse C_p^{-1}) in the principal genus $H^2(-4tqr)$. Let S_p be a class such that $S_p^2 = C_p$. Let K be a positive integer coprime with $2pqr$ which is represented primitively by the form class S_p^{-1}. Then K^2p is represented primitively by the class $(S_p^{-1})^2 S_p^2 = I$ the principal class of $H(-4tqr)$. Hence there exist integers A and B such that

$$K^2 p = A^2 + tqrB^2, \quad (A, B) = 1, \quad (K, 2pqr) = 1. \tag{6.3}$$

From (6.1) and (6.3) we obtain

$$(HA + KM)(HA - KM) = tq(K^2N^2 - rH^2B^2). \tag{6.4}$$

By Lemma 3.6, r does not divide both of $HA \pm KM$. Choose the sign of M so that $r \nmid HA + KM$. Factoring $HA + KM$ into primes, we have

$$HA + KM = \varepsilon 2^\alpha \prod_{(r/q_i)=1} q_i^{e_i} \prod_{(r/r_j)=-1} r_j^{f_j},$$

where $\varepsilon = \pm 1$, α is a nonnegative integer, e_i, f_j are positive integers, and q_i, r_j are distinct odd primes. By Lemma 3.5(ii) each f_j is even. Thus, by the law of quadratic reciprocity, we have

$$\left(\frac{HA + KM}{r}\right) = \left(\frac{\varepsilon}{r}\right)\left(\frac{2}{r}\right)^\alpha \prod_{(r/q_i)=1} \left(\frac{q_i}{r}\right)^{e_i} \prod_{(r/r_j)=-1} \left(\frac{r_j}{r}\right)^{f_j} = 1.$$

Similarly we can choose the sign of M' so that $q \nmid H'A + KM'$, and deduce

$$\left(\frac{H'A + KM'}{q}\right) = 1.$$

Next, by Lemma 3.1, we have

$$\begin{cases} 2(KM + HA)(KM + w_r KN) \equiv (KM + HA + w_r KN)^2 \pmod{r}, \\ 2(KM' + H'A)(KM' + w_q KN') \equiv (KM' + H'A + w_q KN')^2 \pmod{q}, \end{cases}$$

so that

$$\left(\frac{K}{r}\right) = \left(\frac{M + w_r N}{r}\right), \qquad \left(\frac{K}{q}\right) = \left(\frac{M' + w_q N'}{q}\right).$$

If $t = 1$, then the four ambiguous classes are $[1, 0, qr]$, $[q, 0, r]$, $\left[1, 1, \frac{1}{2}(1+qr)\right]$, $\left[2q, 2q, \frac{1}{2}(q+r)\right]$. If $t = 2$, the four ambiguous classes are $[1, 0, 2qr]$, $[2, 0, qr]$, $[q, 0, 2r]$, $[2q, 0, r]$. All these ambiguous classes belong to the principal genus of $H(-4tqr)$. Then p is represented by form class(es) in $H^4(-4tqr) \cup F^2H^4(-4tqr)$

$\Leftrightarrow C_p = J^4$ or F^2J^4 for some form class J in $H(-4tqr)$

$\Leftrightarrow S_p^2 = J^4$ or F^2J^4

$\Leftrightarrow S_p = LJ^2$ or LFJ^2, where L is an ambiguous class, that is, $L^2 = I$,

$\Leftrightarrow S_p = J_1^2$ or FJ_1^2

$\Leftrightarrow K$ is represented by form class(es) in $H^2(-4tqr) \cup FH^2(-4tqr)$

$\Leftrightarrow \left(\frac{K}{q}\right) = 1$

$\Leftrightarrow \left(\frac{M' + w_q N'}{q}\right) = 1.$

Similarly p is represented by form class(es) in $H^4(-4tqr) \cup G^2H^4(-4tqr)$ if and only if $(M + w_rN/r) = 1$. Combining these two assertions we deduce the *double prediction* criterion of the theorem. It is readily verified that the choice of signs of M and M' does not affect the values of the Legendre symbols appearing in the assertion of the theorem. ■

Example. $t = 1$, $q = 73 \equiv 1 \pmod 8$, $r = 89 \equiv 1 \pmod 8$, $(q/r) = 1$, $w_q = 35$, $w_r = 4$, $H(-4tqr) = H(-25988) = G_1 \times G_2$, where G_1 (resp. G_2) is a cyclic group of order 8 generated by the form class $F = [27, -16, 243]$ (resp. $G = [87, 82, 94]$). The genera of $H(-4tqr)$ are:

	$\left(\frac{*}{73}\right)$	$\left(\frac{*}{89}\right)$	$\left(\frac{-1}{*}\right)$
$H^2(-4tqr)$	+	+	+
$FH^2(-4tqr)$	+	−	−
$GH^2(-4tqr)$	−	+	−
$FGH^2(-4tqr)$	−	−	+

Further $H^2(-4tqr)$ comprises sixteen form classes subdivided as follows:

$$\begin{aligned} H^4(-4tqr) &= \{[1,0,6497],\ [2,2,3249],\ [73,0,89],\ [81,16,81]\},\\ F^2H^4(-4tqr) &= \{[9,\pm 2,722],\ [18,\pm 2,361]\},\\ G^2H^4(-4tqr) &= \{[57,\pm 40,121],\ [69,\pm 64,109]\},\\ F^2G^2H^4(-4tqr) &= \{[57,\pm 2,114],\ [69,\pm 28,97]\}. \end{aligned}$$

p	H^2p			H'^2p			ε'	ε	Representation of p
	H	M	N	H'	M'	N'			
97	7	64	3	3	28	1	-1	-1	$97 = 69 \cdot 0^2 + 28 \cdot 0 \cdot 1 + 97 \cdot 1^2$
173	1	10	1	5	63	2	-1	-1	$173 = 57 \cdot 1^2 + 2 \cdot 1 \cdot 1 + 114 \cdot 1^2$
257	7	89	8	5	27	8	-1	$+1$	$257 = 69 \cdot 2^2 + 64 \cdot 2 \cdot (-1) + 109 \cdot (-1)^2$
809	7	32	23	5	72	13	$+1$	-1	$809 = 9 \cdot 3^2 + 2 \cdot 3 \cdot 1 + 722 \cdot 1^2$
1013	7	202	11	7	81	22	$+1$	$+1$	$1013 = 73 \cdot 3^2 + 89 \cdot 2^2$

$H^2p = M^2 + 73N^2$, $H'^2p = M'^2 + 89N'^2$, $\varepsilon' = \left(\frac{M'+35N'}{73}\right)$, $\varepsilon = \left(\frac{M+4N}{89}\right)$.

It remains to investigate further the possibilities of Dirichlet's technique in determining predictive criteria.

Acknowledgements. The first and second authors would like to acknowledge the hospitality of the Centre for Research in Algebra and Number Theory during their visits to Carleton University.

References

[1] S. Arno, *The imaginary quadratic fields of class number* 4, Acta Arith. 60 (1992), 321–334.

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

[3] J. A. Brandler, *Residuacity properties of real quadratic units*, J. Number Theory 5 (1973), 271–286.

[4] E. Brown, *The power of* 2 *dividing the class-number of a binary quadratic discriminant*, ibid. 5 (1973), 413–419.

[5] —, *Class numbers of quadratic fields*, Istituto Nazionale di alta Matematica, Symposia Mathematica (Bologna) 15 (1975), 403–411.

[6] H. Cohn, *A Second Course in Number Theory*, Wiley, New York, 1962.

[7] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, World Sci., Singapore, 1988.

[8] D. A. Cox, *Primes of the Form x^2+ny^2; Fermat, Class Field Theory and Complex Multiplication*, Wiley, New York, 1989.

[9] P. G. L. Dirichlet, *Recherches sur les diviseurs premiers d'une classe de formules du quatrième degré*, J. Reine Angew. Math. 3 (1828), 35–69.

[10] D. R. Estes and G. Pall, *A reconsideration of Legendre–Jacobi symbols*, J. Number Theory 5 (1973), 433–434.

[11] C. F. Gauss, *Disquisitiones Arithmeticae*, English translation by Arthur A. Clarke, Yale University Press, 1966.

[12] R. H. Hudson and K. S. Williams, *Congruences for representations of primes by binary quadratic forms*, Acta Arith. 41 (1982), 311–322.

[13] P. Kaplan, K. S. Williams, and Y. Yamamoto, *An application of dihedral fields to representations of primes by binary quadratic forms*, ibid. 44 (1984), 407–413.

[14] P. A. Leonard and K. S. Williams, *A representation problem involving binary quadratic forms*, Arch. Math. (Basel) 36 (1981), 53–56.

[15] J. B. Muskat, *On simultaneous representations of primes by binary quadratic forms*, J. Number Theory 19 (1984), 263–282.

[16] J. B. Muskat and A. L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. 17 (1970), 185–216.

[17] L. Rédei and H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1933), 69–74.

DEPARTMENT OF MATHEMATICS
AND COMPUTER SCIENCE
BAR-ILAN UNIVERSITY
52900 RAMAT-GAN, ISRAEL

DEPARTMENT OF MATHEMATICS
OKANAGAN UNIVERSITY COLLEGE
KELOWNA, BRITISH COLUMBIA
CANADA V1Y 4X8

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO
CANADA K1S 5B6

Received on 18.5.1994 (2617)