JOURNAL OF NUMBER THEORY 19, 263–282 (1984)

On Simultaneous Representations of Primes by Binary Quadratic Forms

JOSEPH B. MUSKAT*

*Department of Mathematics and Computer Science,
Bar-Ilan University, 52100 Ramat-Gan, Israel*

Communicated by P. T. Bateman

Received August 16, 1982

Let $p \equiv \pm 1 \pmod 8$ be a prime which is a quadratic residue modulo 7. Then $p = M^2 + 7N^2$, and knowing M and N makes it possible to "predict" whether $p = A^2 + 14B^2$ is solvable or $p = 7C^2 + 2D^2$ is solvable. More generally, let q and r be distinct primes, and let an integral solution of $H^2p = M^2 + qN^2$ be known. Under appropriate assumptions, this information can be used to restrict the possible values of K for which $K^2p = A^2 + qrB^2$ is solvable and the possible values of K' for which $K'^2p = qC^2 + rD^2$ is solvable. These restrictions exclude some of the binary quadratic forms in the principal genus of discriminant $-4qr$ from representing p.

1. INTRODUCTION

Let $(a \mid p)$ be the familiar Legendre symbol. If $(a \mid p) = 1$, write $(a \mid p)_4 = 1$ or -1 according as a is or is not a biquadratic residue of p.

In 1825 Gauss announced two criteria for determining $(2 \mid p)_4$ for a prime $p \equiv 1 \pmod 8$. Put

$$p = (4A + 1)^2 + 8B^2 = X^2 + 16Y^2,$$

then $A \equiv Y \pmod 2$, and $(2 \mid p)_4 = 1$ if and only if A and Y are both even. On reading this announcement, Dirichlet proved that $(2 \mid p)_4 = (-1)^A$ and showed that A and Y have the same parity [9, p. 313].

In this paper we adapt Dirichlet's technique to several other situations in which a prime p is represented by positive definite quadratic forms of different discriminants. Our principal results are three general theorems (Theorems 2, 4, and 5) and three particularly interesting corollaries (Theorems 3, 6, and 7).

We may also use Dirichlet's method to show the equivalence of certain

* This research received some support from National Science Foundation Grant GP8973.

0022-314X/84 $3.00

known power residue criteria formulated in terms of coordinates of binary quadratic forms. Theorem 1 is an example of this.

We use nothing deeper than the elementary theory of quadratic forms, the Legendre–Jacobi symbol, and quadratic reciprocity.

2. The Main Results

In what follows, all letters stand for integers, and p, q, and r are primes (except in Theorem 1, where $q=1$). We focus primarily on the following. If q and r satisfy certain congruential restrictions, and p belongs to certain residue classes (mod $4qr$), then there exist integral solutions (H, M, N), (K, A, B), and (K', C, D) to the equations

$$H^2 p = M^2 + qN^2, \qquad (M, N) = 1, \tag{1a}$$

$$K^2 p = A^2 + qrB^2, \qquad (A, B) = 1, \tag{1b}$$

$$K'^2 p = qC^2 + rD^2 \qquad (C, D) = 1, \tag{1c}$$

respectively. We shall derive conditions for the existence of these solutions in Section 3. Section 4 is devoted to some arithmetic preliminaries.

In Section 5 we shall prove

Theorem 1. *Let $p \equiv 1$ or 9 (mod 20) be a prime; then we may write $p = M^2 + N^2$ with N even and $M \equiv 1$ (mod 4), and $p = A^2 + 5B^2$. Noting that either M or N is divisible by 5, we conclude that:*

(a) *if $p \equiv 1$ (mod 20), then A is even if and only if $5 \mid M$,*

(b) *if $p \equiv 9$ (mod 20), then A is even if and only if $5 \mid N$.*

We note that this is the special case $q = 1$, $r = 5$ of Eqs. (1). Part (a) is the corollary to Theorem 7 of [7], proved there by cyclotomy.

The main results of this paper comprise Sections 6 and 7. These are Theorems 2, 4, and 5, the proofs of which use Dirichlet's technique. They deal with cases in which q is odd and $r = 2$, $q = 2$ and r is odd, and q and r are both odd, respectively.

Theorem 2. *Let p and q be distinct odd primes, and $r = 2$. Assume that Eqs. (1) are solvable. If the signs of the odd variables (among M, N, K, K', B, D) are chosen so that each is $\equiv 1$ (mod 4), then K and K' satisfy the following congruences:*

(a) $M + N - K \equiv qB^2 + (1-q)/2 \pmod 8$ *if M is even,*

(b) $M + N - K \equiv B(1+q) \pmod 8$ *if N is even,*

(c) $M+N-2K \equiv -(1+q)/2 \pmod{16}$ *if H is even.*

(d) $M+N-K' \equiv D(1+q) \pmod 8$ *if M is even,*

(e) $M+N-K' \equiv D^2+(q-1)/2 \pmod 8$ *if N is even,*

(f) $M+N-2K' \equiv (1+q)/2 \pmod{16}$ *if H is even.*

The following corollary deals with the interesting special case $q=7$:

THEOREM 3. *Let* $p=M^2+7N^2$ *be a prime* $\equiv \pm 1 \pmod 8$ *with* M *or* $N \equiv 1 \pmod 4$. *Then*

(a) $p=A^2+14B^2$ *is solvable if and only if* $2p+M+N \equiv 3 \pmod 8$.

(b) $p=7C^2+2D^2$ *is solvable if and only if* $2p+M+N \equiv 7 \pmod 8$.

In the following three theorems $r \equiv 1 \pmod 4$. A key role is played by the number u, which is defined to be either 1 or -1 by

$$(Hp^{1/2} \pm M \mid r) = 0 \text{ or } u. \tag{2}$$

From Eqs. (1b) and (1c), $(p \mid r) = 1 = (q \mid r)$, so that $p^{1/2}$ is an integer (mod r). By Eq. (1a),

$$((Hp^{1/2}+M)(Hp^{1/2}-M) \mid r) = (H^2p - M^2 \mid r) = (M^2+qN^2-M^2 \mid r)$$
$$= (qN^2 \mid r) = 0 \text{ or } 1.$$

Thus the choice of sign of $p^{1/2}$ or the sign of $\pm M$ has no effect on u. (In other words, it is impossible that $u=1$ for one choice of signs and $u=-1$ for another choice.)

THEOREM 4. *Let* $r \equiv 1 \pmod 8$ *and* p *be distinct odd primes, and* $q=2$. *Assume Eqs.* (1) *are solvable with* $H=1$. *Then* $(K \mid r) = u$ *and* $(K' \mid r) = (2 \mid r)_4\, u$, *where* u *is defined by* (2).

Note. Clearly K and K' are odd.

THEOREM 5. *Let* $r \equiv 1 \pmod 4$, p *and* q *be distinct odd primes. Assume Eqs.* (1) *are solvable. Define* u *by* (2). *Then* $(K \mid r) = (-1)^f u$ *and* $(K' \mid r) = (-1)^{f'} (q \mid r)_4\, u$, *where* $f=f'=0$ *if* $r \equiv 1 \pmod 8$; *if* $r \equiv 5 \pmod 8$, *then*

$$f=N+B+1, \qquad f'=N+D+1, \qquad \text{if } q \equiv 1 \pmod 4,$$
$$f=H+K+1, \qquad f'=H+K', \qquad \text{if } q \equiv 3 \pmod 4.$$

Finally we obtain as corollaries the following results for the cases $q=3$, $r=13$, and $q=11$, $r=5$:

THEOREM 6. *Let $p = M^2 + 3N^2$ be a prime such that $(p \mid 13) = 1$. Define u to be either* 1 *or* -1 *by* (2). *Then*

(a) $p = A^2 + 39B^2$ *is solvable if and only if* $u = -1$,

(b) $p = 3C^2 + 13D^2$ *is solvable if and only if* $u = 1$.

THEOREM 7. *Let p be a prime which satisfies $(p \mid 5) = (p \mid 11) = 1$. Then $H^2p = M^2 + 11N^2$ with $H = 1$ or* 2, *and*

(a) $p = A^2 + 55B^2$ *is solvable if and only if*

$$p \equiv 1 \pmod{5} \textit{ and } 5 \mid N, \textit{ or}$$

$$p \equiv 4 \pmod{5} \textit{ and } 5 \mid M;$$

(b) $p = 11C^2 + 5D^2$ *is solvable if and only if*

$$p \equiv 1 \pmod{5} \textit{ and } 5 \mid M, \textit{ or}$$

$$p \equiv 4 \pmod{5} \textit{ and } 5 \mid N.$$

Theorem 7 solves an open problem mentioned in [1, p. 144].

We view Theorems 2, 4, and 5 as prescribing congruential restrictions on possible values of K and K'. Any possible value of K or K' must satisfy the condition that $-qr$ be a quadratic residue modulo any odd prime divisor of K or K'. (This follows immediately from Eqs. (1b) and (1c).) A value of K or K' satisfying this condition is called *admissible* if it satisfies the restriction of the appropriate theorem. These restrictions are called *predictive* if they are independent of A and B in the case of K, or of C and D in the case of K'. In other words, the restriction on K or K' depends only upon the representation (1a). A predictive restriction is called *inclusive* if identical restrictions are placed on K and K'. A predictive restriction is called *exclusive* if any admissible value for K (or K') is inadmissible for K' (or K).

The following examples illustrate these definitions:

(a) Theorem 3, the case $q = 7$ and $r = 2$, is an exclusive predictive restriction. In this case Eqs. (1b) and (1c) are solvable with either $K = 1$ and $K' = -3$, or with $K = -3$ and $K' = 1$. The conclusion is that either $p = A^2 + 14B^2$ or $p = 7C^2 + 2D^2$ is solvable, but not both, and the conditions for solvability depend only upon the representation $p = M^2 + 7N^2$.

(b) Theorem 4 gives a predictive restriction; it is inclusive if and only if $(2 \mid r)_4 = 1$.

Note that admissibility does not imply solvability. For example, let $q = 2$, $r = 97$, and $p = 73$. Then

$$73 = 1^2 + 2 \cdot 6^2, \qquad 73^{1/2} \equiv \pm 48 \pmod{97},$$

so by Theorem 4, we have

$$(p^{1/2} \pm M \mid 97) = (\pm 48 \pm 1 \mid 97) = 1.$$

Thus $(K \mid 97) = 1$ and $(K' \mid 97) = (2 \mid 97)_4 = (14 \mid 97) = -1$. Admissible values for K are 1, 3, and 9, while 5, 7, and 13 are admissible values for K'. The equation $K^2 \cdot 73 = A^2 + 194B^2$ is satisfied by $9^2 \cdot 73 = 53^2 + 194 \cdot 4^2$, but has no integral solutions if $K = 1$ or $K = 3$. Similarly, the equation $K'^2 \cdot 73 = 2C^2 + 97D^2$ is satisfied by $7^2 \cdot 73 = 2 \cdot 24^2 + 97 \cdot 5^2$, but has no integral solutions for $K' = 5$ or $K' = 13$.

3. On the Solvability of Equations (1)

Assuming that Eqs. (1) are solvable places certain restrictions on p, q, and r. We present the restrictions associated with the hypotheses of Theorems 2, 4, and 5 in the following three lemmas.

Lemma 1. *Let p and q be distinct odd primes, $r = 2$. If Eqs.* (1) *are solvable, then $(p \mid q) = 1$, and $p, q \equiv \pm 1$* (mod 8). *Moreover, one of H, M, and N is divisible by* 4, *while the other two are odd.*

Proof. Equation (1a) implies $(p \mid q) = (-q \mid p) = 1$. Equation (1b) yields $(-2q \mid p) = 1$, so that $(2 \mid p) = 1$. Hence $p \equiv \pm 1 \pmod 8$. Similarly Eq. (1c) gives $(2 \mid q) = (p \mid q)$, so that $q \equiv \pm 1 \pmod 8$. Now by (1a), $\pm H^2 \equiv M^2 \pm N^2 \pmod 8$. Since $(M, N) = 1$, two of M, N, and H are odd, and the other is divisible by 4.

Note. Obviously $p \equiv 1 + 2qB^2 \equiv q + 2D^2 \pmod 8$. Also

$$\begin{gathered} 4 \mid M \Rightarrow p \equiv q \pmod 8, \qquad 4 \mid N \Rightarrow p \equiv 1 \pmod 8, \\ 4 \mid H \Rightarrow q \equiv 7 \pmod 8. \end{gathered} \tag{3}$$

Lemma 2. *Let p and r be distinct odd primes, $q = 2$. If Eqs.* (1) *are solvable, then $(p \mid r) = 1 = (-2 \mid p)$, so that $p \equiv 1$ or* 3 (mod 8). *If $p \equiv 1$* (mod 8), *then $r \equiv \pm 1$* (mod 8), *while $p \equiv 3$* (mod 8) *implies $r \equiv 1$* (mod 8).

Proof. Equations (1a) and (1b) imply $(-2 \mid p) = 1$ and $(p \mid r) = 1$, respectively. The former implies that $p \equiv 1$ or $3 \pmod 8$. Examining Eq. (1c) (mod 8) gives the rest of the lemma.

Note. The restrictions presented in Theorems 4 and 5 are meaningful only if $(-1 \mid r) = 1$; i.e., if $r \equiv 1 \pmod 4$. Accordingly, the case $p \equiv 1 \pmod 8$, $r \equiv 7 \pmod 8$ was excluded from Theorem 4, and $r \equiv 3 \pmod 4$ from Theorem 5.

LEMMA 3. *Let p, q and r be distinct odd primes. If Eqs.* (1) *are solvable, then* $(p \mid q) = (-q \mid p) = 1$, $(p \mid r) = (r \mid p) = 1$, $(q \mid r) = (r \mid q) = 1$. If $r \equiv 3 \pmod 4$, then $p \equiv q \equiv 1 \pmod 4$.

Proof. Examining Eqs. (1) yields these Legendre symbol values. Then the law of quadratic reciprocity gives the final assertion.

We turn now to the converse problem and show that assuming the congruential restrictions of Lemmas 1, 2, or 3 implies the solvability of Eqs. (1).

A *binary quadratic form* $f = [a, b, c] = ax^2 + bxy + cy^2 = f(x, y)$ of *discriminant* $d = b^2 - 4ac$ is primitive if the g.c.d. (a, b, c) of the coefficients is 1. A form having negative discriminant is called *definite.* If in addition $a, c > 0$, the form is called *positive definite.* Only positive definite forms are considered here.

The form f is said to *represent* the integer m if $f(x, y) = m$ for integers x, y; this representation is *primitive* if $(x, y) = 1$. Representation of m is invariant under any integral linear transformation

$$x = t_1 X + t_2 Y, \qquad y = t_3 X + t_4 Y,$$

where the determinant $t_1 t_4 - t_2 t_3$ is equal to 1. A set of all binary quadratic forms obtainable one from another by applying such linear transformations is called a *class* of forms. Evidently, two forms in the same class have the same discriminant, and to be positive definite is a class property. Every positive definite class has a unique *reduced form* $[a, b, c]$ such that

$$-a < b \leqslant a \leqslant c; \qquad \text{if} \quad a = c, \text{ then } b \geqslant 0.$$

The generic characters of a number m, relatively prime to the discriminant d, consist of a set of Jacobi symbols, which includes

$$\begin{array}{rl} (m \mid v) & \text{for each odd prime divisor } v \text{ of } d, \\ (-1 \mid m) & \text{if } d \equiv 0 \text{ or } 12 \pmod{16}, \\ (2 \mid m) & \text{if } d \equiv 0 \text{ or } 8 \pmod{32}, \\ (-2 \mid m) & \text{if } d \equiv 0 \text{ or } 24 \pmod{32}. \end{array}$$

The generic characters of a form f consist of the generic characters of any odd m prime to d and primitively represented by f. The set of all forms of a given discriminant having a given set of generic characters is called a *genus.* A genus consists of one or more classes, as generic characters are clearly invariants of a given class. The *principal class* is the class that represents 1, and the *principal genus* is the genus whose forms have generic characters all equal to 1. Proofs of all unverified statements can be found, for example, in [9, Art. 79–98].

LEMMA 4 [5, p. 128]. *Let t be relatively prime to d. Then t is represented primitively by a binary quadratic form of discriminant d if and only if the congruence*

$$s^2 \equiv d \pmod{4t}$$

is solvable.

The discriminants studied in this paper are all even, so that we may put $d = 4\Delta$. By Lemma 4, it follows that the prime p, $(p, 2d) = 1$, is represented primitively by a form of discriminant 4Δ if and only if $(\Delta \mid p) = 1$.

LEMMA 5 [3, Sect. 53, 83]. *Let p be an odd prime, not dividing $d = 4\Delta$, whose generic characters are all equal to 1. Then p is represented primitively by a form in the principal genus of discriminant d.*

LEMMA 6. *If p is an odd prime that satisfies*

(a) $r = 2$, $(p \mid q) = 1$, p, $q \equiv \pm 1 \pmod 8$, *but* $q \equiv 1 \pmod 8$ *implies* $p \equiv 1 \pmod 8$; *or*

(b) $q = 2$, $(-2 \mid p) = 1 = (p \mid r)$, $r \equiv \pm 1 \pmod 8$, *but* $r \equiv 7 \pmod 8$ *implies* $p \equiv 1 \pmod 8$; *or*

(c) $(p \mid q) = (-q \mid p) = (p \mid r) = (q \mid r) = 1$, *but* $r \equiv 3 \pmod 4$ *implies* $p \equiv q \equiv 1 \pmod 4$;

then in each case p is represented by a form in the principal genus of discriminants $-4q$ and $-4qr$.

Proof. According to Lemma 5, we must show in each case that all the relevant generic characters equal 1.

In case (a), $(p \mid q) = 1$ is given. If $q \equiv 7 \pmod 8$, then $(2 \mid p) = 1$ follows from the assumption that $p \equiv \pm 1 \pmod 8$. If, however, $q \equiv 1 \pmod 8$, then $(-1 \mid p) = 1 = (-2 \mid p)$ are needed. But these follow from $p \equiv 1 \pmod 8$.

In case (b), $(-2 \mid p) = 1 = (p \mid r)$ are given. If $r \equiv 7 \pmod 8$, then $(2 \mid p) = 1$, which is required, follows from $p \equiv 1 \pmod 8$.

In case (c), the generic characters for the discriminant $-4q$ are $(p \mid q)$ and, if $q \equiv 1 \pmod 4$, $(-1 \mid p)$. $(p \mid q) = 1$ is given. If $q \equiv 1 \pmod 4$, then $(-q \mid p) = (p \mid q) = (q \mid p) = 1$, so $(-1 \mid p) = 1$.

The generic characters for the discriminant $-4qr$ are $(p \mid q)$, $(p \mid r)$ and, if $qr \equiv 1 \pmod 4$, $(-1 \mid p)$. $(p \mid q) = (p \mid r) = 1$ is given. If $r \equiv 3 \pmod 4$, then $q \equiv 1 \pmod 4$ and $qr \equiv 3 \pmod 4$. So the only remaining case is $q \equiv r \equiv 1 \pmod 4$. Then $(-1 \mid p) = 1$, as was shown in the previous paragraph.

Since they represent 1, $[1, 0, q]$ and $[1, 0, qr]$ are forms of their respective principal genera. In order to prove a similar statement about the form $[q, 0, r]$, we need two classical results, along with the seemingly extraneous assumption made in Lemma 6, part (c): $(q \mid r) = 1$.

LEMMA 7 (Legendre) [3, Theorem 91]. *If a, b, and c are relatively prime in pairs, squarefree, and not all of the same sign, then $au^2 + bv^2 + cw^2 = 0$ has nontrivial integral solutions if and only if $-bc$, $-ca$, and $-ab$ are quadratic residues of a, b, and c, respectively.*

Two forms f and g of discriminant d will be called rationally equivalent if f can be transformed into g by a linear transformation with rational matrix R of determinant ±1, where the denominators of R are relatively prime to d.

LEMMA 8 (Eisenstein–H. J. S. Smith) [2, p. 88]. *Two forms f and g of discriminant d are in the same genus if and only if they are rationally equivalent.*

Set $X = t_1x + t_2y$, $Y = t_3x + t_4y$, where t_1, t_2, t_3, and t_4 are rational and $t_1t_4 - t_2t_3 = 1$. It is easy to see that there exists a rational transformation such that $qX^2 + rY^2 = x^2 + qry^2$ if and only if $qu^2 + rv^2 = w^2$ is solvable in integers. (The correspondence is $t_1 = u/w$, $t_3 = v/w$, $t_2 = -rt_3$, $t_4 = qt_1$.) In every case of Lemma 6, q and r are quadratic residues of each other, so that $qu^2 + rv^2 = w^2$ is solvable in integers, by Lemma 7. Thus by Lemma 8, $[q, 0, r]$ is in the principal genus of forms of discriminant $-4qr$.

LEMMA 9. *If the hypotheses of Lemma 6 are satisfied, then in each case, Eqs. (1) have solutions.*

Proof. By Lemma 6, p is represented by a form f of the principal genus of discriminant $-4q$. If $g = [1, 0, q]$, then to $f(x, y) = p$ we apply a rational linear transformation and obtain $g(X, Y) = X^2 + qY^2 = p$. If H is the least common multiple of the denominators of X and Y, then $(H, -4q) = 1$, and we have

$$H^2p = (HX)^2 + q(HY)^2,$$

where HX and HY are relatively prime integers.

By Lemma 6, p is represented by a form f' of the principal genus of discriminant $-4qr$. Having established that $[1, 0, qr]$ and $[q, 0, r]$ are in the principal genus of discriminant $-4qr$, we apply two appropriate rational linear transformations to f' and obtain in a similar fashion that Eqs. (1b) and (1c) are solvable. This completes the proof of Lemma 9.

The discriminants in Theorems 3, 6, and 7 have the property that $[1, 0, qr]$ and $[q, 0, r]$ are the reduced forms of the only two classes in the principal genus of discriminant $d = -4qr$; this can be derived by the Gaussian theory of reduction of positive definite binary quadratic forms (see, for instance, [6, Art. 134]). Thus the necessary conditions for the representation of p are also sufficient, as they are in Theorem 1, where the only class in the principal genus of discriminant -4 contains the reduced form $[1, 0, 1]$, and $[1, 0, 5]$ is the reduced form in the only class in the principal genus of discriminant -20.

4. Dirichlet's Method

Assume that Eqs. (1) are solvable. We obtain the *basic equations*

$$q(K^2N^2 - rH^2B^2) = (HA + KM)(HA - KM) \tag{4}$$

$$K'^2M^2 - rH^2D^2 = q(HC + K'N)(HC - K'N) \tag{4'}$$

by cross-multiplying Eqs. (1a) and (1b), (1a) and (1c), respectively, and rearranging. The heart of the method of Dirichlet involves analysis of the prime divisors of the quantities $HA \pm KM$ and $HC \pm K'N$.

Lemma 10. *Let v be an odd prime distinct from q and r.*

(a) *Let v divide $HA + KM$ (or $HA - KM$). If $(r \mid v) = -1$, then an even power of v exactly divides $HA + KM$ (or $HA - KM$).*

(b) *Let v divide $HC + K'N$ (or $HC - K'N$). If $(r \mid v) = -1$, then an even power of v exactly divides $HC + K'N$ (or $HC - K'N$).*

Note. It suffices to prove the lemma for $HA + KM$ and $HC + K'N$. Replacing H by $-H$ provides proofs for the other cases.

Proof of (a). Let v be an odd prime divisor of $HA + KM$ in (4) different from q and r.

From (4), $(KN)^2 \equiv r(HB)^2 \pmod{v}$. If $v \nmid (KN, HB)$, then $(r \mid v) = 1$.

If $v \mid (KN, HB)$, then $v \mid (K, H)$ or $v \mid (N, B)$, as $(H, N) = 1 = (K, B)$. If $v \mid (K, H)$, then (1a) and (1b) yield $(-q \mid v) = 1$, $(-qr \mid v) = 1$, respectively. Hence $(r \mid v) = 1$.

Now assume that $v \nmid (K, H)$ but $v \mid (N, B)$. If v also divides $HA - KM$, then $v \mid HA$ and $v \mid KM$. But $v \mid HB$ and $v \mid KN$. Hence v divides both $(HA, HB) = H$ and $(KM, KN) = K$. Thus $v \mid (K, H)$; contradiction.

It remains to consider the case where $v \nmid HA - KM$. Assume $v^t \parallel (N, B)$. Then Eq. (4) becomes

$$q[(KN/v^t)^2 - r(HB/v^t)^2] = (HA - KM)(HA + KM)/v^{2t}.$$

We conclude the proof by showing that $v^{2t} \parallel HA + KM$ or $(r \mid v) = 1$. If $v \mid (HA + KM)/v^{2t}$, then

$$(KN/v^t)^2 \equiv r(HB/v^t)^2 \pmod{v}.$$

This implies $(r \mid v) = 1$ unless v divides both KN/v^t and HB/v^t. If $v \mid K$, then by (1b), $v \mid A$, contradicting $(A, B) = 1$. If $v \mid N/v^t$, then $v \mid H$; this leads to a contradiction of $(M, N) = 1$ in (1a).

The proof of (b) is almost identical.

LEMMA 11. *Let* $r \equiv 1 \pmod 4$. *Let* S *denote the set of the four expressions* $HA \pm KM$, $HC \pm K'N$.

(a) *If* r *divides* $HA + KM$ *or* $HA - KM$, *then* $r \mid N$. *If* r *divides* $HC + K'N$ *or* $HC - K'N$, *then* $r \mid M$. *At most one element of* S *is divisible by* r.

(b) *The largest odd divisor of each of the elements of* S *is not a quadratic nonresidue* (mod r).

(c) *If* $r \equiv 1 \pmod 8$, *then the elements of* S *are not quadratic nonresidues* (mod r).

Proof. If r divides $HA + KM$ or $HA - KM$, then by Eq. (4), $r \mid KN$. Hence $r \mid N$, since $r \mid K$ and Eq. (1b) imply $r \mid (A, B)$, a contradiction. If r divides both $HA + KM$ and $HA - KM$, then $r \mid HA$ and $r \mid KM$. Since $r \mid A$ or $r \mid K$ implies $r \mid (A, B)$, r must divide H and M. But by Eq. (1a), this implies $r \mid (M, N)$, a contradiction. We show similarly, by referring to Eqs. (4′), (1c), and (1a), that if r divides $HC + K'N$ or $HC - K'N$, then $r \mid M$, and that r cannot divide both $HC + K'N$ and $HC - K'N$. Finally, if r divides one of $HA + KM$ and $HA - KM$, and also one of $HC + K'N$ and $HC - K'N$, then $r \mid N$ and $r \mid M$, which contradicts $(M, N) = 1$ in (1a). This completes the proof of part (a).

Let $w \in S$, and let v be any odd prime divisor of w distinct from q and r. We invoke the law of quadratic reciprocity and the assumption $r \equiv 1 \pmod 4$ to derive from Lemma 10 that if $(v \mid r) = -1$, then an even power of v exactly divides w. Hence the largest odd divisor of w is not a quadratic nonresidue (mod r), and we have established part (b). Part (c) then follows from noting that $r \equiv 1 \pmod 8$ implies $(2 \mid r) = 1$.

If $r \equiv 5 \pmod 8$, then we must attempt to determine the parities of the powers of 2 which exactly divide each of the elements of S. The following lemma will be useful in this context.

LEMMA 12. *If* $r \equiv 5 \pmod 8$, *then an even power of* 2 *exactly divides* $x^2 - ry^2$.

Proof. Let $2^s \| x$ and $2^t \| y$. If $s \neq t$, then clearly $2^{2w} \| x^2 - ry^2$, where $w = \min\{s, t\}$. If $s = t$, then $x^2 \equiv y^2 \equiv 2^{2s} \pmod{2^{2s+3}}$. Hence $2^{2s+2} \| x^2 - ry^2$.

5. The Case $q = 1$, $r = 5$

This section is devoted to proving Theorem 1.

As noted at the end of Section 3, if $p \equiv 1$ or 9 (mod 20), then (1a) and (1b) are solvable with $H = K = 1$. Elementary considerations (mod 5) show that one of M and N must be divisible by 5. The basic equation (4) becomes

$$N^2 - 5B^2 = (A + M)(A - M).$$

First assume that A is even. Then B, $A + M$, and $A - M$ are odd, since $M \equiv 1 \pmod 4$. According to Lemma 11, part (b), $(A + M \mid 5) = 0$ or 1 and $(A - M \mid 5) = 0$ or 1. The only values (mod 5) of (A, M) which satisfy these conditions are $(\pm 1, 0)$ and $(\pm 2, \pm 2)$, since $5 \nmid A$. If $5 \mid M$, then $A \equiv \pm 4$ (mod 10), and $p = A^2 + 5B^2 \equiv 16 + 5 \equiv 1 \pmod{20}$. If, however, $5 \nmid M$, then $A \equiv \pm 2 \pmod{10}$, and $p = A^2 + 5B^2 \equiv 4 + 5 \equiv 9 \pmod{20}$. This proves Theorem 1 if A is even.

If A is odd, choose the sign of A so that $A \equiv M \equiv 1 \pmod 4$; then $A + M \equiv 2 \pmod 4$. By Lemma 12, $A - M$ is also exactly divisible by an odd power of 2. Since $(2 \mid 5) = -1$, we deduce from Lemma 11, part (b), that $(A \pm M \mid 5) = 0$ or -1. The only values (mod 5) of (A, M) which satisfy these conditions are $(\pm 2, 0)$ and $(\pm 1, \pm 1)$. If $5 \mid M$, then $p \equiv 9 \pmod{20}$, while if $5 \nmid M$, then $p \equiv 1 \pmod{20}$. This proves Theorem 1 if A is odd.

6. The Case q Odd, $r = 2$

In this section we prove Theorem 2 and its corollary for the special case $q = 7$, Theorem 3. We assume that Eqs. (1) hold, and are aided by Lemma 1.

Proof of Theorem 2. We present the arguments for conditions (a), (b), and (c) on K. The arguments for K' are analogous.

By Lemmas 1 (should q divide $HA + KM$) and 10, if v is any odd prime divisor of $HA + KM$, then $(2 \mid v) = 1$, which is equivalent to $v \equiv \pm 1 \pmod 8$, or $v^{2t} \parallel HA + KM$. But $v^2 \equiv 1 \pmod 8$; hence, if $2^s \parallel HA + KM$, then

$$(HA + KM)/2^s \equiv \pm 1 \qquad \pmod 8.$$

We may choose the signs of K and A so that $K = 4k + 1$ *and* $A = 4a + 1$, and consider the basic equation (4) with $r = 2$

$$q(K^2N^2 - 2H^2B^2) = H^2A^2 - K^2M^2 \tag{5}$$

modulo certain powers of 2. There are three cases.

(a) Suppose M is even; put $M = 4m$, $N = 4n + 1$, $H = 4h + 1$. Then $HA + KM$ is odd, so that $s = 0$, and we have

$$HA + KM \equiv 4h + 4a + 1 + 4m \equiv \pm 1 \equiv 1 \pmod{8}.$$

Expanding Eq. (5) (mod 16) and dividing by 2 yields

$$4k + 4n \equiv 4h + 4a + qB^2 + (1 - q)/2 \pmod{8}.$$

Combining the last two congruences (and using $4k \equiv -4k \pmod{8}$) gives

$$4m + 4n - 4k = M + N - K \equiv qB^2 + (1 - q)/2 \pmod{8}.$$

This is congruence (a) of Theorem 2.

(b) Suppose N is even; put $N = 4n$, $M = 4m + 1$, $H = 4h + 1$. By (3), $p \equiv 1 \pmod{8}$, so that $B = 2b$ is even; furthermore, $HA + KM \equiv 2 \pmod{4}$, so that $s = 1$. Then

$$(HA + KM)/2 - 1 \equiv 2(h + a + k + m) \equiv 0 \text{ or } -2 \pmod{8}. \qquad (6)$$

If we expand Eq. (5) (mod 32) and divide by 4, we obtain

$$4n + 2(h + a - k - m) \equiv 2qb^2 \pmod{8}. \qquad (7)$$

(Recall that $x^2 - x$ is even for every integer x.) This congruence implies that b has the same parity as $h + a + k + m$, so that (6) becomes

$$2(h + a + k + m + b^2) \equiv 0 \pmod{8}.$$

Subtracting this congruence from congruence (7) gives

$$4m + 4n - 4k \equiv 2b^2(1 + q) \pmod{8}.$$

Since $1 + q$ is even, $2b^2(1 + q) \equiv 2b(1 + q) \equiv B(1 + q) \pmod{8}$. Hence

$$4m + 4n - 4k = M + N - K \equiv B(1 + q) \pmod{8}.$$

This is congruence (b) of Theorem 2.

(c) Suppose H is even; put $H = 4h$, $M = 4m + 1$, $N = 4n + 1$. As H is even, $HA + KM$ is odd, $s = 0$, so that

$$2(HA + KM) - 2 \equiv 8h + 8k + 8M \equiv 0 \text{ or } -4 \pmod{16},$$

$$8h + 8k + 8m \equiv 0 \pmod{16}.$$

Expand Eq. (5) (mod 32) and divide by 2. Since, by Lemma 1, $q \equiv 7$ (mod 8),

$$8h \equiv 12m + 4n + (1+q)/2 \qquad (\text{mod } 16).$$

Combining the last two congruences, we obtain

$$4m + 4n - 8k = M + N - 2K \equiv -(1+q)/2 \qquad (\text{mod } 16).$$

This is congruence (c) of Theorem 2.

The proofs of congruences (d), (e), and (f) are very similar to those of (b), (a), and (c), respectively.

Remarks. Congruences (c) and (f) of Theorem 2 do not depend at all on A, B, C, or D; thus if H is even, we have predictive restrictions. By (3), $q \equiv 7$ (mod 8). If $q \equiv 15$ (mod 16), then (c) and (f) impose identical restrictions on K and K', so they comprise an inclusive predictive restriction. If, however, $q \equiv 7$ (mod 16), then (c) and (f) impose mutually exclusive restrictions on K and K', so they comprise an exclusive predictive restriction.

If H is odd and $q \equiv 7$ (mod 8), then Theorem 2 yields

$$M + N - K \equiv (1+q)/2 \text{ or } 0 \ (\text{mod } 8) \text{ according as } M \text{ or } N \text{ is even},$$

$$M + N - K' \equiv 0 \text{ or } (1+q)/2 \ (\text{mod } 8) \text{ according as } M \text{ or } N \text{ is even}.$$

These restrictions are predictive. They are inclusive or exclusive according as $q \equiv 15$ or 7 (mod 16). (Note that this is the same situation that prevails where H is even, so that the type of restriction depends only on q (mod 16).)

If $q \equiv 1$ (mod 8), the restrictions on K and K' are not predictive. Note, however, that if the roles of q and r are interchanged, then Theorem 4 provides a predictive restriction for these K and K'.

The case $q = 7$ of Theorem 2, motivated by [8, Theorem 3], has a particularly elegant formulation. If $(p \mid 7) = 1$ and $p \equiv \pm 1$ (mod 8), then $p = M^2 + 7N^2$; moreover, p is represented by one of the two reduced forms $[1, 0, 14]$ and $[2, 0, 7]$ in the principal genus of discriminant -56. Since

$$p = A^2 + 14B^2 \quad \text{implies} \quad (-3)^2 p = 2(A + 7B)^2 + 7(A - 2B)^2,$$

$$p = 7C^2 + 2D^2 \quad \text{implies} \quad (-3)^2 p = (7C + 2D)^2 + 14(C - D)^2,$$

it follows that (1b) and (1c) are solvable with K, $K' = 1$ or -3. Then Theorem 2 implies that $p = A^2 + 14B^2$, that is, $K = 1$, if and only if $M + N \equiv 5$ (mod 8) if M is even, or $M + N \equiv 1$ (mod 8) if N is even. Upon noting that M is even if and only if $p \equiv 7$ (mod 8), we obtain Theorem 3.

A similar situation prevails for $q = 23 \equiv 7$ (mod 16). If $(p \mid 23) = 1$, then (1a) holds with $H = 1$ or $H = -3$. (The latter corresponds to the reduced forms $[3, \pm 2, 8]$ in the principal genus of discriminant -92.) If also $p \equiv \pm 1$

(mod 8), then (1b) and (1c) hold with K, $K' = 1$ or 5 (the relevant reduced forms are $[1, 0, 46]$ and $[2, 0, 23]$). We may formulate for $q = 23$ a theorem similar to Theorem 3.

Here are several examples for $q = 7$ and $q = 23$:

q	p	H	M	N	K	A	B	K'	C	D
7	23	1	4	1	1	−3	1	−3	1	10
7	71	1	8	1	−3	17	5	1	−3	2
23	31	−3	16	1	5	−19	−3	1	1	2
23	167	1	12	1	1	−11	1	5	9	34

In contrast, consider the case $q = 31 \equiv 15 \pmod{16}$. Let $(p \mid 31) = 1$ and $p \equiv \pm 1 \pmod 8$; then (1a) is solvable with $H = 1$ or $H = 5$ (the relevant reduced forms are $[1, 0, 31]$ and $[5, \pm 4, 7]$). If $M + N \equiv 5 \pmod 8$, then (1b) and (1c) are solvable with $K = K' = -3$; if $M + N \equiv 1 \pmod 8$, then they are solvable with $(K, K') = (1, -7)$ or $(-7, 1)$. Thus $K \equiv K' \pmod 8$, which is consistent with the inclusive predictive restriction in this case. Examples follow:

p	H	M	N	K	A	B	K'	C	D
7	5	12	1	−3	1	1	−3	1	4
71	5	16	−7	1	−3	1	−7	−3	40

7. The Case r Odd

Let $r \equiv 1 \pmod 4$. We open this section by relating the quadratic characters (mod r) of $HA \pm KM$ and $HC \pm K'N$. The result, Lemma 14, is needed in the proofs of Theorems 4 and 5. We acknowledge with gratitude the assistence of Emma Lehmer at this point.

Lemma 13. *Let x, y, and z be integers, v an odd prime dividing $z^2 - x^2 - y^2$. Then none of the four products*

$$2(z \pm x)(z \pm y)$$

is a quadratic nonresidue (mod v).

Proof. If v divides $z \pm x$, assume, without loss of generality, that $z \equiv x$ (mod v). Then $v \mid y$, so that

$$2(z + x)(z \pm y) \equiv 4z^2 \pmod v,$$

$$2(z - x)(z \pm y) \equiv 0 \pmod v.$$

Otherwise, put $z-x\equiv w \pmod v$. Then $w(z+x)\equiv y^2 \pmod v$. Also $2wz\equiv w^2+y^2 \pmod v$, so that $2w(z\pm y)\equiv (w\pm y)^2 \pmod v$. The result is now apparent.

LEMMA 14. *Let* $r\equiv 1 \pmod 4$. *If Eqs.* (1) *hold, then* $(p\mid r)=(q\mid r)=1$, *and for all choices of sign,*

(a) $(HA\pm KM\mid r)=(K(Hp^{1/2}\pm M)\mid r)$,

(b) $(HC\pm K'N\mid r)(2K'q^{1/2}(Hp^{1/2}\pm M)\mid r)=0$ or 1.

Proof. Since Eqs. (1) hold, by Lemmas 2 and 3, $(p\mid r)=1=(q\mid r)$. Thus $p^{1/2}$ and $q^{1/2}$ are integral $(\mathrm{mod}\, r)$. Denote by e an integer such that

$$p\equiv e^2 \pmod r.$$

Then Eq. (1b) yields

$$K^2e^2\equiv A^2 \pmod r.$$

Choose the sign of e so that

$$A\equiv Ke \pmod r.$$

Then

$$HA\pm KM\equiv HKe\pm KM\equiv K(Hp^{1/2}\pm M) \pmod r.$$

Part (a) of the lemma is an immediate consequence.

Equation (4′) yields

$$qH^2C^2\equiv qK'^2N^2+K'^2M^2 \pmod r.$$

Then Lemma 13 with $x\equiv q^{1/2}K'N$, $y\equiv K'M$, $z\equiv q^{1/2}HC \pmod r$ implies that none of the four products

$$2q^{1/2}(HC\pm K'N)(q^{1/2}HC\pm K'M)$$

is a quadratic nonresidue $(\mathrm{mod}\, r)$. Equation (1c) permits replacing $q^{1/2}C$ by $p^{1/2}K'$, thereby establishing part (b) of the lemma.

What is the significance of these congruences? By Lemma 11, if $r\equiv 1 \pmod 8$, then $HA\pm KM$ and $HC\pm K'N$ cannot be quadratic nonresidues $(\mathrm{mod}\, r)$. When the solution to (1a) is given, we can predict from these congruences whether or not K and K' are quadratic residues $(\mathrm{mod}\, r)$. When $r\equiv 5 \pmod 8$, we need also the parities of the powers of 2 exactly dividing

$HA \pm KM$ and $HC \pm K'N$. In some cases these parities can be predicted from the solution to (1a); this is discussed later.

Assume now that $q = 2$.

Proof of Theorem 4. By Lemma 2, $r \equiv 1 \pmod 8$. Equation (1a) is solvable with $H = 1$. By Lemma 11, $A \pm KM$ and $C \pm K'N$ cannot be quadratic nonresidues (mod r). If we define u by

$$(p^{1/2} \pm M \mid r) = 0 \text{ or } u,$$

then Lemma 14 implies

$$(K \mid r) = u, \qquad (K' \mid r) = (2^{3/2} \mid r)u = (2^{1/2} \mid r)u = (2 \mid r)_4\, u.$$

Remark. Theorem 4 gives a predictive restriction, because A, B, C, and D are not involved. It is inclusive or exclusive according as $(2 \mid r)_4 = 1$ or -1.

As an example, consider the case $r = 17$. The principal genus of discriminant $-136 = -4 \cdot 34$ contains just the two classes having reduced forms $[1, 0, 34]$ and $[2, 0, 17]$. This implies that exactly one of (1b) and (1c) is solvable with p having coefficient 1; this is consistent with $(2 \mid 17)_4 = -1$. Specifically, $p = A^2 + 34B^2$ or $2C^2 + 17D^2$ according as $(p^{1/2} \pm M \mid 17) = 0$ or 1, or 0 or -1. A similar statement holds for $r = 41$.

Here are some numerical examples:

(a) $r = 17, p = 137 = 3^2 + 2 \cdot 8^2 \equiv 1^2 \pmod{17}$.
$(2 \mid 17)_4 = (6 \mid 17) = -1$.
$(p^{1/2} \pm M \mid 17) = (\pm 1 \pm 3 \mid 17) = 1$, so $(K \mid 17) = 1$, $(K' \mid 17) = -1$.
$1^2 \cdot 137 = 1^2 + 34 \cdot 2^2$, $(1 \mid 17) = 1$.
$5^2 \cdot 137 = 2 \cdot 36^2 + 17 \cdot 7^2$, $(5 \mid 17) = -1$.

(b) $r = 17, p = 2393 = 9^2 + 2 \cdot 34^2 \equiv 9^2 \pmod{17}$.
$(2 \mid 17)_4 = -1$.
$(p^{1/2} \pm M \mid 17) = (\pm 9 \pm 9 \mid 17) = 0$ or 1, so $(K \mid 17) = 1$,
$(K' \mid 17) = -1$.
$1^2 \cdot 2393 = 43^2 + 34 \cdot 4^2$, $(1 \mid 17) = 1$.
$5^2 \cdot 2393 = 2 \cdot 18^2 + 17 \cdot 59^2$, $(5 \mid 17) = -1$.

(c) $r = 41, p = 73 = 1^2 + 2 \cdot 6^2 \equiv 14^2 \pmod{41}$.
$(2 \mid 41)_4 = (17 \mid 41) = -1$.
$(p^{1/2} \pm M \mid 41) = (\pm 14 \pm 1 \mid 41) = -1$, so $(K \mid 41) = -1$, $(K' \mid 41) = 1$.
$7^2 \cdot 73 = 57^2 + 82 \cdot 2^2$, $(7 \mid 41) = -1$.
$1^2 \cdot 73 = 2 \cdot 4^2 + 41 \cdot 1^2$, $(1 \mid 41) = 1$.

(d) $r = 73, p = 19 = 1^2 + 2 \cdot 3^2 \equiv 26^2 \pmod{73}$.

$(2 \mid 73)_4 = (32 \mid 73) = 1.$

$(p^{1/2} \pm M \mid 73) = (\pm 26 \pm 1 \mid 73) = 1$, so $(K \mid 73) = (K' \mid 73) = 1$.

$3^2 \cdot 19 = 5^2 + 146 \cdot 1^2 = 2 \cdot 7^2 + 73 \cdot 1^2$, $(3 \mid 73) = 1$.

Now let q be odd.

Proof of Theorem 5. If $r \equiv 1 \pmod 8$, then $(2 \mid r) = 1$, and the conclusions of the theorem are immediate consequences of Lemma 11, parts (a) and (c), and Lemma 14.

Henceforth assume $r \equiv 5 \pmod 8$. Define s, s', z, and z' by

$$2^s \parallel HA + KM, \qquad 2^{s'} \parallel HC + K'N, \qquad 2^z \parallel HA - KM,$$
$$2^{z'} \parallel HC - K'N.$$

By Eqs. (4) and (4′) and Lemma 12, $s \equiv z \pmod 2$, and $s' \equiv z' \pmod 2$. It suffices, accordingly, to show that $(2^s \mid r) = (-1)^f$ and $(2^{1+s'} \mid r) = (-1)^{f'}$, in view of Lemma 14 and Lemma 11, part (b).

We first study $q \equiv 1 \pmod 4$. Considering Eqs. (1) (mod 4) reveals that H, K, and K' are odd. Then Eqs. (4) and (4′) yield

$$(HA + KM)(HA - KM) \equiv q(N^2 + 3B^2) \pmod 8,$$
$$q(HC + K'N)(HC - K'N) \equiv M^2 + 3D^2 \pmod 8,$$

respectively.

If N and B are both odd, then $2^2 \parallel (HA + KM)(HA - KM)$. Thus $s = 1$. Similarly, if M and D are odd, then $s' = 1$.

If $N + B$ is odd, then also $HA + KM$ is odd, so that $s = 0$. Similarly, if $M + D$ is odd, then $s' = 0$.

If N and B are even, then M and A are both odd. Choose signs so that all odd variables are $\equiv 1 \pmod 4$. Then $HA + KM \equiv 2 \pmod 4$, and $s = 1$. Similarly, if M and D are even, then $s' = 1$.

In summary, $s \equiv N + B + 1 \pmod 2$ and $s' \equiv M + D + 1 \pmod 2$. The conclusion in the theorem about f' in this case follows from noting that since H is odd, M and N have opposite parities.

It remains to investigate $q \equiv 3 \pmod 4$. Choose signs so that all odd variables are $\equiv 1 \pmod 4$. Considering Eqs. (1) (mod 8) yields the following:

If $q \equiv 3 \pmod 8$, then $H \equiv 1$ or $2 \pmod 4$, and $K, K' \equiv 0$ or $1 \pmod 4$.

If $q \equiv 7 \pmod 8$, then $H \equiv 0$ or $1 \pmod 4$, and K, $K' \equiv 1$ or $2 \pmod 4$.

Assume that $q \equiv 3 \pmod 8$. If $K \equiv 0 \pmod 4$, then A is odd, so that $HA + KM \equiv H \equiv 1$ or $2 \pmod 4$. Thus $s \equiv H - 1 \equiv H + K + 1 \pmod 2$. Similarly, if $K' \equiv 0 \pmod 4$, then $s' \equiv H + K' + 1 \pmod 2$.

Now let $K \equiv 1 \pmod 4$. If H is even, then M is odd, so that $s = 0 \equiv H +$

$K+1 \pmod 2$. Similarly, if $K' \equiv 1 \pmod 4$ and H is even, then $s' \equiv H + K' + 1 \pmod 2$.

Finally consider $K \equiv H \equiv 1 \pmod 4$. Then $HA + KM \equiv A + M \pmod 4$. Similarly, if $K' \equiv H \equiv 1 \pmod 4$, then $HC + K'N \equiv C + N \pmod 4$. By considering Eqs. (1) (mod 8), we obtain the following table, in which all variables are given (mod 4), except for p, which is given (mod 8):

p	A	M	C	N
1	1	1	2	0
3	2	0	1	1
5	1	1	0	2
7	0	2	1	1

In every case $A + M \equiv C + N \equiv 2 \pmod 4$. Hence

$$s = s' = 1 \equiv H + K + 1 \equiv H + K' + 1 \qquad \pmod 2.$$

In summary, if $q \equiv 3 \pmod 8$, then $s \equiv H + K + 1 \pmod 2$ and $s' \equiv H + K' + 1 \pmod 2$.

If $q \equiv 7 \pmod 8$, the analysis is almost identical to that for $q \equiv 3 \pmod 8$. In particular, if $H \equiv K \equiv K' \equiv 1 \pmod 4$, the above table remains valid, provided the entries 3 and 7 in the p column are interchanged.

Remark. If $r \equiv 1 \pmod 8$, then Theorem 5 yields predictive restrictions that are inclusive or exclusive according as $(q^{1/2} \mid r) = (q \mid r)_4 = 1$ or -1. Likewise, if $r \equiv 5 \pmod 8$ and $q \equiv 3 \pmod 4$, the restrictions are predictive. One may formulate the restrictions as

$$(-1)^K (K \mid r) = -(-1)^H u, \qquad (-1)^{K'} (K' \mid r) = (-1)^H (q \mid r)_4 u. \qquad (8)$$

Observe that the restrictions on $(-1)^K (K \mid r)$ and $(-1)^{K'} (K' \mid r)$ are inclusive or exclusive according as $(q \mid r)_4 = -1$ or 1. If, however, $r \equiv 5 \pmod 8$ and $q \equiv 1 \pmod 4$, then the restrictions involve the variables B and D, so they are not even predictive.

We now present the proofs of two special cases of Theorem 5, motivated by [8, Theorems 4 and 5] and [8, Theorem 6], respectively.

Proof of Theorem 6. Here $q = 3$, $r = 13$. Since $(p \mid 3) = 1$ by Lemma 3, Eq. (1a) is solvable with $H = 1$. In addition, $(p \mid 13) = 1$, and the reduced forms of the only classes in the principal genus of discriminant $-156 = -4 \cdot 39$ are $[1, 0, 39]$ and $[3, 0, 13]$, so that either (1b) is solvable with $K = 1$ or (1c) is solvable with $K' = 1$. This exclusive restriction is consistent with $(3 \mid 13)_4 = (4 \mid 13) = 1$. Then according to (8), $K = 1$ if and only if $u = -1$, while $K' = 1$ if and only if $u = 1$. The conclusion of the theorem now follows.

Here are some numerical examples. Note in this context that $p = A^2 + 39B^2$ implies $4^2p = 3(A \pm 13B)^2 + 13(A \mp 3B)^2$, while $p = 3C^2 + 13D^2$ implies $4^2p = (3C \pm 13D)^2 + 39(C \mp D)^2$.

p	M	N	$p^{1/2} \pm M (\text{mod } 13)$	K	A	B	K'	C	D
43	4	3	$\pm 6, \pm 2$	1	2	1	4	11	5
							4	15	1
61	7	2	$\pm 3, \pm 4$	4	1	5	1	4	1
				4	25	3			

Proof of Theorem 7. Here $q = 11$, $r = 5$. The reduced forms of discriminant -44 are $|1, 0, 11|$ and $|3, \pm 2, 4|$; all are in the principal genus. If $p = 3x^2 \pm 2xy + 4y^2$, then

$$4p = (x \pm 4y)^2 + 11x^2.$$

Thus Eq. (1a) is solvable with $H = 1$ or 2.

The only reduced forms in the principal genus of discriminant $-220 = -4 \cdot 55$ are $[1, 0, 55]$ and $[5, 0, 11]$. Hence either (1b) is solvable with $K = 1$ or (1c) is solvable with $K' = 1$. (This exclusive restriction is consistent with $(11 \mid 5)_4 = 1$.) Then Theorem 5 implies that (1b) is solvable with $K = 1$ if and only if $(-1)^H (Hp^{1/2} \pm M \mid 5) = 0$ or 1, while (1c) is solvable with $K' = 1$ if and only if $(-1)^H (Hp^{1/2} \pm M \mid 5) = 0$ or -1.

The conclusion as stated in Theorem 7 is now obtained by working out the possibilities (mod 5) of the above conditions, using the fact that $(p \mid 5) = 1$ implies either $5 \mid M$ or $5 \mid N$.

Here are some numerical examples. Note that $p = A^2 + 55B^2$ implies $4^2p = 11(A \pm 5B)^2 + 5(A \mp 11B)^2$, while $p = 11C^2 + 5D^2$ implies $4^2p = (11C \pm 5D)^2 + 55(C \mp D)^2$.

p	H	M	N	$Hp^{1/2} \pm M (\text{mod } 5)$	K	A	B	K'	C	D
31	2	5	3	± 2	4	1	3	1	1	2
					4	21	1			
59	2	15	1	± 1	1	2	1	4	3	13
								4	7	9
71	2	3	5	$0, \pm 1$	1	4	1	4	1	15
								4	9	7

8. Concluding Remarks

It is clear from Lemma 9 that the form(s) $[a, \pm b, c]$ of discriminant $-4qr$ determine a pair (K, K'). (The numbers are not unique, but we choose those whose absolute values are least.) Note that it is not always possible to recover the form when K or K' is given. For example, if $q = 73$ and $r = 89$, we find the following pairs (K, K'): $(1, 57)$, $(3, 19)$, $(9, 57)$, $(11, 11)$, $(13, 29)$, $(19, 3)$, $(29, 13)$, $(39, 39)$, $(57, 1)$, $(57, 9)$; the number 57 has two different "mates," and $K = 57$ is associated with the forms $[73, 0, 89]$ and $[2, 2, 3249]$.

In this example the values of K (or K') are divided into two subsets, in accordance with Theorem 5. The quadratic residues (mod 89) are 1, 9, 11, 39, 57; the quadratic nonresidues (mod 89) are 3, 13, 19, 29. Since $73 \equiv 89 \equiv 1 \pmod 8$, we may interchange q and r and still have a predictive situation. The prediction still applies to the classes of forms of discriminant $-4 \cdot 73 \cdot 89 = -25988$, so we obtain the same values of K and K'. But now the values of K and K' are considered with respect to the modulus 73. The quadratic residues are 1, 3, 9, 19, 57; the quadratic nonresidues are 11, 13, 29, 39. Note that if we make both predictions, with respect to $q = 73$ and with respect to $q = 89$, we are able to divide the values of K and K' into four subsets, rather than two: 1, 9, 57; 11, 39; 3, 19; 13, 29.

There are indications that the theory of spinor genera of binary quadratic forms of Estes and Pall [4] may yield a deeper understanding of the significance of Theorems 2, 4, and 5, and in particular, the phenomenon noted in the previous paragraph. We propose to probe this in a future study.

ACKNOWLEDGMENTS

We wish to express profound appreciation to Professor Ezra Brown for his extraordinary efforts in reorganizing this paper, and to Dr. Shmuel Schreiber, who contributed numerous suggestions for greater clarity and accuracy. We wish to thank the computing centers of the University of Pittsburgh, Bar-Ilan University, and the University of Illinois for providing access to their computing facilities.

REFERENCES

1. H. DAVENPORT,"The Higher Arithmetic," 3rd ed., Hutchinson, London, 1968.
2. L. E. DICKSON, "History of the Theory of Numbers, Vol. III, Quadratic and Higher Forms," Chelsea, New York, 1952.
3. L. E. DICKSON, "Introduction to the Theory of Numbers," Dover, New York, 1957.
4. D. R. ESTES AND G. PALL, Spinor genera of binary quadratic forms, *J. Number Theory* 5 (1973), 421–432.
5. J. HUNTER, "Number Theory," Oliver & Boyd, Edinburgh/London, 1964.
6. G. B. MATHEWS, "Theory of Numbers," Chelsea, New York.
7. J. B. MUSKAT AND A. L. WHITEMAN, The cyclotomic numbers of order twenty, *Acta Arith.* **17** (1970), 185–216.
8. J. B. MUSKAT AND Y.-C. ZEE, Sign ambiguities of Jacobi sums, *Duke Math. J.* **40** (1973), 313–334.
9. H. J. S. SMITH, "Report on the Theory of Numbers," Chelsea, New York, 1965.