ON THE CHARACTERISTIC ROOTS OF THE PRODUCT OF CERTAIN RATIONAL INTEGRAL MATRICES OF ORDER TWO

Thesis by

Lorraine Lois Turnbull Foster

In Partial Fulfillment of the Requirements
For the Degree of
Doctor of Philosophy

California Institute of Technology
Pasadena, California
1964
(Submitted April 28, 1964)

ACKNOWLEDGMENTS

I wish to thank my research advisor, Dr. Olga Taussky Todd, for her guidance and kind encouragement during the preparation of this thesis, and for bringing to my attention the area of study with which this thesis is concerned.

I also wish to acknowledge fellowships from the National Science Foundation, the Woodrow Wilson Foundation, and the General Electric Foundation, and research and teaching assistantships from the California Institute.

Further, I am indebted to the National Science Foundation for research grants which enabled me to use the IBM 709 and 7090 computers.

ABSTRACT

Let $N(p,q)$ denote the companion matrix of $x^2 + px + q$, for rational integers p and q, and let $M(p,q)=N(p,q)(N(p,q))'$. Further let $F(M(p,q))$ and $F(N(p,q))$ denote the fields generated by the characteristic roots of $M(p,q)$ and $N(p,q)$ over the rational field, R. This thesis is concerned with $F(M(p,q))$, especially in relation to $F(N(p,q))$. The principal results obtained are outlined as follows:

Let S be the set of square-free integers which are sums of two squares. Then $F(M(p,q))$ is of the form $R(\sqrt{c})$, where $c \in S$. Further, $F(M(p,q)) = R$ if and only if $pq = 0$. Suppose $c \in S$. Then there exist infinitely many distinct pairs of integers (p,q) such that $F(M(p,q)) = R(\sqrt{c})$.

Further, if $c \in S$, there exists a sequence $\{(p_n,q_n)\}$ of distinct pairs of integers such that $F(N(p_n,q_n)) = R(\sqrt{c})$ and $F(M(p_n,q_n)) = R(\sqrt{cd_n})$, where the d_n are some integers such that $(c,d_n) = 1$. If $c \in S$ and c is odd or $c = 2$, there exists a sequence $\{(p_n',q_n')\}$ of distinct pairs of integers such that $F(M(p_n',q_n')) = R(\sqrt{c})$ and $F(N(p_n',q_n')) = R(\sqrt{cd'})$, for some integers d_n' such that $(c,d_n') = 1$.

There are five known pairs of integers (p,q), with $pq \neq 0$ and $q \neq -1$, such that $F(M(p,q))$ and $F(N(p,q))$ coincide. For $q \equiv 2 (\mathrm{mod}\ 4)$ and for certain odd integers q, the fields $F(M(p,q))$ and $F(N(p,q))$ cannot coincide for any integers p.

Finally, for any integer $p \neq 0$ (or $q \neq 0, -1$) there exist at most a finite number of integers q (or p) such that the two fields coincide.

TABLE OF CONTENTS

INTRODUCTION

Let $A = (a_{ij})$ be a matrix of order n with elements in the complex field. We say A is normal if and only if $\overline{A}'A = A\overline{A}'$ where $\overline{A}' = (\overline{a_{ji}})$. It is known that if A is normal, with characteristic roots λ_i, $i = 1,\ldots,n$, then* the characteristic roots of $A\overline{A}'$ are given by $\lambda_i \cdot \overline{\lambda_i}$, $i = 1,\ldots,n$. Conversely, if the characteristic roots of $A\overline{A}'$ can be written as $\lambda_i\overline{\lambda_{\delta_i}}$, $i = 1,\ldots,n$, where $\{\delta_1,\ldots,\delta_n\}$ is some permutation of $\{1,\ldots,n\}$, then A is normal.** Hence it seems of interest to study the characteristic roots of $A\overline{A}'$ in comparison with the characteristic roots of A in the case of non-normal matrices A. Results are known which compare the magnitudes of these roots. Here a different point of view is adopted. The matrices A are restricted to a set of matrices of order two over the rational integers and the algebraic number fields in which the characteristic roots of A and $A\overline{A}'$ lie are compared.

Specifically, the matrices studied in this thesis are the companion matrices of the polynomials

$$x^2 + px + q ,$$

* This follows immediately from Theorem 1, [1].

** This was proven by A. J. Hoffman and O. Taussky in [2].

i. e., the matrices

$$\begin{bmatrix} 0 & 1 \\ -q & -p \end{bmatrix}$$

where p and q are rational integers. We denote the above matrix by N(p,q). Further, we define

$$M(p,q) = N(p,q)(N(p,q))' \quad .$$

Then we have

$$M(p,q) = \begin{bmatrix} 1 & -p \\ -p & p^2+q^2 \end{bmatrix}$$

and

$$(N(p,q))'N(p,q) = \begin{bmatrix} q^2 & pq \\ pq & 1+p^2 \end{bmatrix} \quad .$$

Evidently N(0,1) is normal and N(p,-1) is normal (and, in fact, symmetric) for all integers p. With these exceptions, N(p,q) is not normal.

We define functions $\delta(p,q)$ amd $\Delta(p,q)$ as follows:

$$\delta(p,q) = p^2 - 4q$$

$$\Delta(p,q) = (p^2 + q^2 + 1)^2 - 4q^2 \ .$$

We note that $\Delta(p,q)$ can also be expressed in the following three forms

$$(p^2 + (q + 1)^2)(p^2 + (q - 1)^2)$$

$$4p^2 + (p^2 + q^2 - 1)^2$$

$$4p^2q^2 + (p^2 - q^2 + 1)^2 \quad .$$

All four forms of $\Delta(p,q)$ are used in this work.

Let us denote the characteristic roots of N(p,q) and M(p,q) by $\lambda_N^{\pm}(p,q)$ and $\lambda_M^{\pm}(p,q)$, respectively, so that

$$\lambda_N^{\pm}(p,q) = (-p \pm \sqrt{\delta(p,q)})/2$$

$$\lambda_M^{\pm}(p,q) = (p^2 + q^2 + 1 \pm \sqrt{\Delta(p,q)})/2 \quad .$$

We denote the fields which $\lambda_N^{\pm}(p,q)$ and $\lambda_M^{\pm}(p,q)$ generate over the rational number field, R, by F(N(p,q)) and F(M(p,q)), respectively.

We define $g_\delta(p,q)$ to be the square-free part of $\delta(p,q)$ if $\delta(p,q) \neq 0$, and $g_\delta(p,q) = 0$ if $\delta(p,q) = 0$. Similarly we define $g_\Delta(p,q)$. Then we have:

$$F(N(p,q)) = R(\sqrt{\delta(p,q)}) = R(\sqrt{g_\delta(p,q)})$$
$$F(M(p,q)) = R(\sqrt{\Delta(p,q)}) = R(\sqrt{g_\Delta(p,q)}) \quad .$$

This thesis is therefore concerned with the relationships between $g_\delta(p,q)$ and $g_\Delta(p,q)$. Occasional other related problems are also given some treatment here.

Many of the conjectures proven in this work were suggested by calculations performed on the IBM 709 and 7090 computers. The question of the number of solutions (p,q) of the equation

(1) $\quad F(M(p,q)) = F(N(p,q))$

with $q \neq -1$ and $pq \neq 0$ is still unanswered. (Since N(p,-1) is symmetric, it has real roots. Hence, by the normality of N(p,-1), $\lambda_M^{+}(p,-1) = (\lambda_N^{+}(p,-1))^2$ so that F(M(p,-1)) $= R(p(p^2+4)^{\frac{1}{2}}) = R((p^2+4)^{\frac{1}{2}}) = F(N(p,-1))$, for all p. Also, it is easily seen that F(M(p,0)) = F(N(p,0)) and $F(M(0,-n^2)) = F(N(0,-n^2))$, for all integers p and n.) The computer data and a number of results lead us to conjecture that there exist only finitely many pairs (p,q) with $q \neq -1$ and $pq \neq 0$ which are solutions of equation 1.

I. THE NATURE OF F(M(p,q))

The following two theorems will be useful in this and subsequent chapters.

Theorem A. Let P be a prime congruent to 1 or 2 modulo 4. Then there exist integers x and y such that

$$x^2 - Py^2 = -1 \ . \ \blacksquare$$

For P $\equiv$ 1(mod 4), the conclusion of this theorem follows from Theorem 107 of [3], pages 203-4. For P = 2, the conclusion of Theorem A follows from the fact that $1 + \sqrt{2}$ is a solution* of $x^2 - 2y^2 = -1$.

Theorem B. Let c be a positive integer which is not a perfect square. Then the equation

$$x^2 - cy^2 = 1$$

has a fundamental solution $x_1 + \sqrt{c}\,y_1$ and all other solutions are of the form $\pm x_n \pm \sqrt{c}\ y_n$ where

$$x_n + \sqrt{c}\,y_n = (x_1 + \sqrt{c}\,y_1)^n \ , \quad n = 1, 2, \ldots \quad . \ \blacksquare$$

This theorem follows from Theorem 104 of [3], pages 197-9.

The first significant fact which we notice concerning the nature of F(M(p,q)) is expressed in the following

* A number $s+t\sqrt{D}$ is said to be a solution of the equation $x^2 - y^2D = H$ if and only if $s^2 - t^2D = H$. This usage is not uncommon.

theorem:

Theorem 1.1. $F(M(p,q)) = R$ if and only if $pq = 0$.

Proof: Without restricting generality, we can consider p and q to be non-negative integers. We first assume that $pq \neq 0$ and show that $F(M(p,q))$ cannot be rational. Thus we wish to show that*

$$\Delta(p,q) = (p^2 + q^2 - 1)^2 + 4p^2 \neq \square \ .$$

Now, $(p^2 + q^2 - 1)^2 + 4p^2 = (p^2 + q^2)^2 + 2(p^2 - q^2) + 1.$

Suppose that $p > q > 0$. Observe that

$$(p^2 + q^2 + 1)^2 = (p^2 + q^2)^2 + 2(p^2 + q^2) + 1 > \Delta(p,q).$$

Also, $2(p^2 - q^2) + 1 > 0$, so that

$$(p^2 + q^2)^2 < \Delta(p,q) < (p^2 + q^2 + 1)^2.$$

Hence in this case: $\Delta(p,q) \neq \square$.

Now suppose that $q > p > 0$. We have

$$(p^2 + q^2 - 1)^2 = (p^2 + q^2)^2 - 2(p^2 + q^2) + 1 < \Delta(p,q).$$

Also, $2(p^2 - q^2) + 1 = -2|p^2 - q^2| + 1 < 0$, so that

$$(p^2 + q^2 - 1)^2 < \Delta(p,q) < (p^2 + q^2)^2 ,$$

and in this case also, $\Delta(p,q) \neq \square$. In the remaining case, $q = p > 0$ so that $\Delta(p,q) = \Delta(p,p) = (2p^2)^2 + 1 \neq \square$.

Hence for $pq \neq 0$, $\Delta(p,q) \neq \square$.

Now observe that $\Delta(0,q) = (q^2 - 1)^2$ and $\Delta(p,0) = (p^2 + 1)^2$, and the proof of the theorem is complete.■

For $pq \neq 0$, the above theorem tells us that

* In this thesis "$\square$" will always denote a square of a rational integer.

$g_\Delta(p,q) \neq 1$. Further, since $g_\Delta(p,q)$ is the square free part of $(p^2 + (q+1)^2)(p^2 + (q-1)^2)$, we conclude that if $pq \neq 0$ then $g_\Delta(p,q) > 1$, and $g_\Delta(p,q)$ is of the form $2^\alpha d$, where α is either one or zero, and d is a product of distinct primes of the form $4N+1$. We ask what numbers $2^\alpha d$ are actually found in the set $\{g_\Delta(p,q) \mid pq \neq 0\}$. The following theorem gives us a partial answer to this question.

Theorem 1.2. Let P be a prime congruent to one or two modulo four. Then there exist infinitely many pairs of integers (p,q) such that $F(M(p,q)) = R(\sqrt{P})$.

Proof: Let $x_1 + y_1\sqrt{P}$ denote the fundamental solution* of the equation $x^2 - Py^2 = -1$. Define integers x_n and y_n by

$$x_n + y_n\sqrt{P} = (x_1 + y_1\sqrt{P})^{2n-1}, \qquad n = 1, 2, \ldots .$$

We can assume that x_1 and y_1 were chosen to be positive so that the sequences $\{x_n\}$ and $\{y_n\}$ are positive and strictly increasing. Further, $x_n^2 - Py_n^2 = -1$, $n = 1, 2, \ldots$. Now define $p_n = 2x_n$. Then $0 < p_1 < p_2 < \ldots$. Finally,

$$\Delta(p_n,1) = p_n^2(p_n^2 + 4) = p_n^2(4x_n^2 + 4) = 4p_n^2Py_n^2,$$

so that $F(M(p_n,1)) = R(\sqrt{P})$, $n = 1, 2, \ldots$. ∎

Since every prime $P \equiv 1$ or $2 \pmod 4$ can be expressed as a sum of two squares, it will be seen that Theorem 1.2 is in fact a special case of the following general theorem.

Theorem 1.3. Let c be any integer of the form a^2+b^2 which

* Such a solution exists by Theorem A.

is not a perfect square. Then there exists a sequence of pairs of integers $\{(p_n,q_n)\}$ such that the sequences $\{p_n\}$ and $\{q_n\}$ are strictly increasing, and such that $F(M(p_n,q_n)) = R(\sqrt{c})$, $n = 1, 2, \ldots$.

Proof: Consider the equation

(1.1) $u^2 - cv^2 = ca^2$.

Since $c^2 - cb^2 = c(c - b^2) = ca^2$, $c + b\sqrt{c}$ is a solution of equation 1.1. Consider also the equation

(1.2) $x^2 - cy^2 = 1$.

Since c is not a perfect square, this equation is solvable, by Theorem B. Let $s_1 + t_1\sqrt{c}$ denote a solution of equation 1.2 with s_1 and $t_1 > 0$. Now define s_n, t_n, x_n, and y_n by

$$s_n + t_n\sqrt{c} = (s_1 + t_1\sqrt{c})^n$$

$$x_n + y_n\sqrt{c} = (s_1 + t_1\sqrt{c})^{2n} , \quad n = 1, 2, \ldots \quad .$$

(This construction, though it may seem in part superfluous for the moment, is used to facilitate the proof of a later theorem, Theorem 2.8.) Clearly $s_n + t_n\sqrt{c}$ and $x_n + y_n\sqrt{c}$ are solutions of equation 1.2 for each n. Also

$$\begin{aligned} x_n + y_n\sqrt{c} &= ((s_1 + t_1\sqrt{c})^n)^2 = (s_n + t_n\sqrt{c})^2 \\ &= (s_n^2 + t_n^2c) + \sqrt{c}(2s_nt_n), \text{ for } n \geq 1. \end{aligned}$$

Clearly $x_n > x_{n-1}$ and $y_n > y_{n-1}$ for all $n > 1$. Define

(1.3) $$\begin{aligned} u_n + v_n\sqrt{c} &= (c + b\sqrt{c})(x_n + y_n\sqrt{c}) \\ &= (cx_n + cby_n) + \sqrt{c}(bx_n + cy_n), \ n \geq 1. \end{aligned}$$

It is clear that $u_n + v_n\sqrt{c}$ is a solution of equation 1.1 for $n \geq 1$. Furthermore $u_n \equiv 0(\text{mod } c)$ and $v_n \equiv b(\text{mod } c)$, since $x_n \equiv s_n^2 \equiv 1(\text{mod } c)$, $n \geq 1$. It follows that

$$8u_n \equiv 0 (\text{mod } 4c), \quad 8v_n \equiv 8b (\text{mod } 4c),$$

so that there exist integers k_n and m_n such that

(1.4) $m_n = 8u_n/4c, \quad k_n = 8(v_n - b)/4c, \quad n \geq 1.$

Since we may assume that $a, b > 0$, it is evident that $u_n > u_{n-1}$ and $v_n > v_{n-1}$. Thus the integers k_n form a strictly increasing sequence. Now

$$(8u_n)^2 - c(8v_n)^2 = 64ca^2, \text{ for } n \geq 1,$$

by equation 1.1. Hence from equation 1.4 we have:

$$\begin{aligned} 64ca^2 &= (4cm_n)^2 - c(4ck_n + 8b)^2 \\ &= (4c)^2 m_n^2 - (4c)^2 ck_n^2 - 64c^2k_nb - 64cb^2. \end{aligned}$$

Rearranging we have

$$(4c)^2(m_n^2 - ck_n^2 - 4k_nb) = 64c(a^2 + b^2) = (4c)^2 4 .$$

Hence we have

(1.5) $m_n^2 = ck_n^2 + 4k_nb + 4, \quad n \geq 1$.

Recall that $\Delta(p,q) = (p^2 + (q + 1)^2)(p^2 + (q - 1)^2)$.

Let $p_n = k_na, \quad q_n = k_nb + 1, \quad n \geq 1.$

Then the sequences $\{p_n\}$ and $\{q_n\}$ are strictly increasing. Finally,

$$\begin{aligned} p_n^2 + (q_n - 1)^2 &= k_n^2a^2 + k_n^2b^2 = k_n^2c \\ p_n^2 + (q_n + 1)^2 &= k_n^2a^2 + k_n^2b^2 + 4k_nb + 4 \\ &= k_n^2c + 4k_nb + 4 = m_n^2 \end{aligned}$$

by equation 1.5. Hence $\Delta(p_n,q_n) = k_n^2m_n^2c$ and $F(M(p_n,q_n)) = R(\sqrt{k_n^2m_n^2c}) = R(\sqrt{c}), n \geq 1.$ ∎

For illustration, let us give an example of the above construction of pairs (p_n,q_n). Suppose $c = 10$. Then we can set $a = 3$, $b = 1$. Also, we can choose

$$s_1 + t_1\sqrt{10} = (3 + \sqrt{10})^2 = 19 + 6\sqrt{10} .$$

Then $x_1 + y_1\sqrt{10} = (19 + 6\sqrt{10})^2 = (721 + 228\sqrt{10})$,

$$m_1 = 8u_1/4c = 2c(x_1 + y_1)/c = 2(x_1 + y_1) = 2\cdot 949 ,$$

and
$$k_1 = 2(v_1 - b)/c = 2(b(x_1 - 1) + cy_1)/c$$
$$= 2(b(x_1 - 1)/c + y_1) = 2(72 + 228) = 2\cdot 300,$$

by equation 1.3. As in the above proof, we define

$$p_1 = k_1a = 3\cdot 2\cdot 300 = 1800,$$
$$q_1 = k_1b + 1 = 2\cdot 300 + 1 = 601.$$

Hence $p_1^2 + (q_1 - 1)^2 = 4\cdot 300^2(9 + 1) = 10\cdot\Box$

and
$$p_1^2 + (q_1 + 1)^2 = 4(810,000 + 90601) = 4\cdot 900,601$$
$$= 4\cdot 949^2,$$

so that $F(M(1800,601)) = R(\sqrt{10})$.

Since the product of two integers which are sums of squares can also be expressed as a sum of squares, it is evident from previous remarks and from Theorem 1.3 that the set of fields $\{F(M(p,q)) \mid pq \neq 0\}$ is precisely the set $\{R(\sqrt{c}) \mid c \neq 1,\ c = \prod P_i,\ P_i \equiv 1, 2 (\text{mod } 4),\ P_i \text{ prime}\}$.

From a non-field theoretic standpoint, Theorem 1.3 tells us that for any sum of two squares, c, which is not a perfect square, there exist pairs (p,q) such that $\Delta(p,q) = c\cdot\Box$. We ask if perhaps there exist pairs (p,q) such that $\Delta(p,q) = c$ for such c. The answer is in the negative, as is clear from the following simple theorems, stated here without proof.

Theorem 1.4. $\Delta(p,q) \equiv 0, 1, 4,$ or $5 \pmod 8$ and there exist pairs (p,q) such that each of these congruences is satisfied.▮

Theorem 1.5. $\Delta(p,q) \equiv 0, 1, 4, 5,$ or $9 \pmod{16}$ and each of these cases occurs.▮

II. CERTAIN RELATIONS BETWEEN F(M(p,q)) AND F(N(p,q))

The following theorem will be of use in this chapter:

Theorem C. If ξ is a simple root of the congruence

$$f(x) \equiv 0 (\text{mod } P)$$

where P is prime, then there exists precisely one root η modulo P^{α} of the congruence

$$f(x) \equiv 0 (\text{mod } P^{\alpha})$$

such that $\xi \equiv \eta$ (mod P).

For a proof of this theorem see for instance [3], Theorem 50, page 87.

In the following work we write: $P^{\alpha} \overline{|}\ b$ if and only if $P^{\alpha} | b$ and $P^{\alpha+1} \nmid b$, where α and b are integers, $\alpha > 0$, and P is prime. (This notation is found in [6], for example.)

The following theorems are concerned with various comparisons of the fields F(M(p,q)) and F(N(p,q)). We will eventually prove that there exist infinitely many pairs (p,q), with $q \neq -1$, $pq \neq 0$, such that $g_{\delta}(p,q) | g_{\Delta}(p,q)$. Then we will show that there also exist infinitely many pairs (p,q) with $q \neq -1$, $pq \neq 0$, such that $g_{\Delta}(p,q) | g_{\delta}(p,q)$.

We observe that if d is an integer which is square-free, and $d | (p^2 + (q - 1)^2, \delta(p,q))$, then $d | (q + 1)^2$ so that in fact $d | (q + 1)$. Then $d | (p^2 + 4)$. These facts suggested the following theorems:

Theorem 2.1. Suppose d is a positive integer of the form t^2s, where s is odd. Further suppose that $d \mid (p^2+4)$, for some integer $p > 0$. Then there exists an integer $q \neq 0, -1$ such that $F(N(p,q)) = R(\sqrt{d})$ and $F(M(p,q)) = R(\sqrt{dc})$, where c is some integer such that $(c,d) = 1$.

Proof: We define an integer f as follows:

$$f = \begin{cases} d & \text{if } t \text{ is odd} \\ d/4 & \text{if } t \text{ is even} \end{cases} .$$

Since $p^2 \equiv 0, 1, 4, \text{ or } 9 \pmod{16}$, it is clear that $p^2 + 4 \not\equiv 0 \pmod{16}$. Hence $t \equiv 1$ or $2 \pmod 4$ and $s \equiv 1 \pmod 4$, since $p^2 + 4$ can have no prime factors of the form $4N+3$. Hence $f \equiv 1 \pmod 4$. We define $d' = (p^2 + 4)/f$. Clearly d' is an integer and $d' \equiv 0$ or $1 \pmod 4$. We can therefore define a positive integer k by

$$k = \begin{cases} 2fd' + 1 & \text{if } d' \equiv 1 \pmod 4 \\ f(d' + 1) + 1 & \text{if } d' \equiv 0 \pmod 8 \\ 3f(d' + 1) + 1 & \text{if } d' \equiv 4 \pmod 8 \end{cases} .$$

Observe that in all cases $k^2 \equiv d' \pmod 4$. Also, when d' is even, $k^2 \not\equiv d' \pmod 8$. We let q be the integer defined as follows:

$$q = (f(d' - k^2)/4) - 1.$$

Evidently $k^2 > d'$ so that $q < -1$. Then

$$\begin{aligned} \delta(p,q) &= p^2 - 4q = p^2 + 4 - 4(q + 1) \\ &= fd' - 4f(d' - k^2)/4 = fk^2 . \end{aligned}$$

Also,
$$\begin{aligned} p^2 + (q - 1)^2 &= p^2 + (q + 1)^2 - 4q \\ &= f(k^2 + f((d' - k^2)/4)^2) = fc_1 \end{aligned}$$

where c_1 is defined by this equation. Now it is clear that $(f,c_1) = 1$, since $(f,k) = 1$, by the construction of k. Also, since $f \mid (p^2 + 4)$ and $f \equiv 1 \pmod 4$, we must have $(f,p) = 1$. Now $f \mid (q + 1)$ so we must have $(f,(p^2 + (q + 1)^2)) = 1$. Let $c = c_1(p^2 + (q + 1)^2)$. Then $(f,c) = 1$,

$$F(N(p,q)) = R(\sqrt{f}) = R(\sqrt{d}),$$

and

$$F(M(p,q)) = R(\sqrt{fc}) = R(\sqrt{dc}) .$$

If d is odd, then $(d,c) = (f,c) = 1$, and the theorem is proven. If d is even then $d' = (p^2 + 4)/f = 4((p^2 + 4)/d) \equiv 0 \pmod 4$, $k^2 \equiv 0 \pmod 4$, and $k^2 \not\equiv d' \pmod 8$. Thus

$$c_1 = k^2 + f((d' - k^2)/4)^2 \equiv 0 + 1\cdot 1 \equiv 1 \pmod 2).$$

Also, since d is even, we know that p is even and hence

$$p^2 + (q + 1)^2 = p^2 + f^2((d' - k^2)/4)^2$$
$$\equiv 0 + 1\cdot 1 \equiv 1 \pmod 2 .$$

Thus $(2,c) = 1$ so that $(d,c) = (4f,c) = 1$ and the theorem is proven.∎

We recall that $g_\delta(p,q)$ and $g_\Delta(p,q)$ denote the unique square-free integers such that:

$$F(N(p,q)) = R(\sqrt{g_\delta(p,q)}), \quad F(M(p,q)) = R(\sqrt{g_\Delta(p,q)}).$$

We have the following theorem:

Theorem 2.2. For every integer $p > 0$ there exist infinitely many distinct integers q such that $g_\delta(p,q) \mid g_\Delta(p,q)$ and $|g_\delta(p,q)| \neq 1$.

Proof: We note that $p^2 + 4$ is of the form $2^\alpha t$, where $\alpha = 0$, 2, or 3, and t is a product of primes of the form

4N+1. We first assume that $p \neq 2$. Then we can choose an odd, square-free integer $d > 1$ such that $d \mid (p^2 + 4)$. This is true if $p = 1$, for in this case we choose $d = 5$. For $p > 2$ we observe that $p^2 + 4 = 2^{\alpha}t > 8$ so that $t > 1$ and hence we can choose d to be any prime factor of t. We define $d' = (p^2 + 4)/d$. Since $d' \equiv 0$ or $1 (\bmod 4)$ and d is odd, we can choose a positive integer e so that $e^2 \equiv d' (\bmod 4)$ and $(e,d) = 1$. We then choose

$$k_n = 2dn + e, \qquad n = 0, 1, 2, \ldots \quad .$$

Clearly, $k_n^2 \equiv e^2 \equiv d' (\bmod 4)$, $(k_n,d) = 1$, and $k_n > 0$, $n = 0, 1, 2, \ldots$. We then define

$$(2.1) \quad q_n = (d(d' - k_n^2)/4) - 1, \qquad n = 0, 1, 2, \ldots \quad .$$

As in the proof of Theorem 2.1 (with $f = d$), we observe that

$$F(N(p,q_n)) = R(\sqrt{d})$$

and
$$F(M(p,q_n)) = R(\sqrt{dc_n}),$$

where $c_n = (p^2 + (q_n + 1)^2)(k_n^2 + d((d' - k_n^2)/4)^2)$. Since $d \mid (p^2 + 4)$, $d \mid (q_n + 1)$, $(d,k_n) = 1$, and d is odd, we conclude that $(d,c_n) = 1$, $n = 0, 1, 2, \ldots$. Clearly the sequence $\{q_n\}$ is strictly decreasing. Further,

$$g_\delta(p,q_n) = d > 1 \quad \text{and} \quad g_\Delta(p,q_n) = dc_n' \; ,$$

where c_n' is the square-free part of c_n. Hence, if $p \neq 2$ the theorem is proven.

Now suppose $p = 2$. Let

$$(2.2) \qquad q_n = 1 - 2n^2, \qquad n = 1, 2, \ldots \quad .$$

Then
$$p^2 - 4q_n = 4(1 - q_n) = 2\cdot(2n)^2.$$

Also
$$\Delta(p,q_n) = (p^2 + q_n^2 - 1)^2 + (2p)^2$$

so that $\Delta(2,q_n) = (3 + q_n^2)^2 + 16.$

Now $3 + q_n^2 \equiv 3 + 1 \equiv 4 (\text{mod } 8)$

so that
$$\Delta(2,q_n)/16 = ((3 + q_n^2)/4)^2 + 1$$
$$\equiv 1 + 1 \equiv 2 (\text{mod } 4)$$

and thus $\Delta(2,q_n) = 2c_n'\Box$, where c_n' is some square-free odd integer. Also, $g_\delta(2,q_n) = 2$ and $g_\Delta(2,q_n) = 2c_n'$. Evidently the sequence $\{q_n\}$ is strictly decreasing. Hence the theorem is proven. ▮

Corollary. If $p > 1$ there exists an integer q such that $|q| \leq 3p^2$, $q \neq -1$, $g_\delta(p,q) \mid g_\Delta(p,q)$, and $g_\delta(p,q) \neq 1$.

Proof: (We first note that the requirement $q \neq -1$ is necessary to make the corollary meaningful, since $g_\delta(p,-1) = g_\Delta(p,-1) \neq 1$ trivially for $p \neq 0$. We also note that an examination of cases demonstrates that the conclusion of the corollary is false in the case $p = 1$.) From the proof of Theorem 2.2 we see that if $p = 2$ we can choose $q = 1 - 2\cdot 2^2 = -7$ (as in equation 2.2) and all of the assertions of the corollary are satisfied. Hence we may assume $p > 2$. Then we choose d and d' as directed in the proof of Theorem 2.2. There are four possible cases.

Case I: $d' = 4$. Take $n = 0$ and $e = 4$ in the proof of Theorem 2.2. (Clearly $e^2 \equiv d'(\text{mod } 4)$ and $(e,d) = 1$ so that the conditions of the theorem are fulfilled.) Then we define

$$q_0 = d(d' - e^2)/4 - 1$$

as in equation 2.1, and conclude as in Theorem 2.2 that

$$g_\delta(p,q_o) = d > 1, \quad g_\Delta(p,q_o) = dc'_o,$$

(since d is square-free). Now $q_o + 1 = d(4 - 16)/4$ $= -3d \neq 0$ so that $q_o \neq -1$ and $|q_o| < (p^2 + 4) + 1 < 3p^2$, since $p^2 \geq 9$ by hypothesis. Thus the corollary is true in this case.

Case II. $d' \equiv 0 \pmod 4$, $d' > 4$. Take $e = 2$. Then $(d,e) = 1$ and $e^2 \equiv d' \pmod 4$. Further,

$$0 < q_o + 1 = (d(d' - e^2))/4 < dd'/4 = (p^2 + 4)/4$$
$$< 3p^2$$

and $q_o \neq -1$, so as in the case above we find the corollary to be true.

Case III. $d' = 1$. In this case $p^2 + 4 = d$. Obviously, $(3,d) = 1$. Also, $3^2 \equiv d' \pmod 4$ so that we may choose $e = 3$ in this case. Then

$$q_o + 1 = d(d' - e^2)/4 = d(1 - 9)/4 = -2d \neq 0.$$

Hence $|q_o| = |-2d - 1| = 2d + 1 = 2p^2 + 8 + 1 \leq 3p^2$ and as above we have the desired result.

Case IV. $d' \equiv 1 \pmod 4$, $d' > 1$. We choose $e = 1$. Clearly $(d,e) = 1$, and $e^2 \equiv d' \pmod 4$. Then

$$0 < q_o + 1 = d(d' - e^2)/4 < 3p^2, \; q_o \neq -1$$

and we have proven the corollary. ∎

In Theorem 2.1 we required that d be positive (and of the form $s \cdot \square$, where s is odd). A similar theorem dealing instead with $-d$ is as follows:

Theorem 2.3. Suppose p is even, $p > 0$. Suppose also that d is a positive integer of the form $t^2 s$, where s is odd, and that $d \mid (p^2 + 4)$. Then there exists an integer $q > 0$ such that $F(N(p,q)) = R(\sqrt{-d})$ and $F(M(p,q)) = R(\sqrt{cd})$, for some integer c such that $(c,d) = 1$.

Proof: We note that the requirement that p be even is necessary. For, if $F(N(p,q)) = R(\sqrt{-d})$ then $p^2 - 4q = -s\cdot\square$ so that $p^2 \equiv -\square(\text{mod } 4)$ and hence $p^2 \equiv 0(\text{mod } 4)$.

We may write $p = 2p_1$, where p_1 is an integer. We define

$$e = \begin{cases} d & \text{if } t \text{ is odd} \\ d/4 & \text{if } t \text{ is even} \end{cases} .$$

We also define $d' = (p^2 + 4)/e$ and observe that $d'/4$ is an integer which we denote by d''. Since e is odd we can choose a positive integer j such that $(j,e) = 1$ and $d'' \not\equiv j$ (mod 2). We let

$$q = e(d'' + j^2) - 1 \geq 1(1 + 1) - 1 > 0.$$

Then $p^2 - 4q = ed' - 4ed'' - 4ej^2 = -4ej^2$

so that $F(N(p,q)) = R(\sqrt{-4e}) = R(\sqrt{-d})$. Also

$$\begin{aligned} p^2 + (q-1)^2 &= -4ej^2 + e^2(d'' + j^2)^2 \\ &= e(-4j^2 + e(d'' + j^2)^2) = eh_1, \end{aligned}$$

where h_1 is defined by this equation and is evidently odd by our choice of j. Further,

$$p^2 + (q + 1)^2 = 4p_1^2 + e^2(d'' + j^2)^2 = h_2,$$

where h_2 is defined by this equation and is odd. Let $c = h_1h_2$. Then

$$F(M(p,q)) = R(\sqrt{ec}) = R(\sqrt{dc}).$$

Since $(e,j) = 1$, e is odd, and $e \mid (p^2 + 4)$, it is clear that $(e,c) = 1$. Since h_1 and h_2 are odd, $(2,c) = 1$. Hence $(4e,c) = 1$ so that certainly $(d,c) = 1$.∎

In Theorems 2.1 and 2.3 we required that the square-free part of d be odd. We now suppose that the square-free part of d is even. We are able to consider the case in which $F(N(p,q)) = R(\sqrt{d})$ and the case in which $F(N(p,q)) = R(\sqrt{-d})$, $d > 0$, simultaneously.

Theorem 2.4. Suppose d is a positive integer of the form $2t^2s$, where s is a square-free odd integer. Suppose also that $d \mid (p^2 + 4)$ and $e^2 = 1$. Then:

(a) If $p^2 + 4 \equiv 0 \pmod 8$, there exists an integer $q \neq 0, -1$, such that $F(N(p,q)) = R(\sqrt{ed})$ and $F(M(p,q)) = R(\sqrt{dc})$, where c is an integer such that $(c,d) = 1$.

(b) If $p^2 + 4 \not\equiv 0 \pmod 8$, then there exist no integers q and c such that $F(N(p,q)) = R(\sqrt{ed})$, $F(M(p,q)) = R(\sqrt{cd})$, and $(c,d/t^2) = 1$.

Proof: Since $2 \mid d \mid (p^2 + 4)$, we can define an integer p_1 by $p_1 = p/2$. To prove (a) we suppose that $p^2 + 4 \equiv 0 \pmod 8$. We let

$$f = \begin{cases} d & \text{if } t \text{ is odd} \\ d/4 & \text{if } t \text{ is even} \end{cases} .$$

Let d' be the integer defined as follows:

$$d' = (p^2 + 4)/f .$$

Clearly $2 \,\rceil f$ and $2^2 \rceil\, d'$, so that we can define odd integers d'' and f_1 by the following:

$$d'' = d'/4, \quad f_1 = f/2 .$$

Choose an even positive integer j so that $(f_1,j) = 1$, $j > 2d''$, and define

$$q = f(d'' - ej^2) - 1.$$

If $e < 0$ then $q \geq 2 - 1 = 1$, and if $e > 0$ then

$$q \leq f(d'' - 4d'') - 1 < -1.$$

Hence $q \neq 0, -1$. Now,

$$p^2 - 4q = fd' - 4f(d'' - ej^2) = 4fej^2$$

so that $F(N(p,q)) = R(\sqrt{ef}) = R(\sqrt{ed})$. Also,

$$\begin{aligned} p^2 + (q-1)^2 &= 4fej^2 + f^2(d'' - ej^2)^2 \\ &= 2f(2j^2e + f_1(d'' - ej^2)^2) = 2fh_1, \end{aligned}$$

and

$$\begin{aligned} p^2 + (q+1)^2 &= 4p_1^2 + f^2(d'' - ej^2)^2 \\ &= 4(p_1^2 + f_1^2(d'' - ej^2)^2) = 4h_2, \end{aligned}$$

where h_1 and h_2 are defined by these equations. Now since $p^2 + 4 \equiv 0 \pmod 8$, we know that p_1 is odd. Also, since $f_1d'' \mid (p^2 + 4)$ and d'' and f_1 are odd, we conclude that $f_1 \equiv 1 \equiv d'' \pmod 4$. Since j is even,

$$h_1 \equiv 2\cdot 0 + 1(1 + 0)^2 \equiv 1 \pmod 4$$

and

$$h_2 \equiv p_1^2 + f_1^2(d'' - ej^2)^2 \equiv 1 + 1 \equiv 2 \pmod 4.$$

Hence $\Delta(p,q) = 4^2fh_1(h_2/2) = 4^2cf$, where c is an odd integer and $(c,f) = 1$, since $(f_1,j) = 1$. Then $(f,c) = 1 = (4f,c)$ so that $(d,c) = 1$. Also $F(M(p,q)) = R(\sqrt{cf})) = R(\sqrt{dc})$. Thus (a) is proven.

To prove (b) we assume that $p^2 + 4 \not\equiv 0 \pmod 8$, so that in fact, $p^2 + 4 \equiv 4 \pmod 8$, since p is even. We suppose that (b) is false. Then there exist integers q and c (we may surely assume that c is square-free) such that:

$$(2.3) \quad F(N(p,q)) = R(\sqrt{ed}) = R(\sqrt{2se})$$

$$(2.4) \quad F(M(p,q)) = R(\sqrt{dc}) = R(\sqrt{2sc}),$$

where $1 = (c,d/t^2) = (2s,c)$. Since $p^2 + 4 \equiv 4 (\mathrm{mod}\ 8)$, $(p^2 + 4)/4s$ is an odd integer, say g. Now

$$\delta(p,q) = p^2 + 4 - 4(q + 1) = 4sg - 4(q + 1)$$

so that from equation 2.3,

$$4sg - 4(q + 1) = 2k^2se$$

for some positive integer k. Since s is odd we conclude that $k/2$ is a positive integer, say m. Thus

$$q + 1 = s(g - 2m^2e).$$

Hence

$$\begin{aligned} p^2 + (q - 1)^2 &= p^2 - 4q + (q + 1)^2 \\ &= 2sk^2e + s^2(g - 2m^2e)^2 \\ &= s(2k^2e + s(g - 2m^2e)^2) = sn_1 \end{aligned}$$

and

$$p^2 + (q + 1)^2 = 4p_1^2 + s^2(g - 2m^2e)^2 = n_2,$$

where n_1 and n_2 are defined by these equations and are both odd since s and g are both odd. Hence $\Delta(p,q) = sn_1n_2$. But, according to equation 2.4 we must have $\Delta(p,q) = 2sc\cdot\square$. But this is a contradiction since s, n_1, and n_2 are odd. Hence the truth of (b) is established. (We observe that in the statement of Theorem 2.4 we need not restrict e to be ± 1. In fact, the only property of e used in the proof of the theorem is that $(d,e) = 1$.) ■

We use the preceding theorems to prove the following comprehensive statement:

Theorem 2.5. Let d be a square-free positive integer of the form $a^2 + b^2$. Then there exist sequences $\{p_n\}$, $\{q_n\}$, and

$\{q_n'\}$ such that $p_n < p_{n+1}$, $q_n \neq 0, -1$, $F(N(p_n,q_n)) = R(\sqrt{d})$, $F(M(p_n,q_n)) = R(\sqrt{dc_n})$, $F(N(p_n,q_n')) = R(\sqrt{-d})$, and $F(M(p_n,q_n')) = R(\sqrt{dc_n'})$, where c_n and c_n' are integers which are relatively prime to d, n = 1, 2, ...

Proof: We consider two cases: in the first case d is odd and in the second case d is even. In the first case d is of the form $\prod_{i=1}^{t} P_i$, where each P_i is equal to one or to a prime of the form $4N + 1$, and the P_i are distinct. Clearly each of the equations

$$x^2 + 1 \equiv 0 (\text{mod } P_i) \qquad i = 1, 2, \ldots, t$$

has a solution which we shall denote by x_i . Further, since the integers P_i are relatively prime, by the Chinese Remainder Theorem there exists an integer z such that

$$z \equiv x_i (\text{mod } P_i), \quad i = 1, 2, \ldots, t,$$

so that

$$(2.5) \qquad z^2 + 1 \equiv 0(\text{mod } d).$$

Let us define

$$(2.6) \qquad p_n = 2(z + (n - 1)d), \quad n = 1, 2, \ldots \quad .$$

Then by equation 2.5 we have

$$p_n^2 + 4 \equiv 4(z^2 + 1) \equiv 0(\text{mod } d), \qquad n = 1, 2, \ldots \quad .$$

Then by Theorem 2.1, for each p_n there exists an integer $q_n \neq 0, -1$, such that $F(N(p_n,q_n)) = R(\sqrt{d})$ and $F(M(p_n,q_n)) = R(\sqrt{dc_n})$, where c_n is some integer such that $(d,c_n) = 1$. Also, since p_n is even, by Theorem 2.3 there exists an integer $q_n' \neq 0, -1$, such that $F(N(p_n,q_n')) = R(\sqrt{-d})$

and $F(M(p_n,q_n')) = R(\sqrt{dc_n'})$, for some integer c_n' such that $(d,c_n') = 1$, $n = 1, 2, \ldots$. Clearly the sequence $\{p_n\}$ is strictly increasing since $d \geq 1$, so that the theorem is true if d is odd.

In the second case d is even and hence of the form $2\prod_{i=1}^{t} P_i$ where the P_i are as specified in the first case. We can choose integers x_i, $i = 1, 2, \ldots, t+1$, so that

$$x_i^2 + 1 \equiv 0 (\text{mod } P_i), \quad i = 1, 2, \ldots, t$$

and $$x_{t+1}^2 + 1 \equiv 0 (\text{mod } 2).$$

Hence, as above, we can choose an integer z such that

$$z^2 + 1 \equiv 0 (\text{mod } d).$$

Clearly z is an odd integer. We define integers p_n by equation 2.6. Then $p_n^2 + 4 \equiv 0(\text{mod } d)$ and $p_n/2 \equiv 1(\text{mod } 2)$ so that $p_n^2 + 4 \equiv 0(\text{mod } 8)$, $n = 1, 2, \ldots$. Thus by Theorem 2.4 (with $e = 1$), for each integer p_n there exists an integer $q_n \neq 0, -1$, such that $F(N(p_n,q_n)) = R(\sqrt{d})$ and $F(M(p_n,q_n)) = R(\sqrt{dc_n})$, for some integer c_n such that $(d,c_n) = 1$. Also, by Theorem 2.4 (with $e = -1$), for each p_n, there exists an integer $q_n' \neq 0, -1$, such that $F(N(p_n,q_n')) = R(\sqrt{-d})$ and $F(M(p_n,q_n')) = R(\sqrt{dc_n'})$, where c_n' is some integer such that $(d,c_n') = 1$. As in the previous case, the sequence $\{p_n\}$ is seen to be strictly increasing, so that the proof of the theorem is complete.

From a non-field theoretic viewpoint, the following simple theorem comes to our attention relating $\Delta(p,q)$ and

$\delta(p,q)$ for certain pairs (p,q).

Theorem 2.6. Suppose $4 \mid p$, $p > 0$. Then there exists an integer $q \neq -1$ such that $\Delta(p,q) = c\delta(p,q)$, for some integer c.

Proof: Let $U = \{y \mid y \mid ((p/2)^2 + 1),\ y \equiv 1 (\mathrm{mod}\ 4),\ y > 1\}$. Then $U \neq \emptyset$ since $((p/2)^2 + 1) \in U$. Choose $y \in U$. Let m be the integer given by:

$$m = (y - 1)/4 .$$

Then let

$$q = (4m(p/2)^2 - 1)/(1 + 4m) = ((y - 1)(p/2)^2 - 1)/y$$
$$= (y(p/2)^2 - ((p/2)^2 + 1))/y ,$$

and this last expression is an integer. Then

$$q + 1 = 4m((p/2)^2 + 1)/(1 + 4m) \neq 0$$

so that $q \neq -1$. Further,

$$m(p^2 - 4q) = 4m((p/2)^2 - (4m(p/2)^2 - 1)/(1 + 4m))$$
$$= q + 1.$$

Hence $p^2 + (q - 1)^2 = p^2 - 4q + (q + 1)^2 = m_1(p^2 - 4q)$ where $m_1 = 1 + m^2(p^2 - 4q)$, and this proves the theorem. ▮

We have shown in Theorem 2.2 that there exist infinitely many pairs (p,q), with $q \neq -1$, $pq \neq 0$, such that $g_\delta(p,q) \mid g_\Delta(p,q)$. The following two theorems each tell us that there also exist infinitely many pairs (p,q), with $q \neq -1$, $pq \neq 0$, such that $g_\Delta(p,q) \mid g_\delta(p,q)$.

Theorem 2.7. There exists a sequence $\{(p_n,q_n)\}$ of distinct pairs of integers such that $F(M(p_n,q_n)) = R(\sqrt{2})$ and $F(N(p_n,q_n)) = R(\sqrt{2d_n})$, where d_n is an odd integer and

$q_n \neq -1$, $n = 1, 2, \ldots$.

Proof: Consider the equation

$$x^2 - 2y^2 = -1. \tag{2.7}$$

The solutions of this equation are of the form $\pm x_n \pm y_n\sqrt{2}$, where x_n and y_n are defined by

$$x_n + y_n\sqrt{2} = (1 + \sqrt{2})^{2n-1}, \quad n = 1, 2, \ldots \quad . \tag{2.8}$$

We can show that the numbers x_n and y_n are all odd. For, from equation 2.7, each x_n is surely odd and thus

$$2y_n^2 = x_n^2 + 1 \equiv 2(\text{mod } 4),$$

so that y_n cannot be even. We can define a sequence of pairs of integers $\{(s_n, t_n)\}$ by the requirements

$$|s_n| = |x_n|, \quad |t_n| = |y_n|, \quad s_n \equiv t_n \equiv -1(\text{mod } 4), \; n \geq 1.$$

We further define

$$p_n = s_n + t_n, \; q_n = t_n.$$

Then we have

$$p_n^2 - q_n^2 + 1 - 2p_nq_n = (s_n + t_n)^2 - t_n^2 + 1 - 2(s_n + t_n)t_n \tag{2.9}$$
$$= s_n^2 + 2s_nt_n + 1 - 2s_nt_n - 2t_n^2 = 0.$$

Then we see that

$$(p_n^2 - q_n^2 + 1)^2 = 4p_n^2q_n^2 \tag{2.10}$$

so that

$$\Delta(p_n, q_n) = (p_n^2 - q_n^2 + 1)^2 + 4p_n^2q_n^2 = 8p_n^2q_n^2.$$

Hence

$$F(M(p_n, q_n)) = R(\sqrt{2}).$$

Furthermore, by the above,

$$p_n^2 - 4q_n = (s_n + t_n)^2 - 4t_n = 4((s_n + t_n)^2/4 - t_n). \tag{2.11}$$

Since $s_n + t_n \equiv -2 \pmod 4$, we have

$$((s_n + t_n)/2)^2 - t_n \equiv 1 + 1 \equiv 2 \pmod 4.$$

Hence $F(N(p_n, q_n)) = R(\sqrt{2d_n})$ where d_n is the square-free part of $(((s_n + t_n)/2)^2 - t_n)/2$ and is odd. Evidently $|t_1| < |t_2| < |t_3| < \ldots$. Hence $|q_1| < |q_2| < |q_3| < \ldots$, so that the sequence $\{(p_n, q_n)\}$ consists of distinct pairs. Also, if $q_n = -1$, for some n, we can delete the nth pair from the sequence thus fulfilling all conditions of the theorem.∎

To illustrate the above theorem, we note that

$$x_1 + y_1\sqrt{2} = 1 + \sqrt{2}, \qquad x_2 + y_2\sqrt{2} = 7 + 5\sqrt{2},$$
$$x_3 + y_3\sqrt{2} = 41 + 29\sqrt{2}.$$

Thus $(s_1, t_1) = (-1, -1)$, $(s_2, t_2) = (7, -5)$, $(s_3, t_3) = (-41, -29)$ and hence $(p_1, q_1) = (-2, -1)$, $(p_2, q_2) = (2, -5)$,

$$(p_3, q_3) = (-70, -29).$$

Then
$$\Delta(p_1, q_1) = (p_1^2 + (q_1 + 1)^2)(p_1^2 + (q_1 - 1)^2) = 4(4 + 4) = 2 \cdot 4^2,$$

and similarly,
$$\Delta(p_2, q_2) = (4 + 36)(4 + 16) = 2 \cdot 20^2,$$
$$\Delta(p_3, q_3) = 4^2(1225 + 196)(1225 + 225) = 2(4 \cdot 5 \cdot 7 \cdot 29)^2.$$

Further,
$$\delta(p_1, q_1) = p_1^2 - 4q_1 = 4 + 4 = 2 \cdot 2^2$$
$$\delta(p_2, q_2) = 4 + 20 = 2 \cdot 3 \cdot 2^2$$
$$\delta(p_3, q_3) = 4(1225 + 29) = 2(2^2 \cdot 3 \cdot 11 \cdot 19) .$$

The results of these calculations are as expected from the theorem.

While Theorem 2.7 tells us that there are infinitely many pairs (p,q), with $q \neq -1$, such that $g_\Delta(p,q) \nmid g_\delta(p,q)$ and $g_\Delta(p,q) = k$, where $k = 2$, the next theorem tells us that the same statement holds for an infinite number of integers $k > 0$. We first have a lemma:

Lemma.* Let $c > 1$ be an integer of the form $\prod P_i^{\alpha_i}$, where each prime P_i is of the form $4N+1$. Then there exists at least one pair of integers (a,b) such that $c = a^2 + b^2$ and $(b,c) = 1$.

Theorem 2.8. Let d be an odd integer which is a product of primes of the form $4N+1$. Suppose further that d is not a perfect square. Then there exists a sequence $\{(p_n', q_n')\}$, where the sequences $\{p_n'\}$ and $\{q_n'\}$ are strictly increasing, such that $F(M(p_n', q_n')) = R(\sqrt{d})$, $F(N(p_n', q_n')) = R(\sqrt{dd_n})$, where $(d, d_n) = 1$.

Proof: Let $s_o + t_o\sqrt{d}$ denote any solution of the equation

$$(2.12) \qquad s^2 - dt^2 = 1, \qquad s_o > 0,\ t_o > 0 .$$

(Such a solution exists by Theorem B.) Write $d = \prod_{i=1}^{m} P_i^{\beta_i}$ where the primes P_i are distinct and each $\beta_i > 0$. Further, write $t_o = k\prod_{i=1}^{m} P_i^{\alpha_i}$ where $\alpha_i \geq 0$, $i = 1,\ldots,m$, and $(k,d) = 1$. Define

$$d' = t_o/k, \qquad c = (d')^2 d .$$

Then we have

[*] A proof of this result can be found in [4], pages 164-6.

(2.13) $s_o^2 - k^2c = s_o^2 - (d')^2k^2d = s_o^2 - t_o^2d = 1.$

We can write $c = a^2 + b^2$ where $(b,c) = 1$. Such a and b can be chosen by the lemma. Now c is of the form prescribed in Theorem 1.3 and $s_o + k\sqrt{c}$ is a solution of

(2.14) $$s^2 - t^2c = 1.$$

We define

(2.15) $s_1 + t_1\sqrt{c} = (s_o + k\sqrt{c})^2 = (s_o^2 + k^2c) + 2s_o k\sqrt{c}$.

Furthermore, define

(2.16)
$$\begin{aligned} s_n + t_n\sqrt{c} &= (s_1 + t_1\sqrt{c})^n \\ x_n + y_n\sqrt{c} &= (s_n + t_n\sqrt{c})^2 \\ u_n + v_n\sqrt{c} &= (c + b\sqrt{c})(x_n + y_n\sqrt{c}) \\ &= (cx_n + cby_n) + \sqrt{c}(bx_n + cy_n) \\ k_n &= 2(v_n - b)/c \\ p_n &= k_n a, \\ q_n &= k_n b + 1, \qquad \text{for } n \geq 1, \end{aligned}$$

as in the proof of Theorem 1.3. (In the proof of Theorem 1.3 we demonstrated that the numbers k_n are in fact integral.) By induction, we prove that $s_n \equiv 1(\text{mod } c)$, $n \geq 1$.

Clearly, $s_1 \equiv 1(\text{mod } c)$, since by equations 2.13 and 2.15

$$s_1 = s_o^2 + k^2c \equiv 2ck^2 + 1 \equiv 1(\text{mod } c).$$

Also

(2.17) $$\begin{aligned} s_n + t_n\sqrt{c} &= (s_{n-1} + t_{n-1}\sqrt{c})(s_1 + t_1\sqrt{c}) \\ &= s_{n-1}s_1 + ct_{n-1}t_1 + \sqrt{c}(t_{n-1}s_1 + s_{n-1}t_1) \end{aligned}$$

so that if we assume $s_{n-1} \equiv 1(\text{mod } c)$ then $s_n \equiv 1 \circ 1 + 0$ $\equiv 1(\text{mod } c)$ and the induction is complete.

Further,

$$(t_1,c) = (2s_0k,c) = (2s_0,c)$$

since $(k,c) = 1$ by the definition of c. Also, $(2s_0,c) = 1$ by equation 2.13 and the fact that d is odd. Hence

(2.18) $$(t_1,c) = 1.$$

We now show that $t_n \equiv nt_1 (\text{mod } c)$ for $n \geq 1$. We prove this statement inductively noting that it is certainly true for $n = 1$. Assuming then that

$$t_{n-1} \equiv (n - 1)t_1 (\text{mod } c),$$

where $n \geq 2$, we have from equation 2.17:

$$t_n = t_{n-1}s_1 + s_{n-1}t_1 \equiv t_{n-1} + t_1 \equiv (n - 1)t_1 + t_1$$
$$\equiv nt_1 (\text{mod } c)$$

and this completes the proof by induction.

Now consider the equations

(2.19) $$f(y) = y^2 + 1 \equiv 0 (\text{mod } P_i), \quad i = 1,\ldots,m .$$

Each of these equations is solvable since each P_i is of the form $4N + 1$. For each integer i, denote one solution of equation 2.19 by y_i. Since $f'(y_i) \not\equiv 0 (\text{mod } P_i)$, $i = 1,\ldots,m$, we conclude by Theorem C that there exist integers y_i' such that

(2.20) $$y_i' \equiv y_i (\text{mod } P_i), \quad f(y_i') \equiv 0 (\text{mod } P_i^{2\alpha_i+\beta_i}),$$
$$i = 1,\ldots,m .$$

Then by the Chinese Remainder Theorem we can choose an integer z such that

$$z \equiv y_i' (\text{mod } P_i^{2\alpha_i+\beta_i}), \quad i = 1,\ldots,m$$

and hence by equation 2.20 we have

(2.21) $$f(z) = z^2 + 1 \equiv 0 (\text{mod } c),$$

since $c = \prod_{i=1}^{m} P_i^{2\alpha_i+\beta_i}$ and the primes P_i are distinct.

Now since $t_n \equiv nt_1 (\text{mod } c)$ and $(t_1,c) = 1$, as is demonstrated above, it is clear that the numbers:

$$t_{1+rc}, t_{2+rc}, \ldots, t_{c(1+r)}$$

where r is any positive integer, form a complete residue system modulo c. Also, since $(2b,c) = 1$, the integers

$$2bt_{1+rc}, 2bt_{2+rc}, \ldots, 2bt_{c(1+r)}$$

also represent a complete residue system modulo c. Further, since $t_{m+c} \equiv t_m (\text{mod } c)$ for all $m \geq 1$, we can choose an integer N such that

(2.22) $$2bt_{N+rc} \equiv z - 1 (\text{mod } c)$$

for every integer $r \geq 0$.

Then:

(2.23) $$(2bt_{N+rc} + 1)^2 + 1 \equiv z^2 + 1 \equiv 0 (\text{mod } c),$$

by equations 2.21 and 2.22.

Now by equations 2.16,

(2.24) $$\begin{aligned} p_{N+rc}^2 - 4q_{N+rc} &= k_{N+rc}^2 a^2 - 4(k_{N+rc} b + 1) \\ &= (-k_{N+rc}^2 b^2 - 4k_{N+rc} b - 4) + k_{N+rc}^2 c \\ &\equiv -(k_{N+rc} b + 2)^2 (\text{mod } c) . \end{aligned}$$

In general, from equations 2.16 we know that

$$\begin{aligned} k_n &= 2(v_n - b)/c = 2(bx_n + cy_n - b)/c \\ &= 2(b(s_n^2 + t_n^2 c) + c(2s_n t_n) - b)/c \\ &= 2(b(s_n^2 + t_n^2 c - 1)/c + 2s_n t_n) . \end{aligned}$$

Moreover, since $s_n^2 - t_n^2c = 1$, we have

$$(2.25)\ k_n = 2(b(2t_n^2c)/c + 2s_nt_n) = 4(bt_n^2 + s_nt_n)$$
$$\equiv 4(bt_n^2 + t_n)(\text{mod } c),$$

since $s_n \equiv 1(\text{mod } c)$ as is demonstrated above. Thus from equations 2.23 and 2.25 we have:

$$(2.26)\ k_{N+rc}b + 2 \equiv 4bt_{N+rc}(bt_{N+rc} + 1) + 2$$
$$= (2bt_{N+rc} + 1)^2 + 1 \equiv 0(\text{mod } c)\ .$$

Hence by equations 2.24 and 2.26 we have

$$p_{N+rc}^2 - 4q_{N+rc} \equiv 0(\text{mod } c), \quad r = 0, 1, 2, \ldots \quad .$$

Furthermore, since

$$(2.27)\ p_{N+rc}^2 - 4q_{N+rc} = -(k_{N+rc}b + 2)^2 + k_{N+rc}^2c,$$

we can show that $((p_{N+rc}^2 - 4q_{N+rc})/c, c) = 1.$

For, if $P \mid ((p_{N+rc}^2 - 4q_{N+rc})/c, c)$, where P is prime, then $P = P_i$ for some i. Then

$$P_i^{2\alpha_i+\beta_i+1} \mid (p_{N+rc}^2 - 4q_{N+rc})\ .$$

Also, by equation 2.26 we know that

$$P_i^{2(2\alpha_i+\beta_i)} \mid (k_{N+rc}b + 2)^2$$

so that

$$P_i^{2\alpha_i+\beta_i+1} \mid (k_{N+rc}b + 2)^2.$$

Hence from equation 2.27 we would have

$$P_i^{2\alpha_i+\beta_i+1} \mid k_{N+rc}^2c$$

so that

$$P_i \mid k_{N+rc}$$

which is impossible in view of equation 2.26. Hence

$$F(N(p_{N+rc},q_{N+rc})) = R(\sqrt{cd_{r+1}}) = R(\sqrt{(d')^2dd_{r+1}})$$
$$= R(\sqrt{dd_{r+1}}) ,$$

where d_{r+1} is an integer such that $(d_{r+1},c) = 1$, $r \geq 0$. Further, from the proof of Theorem 1.3, we know that

$$F(M(p_{N+rc},q_{N+rc})) = R(\sqrt{c}) = R(\sqrt{d}), \quad r = 0, 1, 2, \ldots \quad .$$

Since the sequence $\{(p_{N+rc},q_{N+rc})\}$ is a subsequence of the sequence $\{(p_n,q_n)\}$, the sequences $\{p_{N+rc}\}$ and $\{q_{N+rc}\}$ are strictly increasing, by the proof of Theorem 1.3.

Finally, we set

$$p_n' = p_{N+(n-1)c}, \quad q_n' = q_{N+(n-1)c}, \quad n \geq 1,$$

and the proof of the theorem is complete.∎

As an illustration of the above theorem, consider the case $d = 5$. Since $9^2 - 4^2 5 = 1$, and $(4,5) = 1$, we set $c = 5 = d$ and define $a = 1$, $b = 2$. We take

$$s_1 + t_1\sqrt{5} = (9 + 4\sqrt{5})^2 = 161 + 72\sqrt{5} .$$

Then

$$s_2 + t_2\sqrt{5} = (s_1 + t_1\sqrt{5})^2 = (161 + 72\sqrt{5})^2$$
$$= 51841 + 23184\sqrt{5} .$$

Now $2^2 + 1 \equiv 0 \pmod 5$ so we can take $z = 2$. We then wish to choose an integer N such that $2bt_N \equiv z - 1 \pmod c$, as in equation 2.22 above. In our case equation 2.22 becomes

$$4t_N \equiv 1 \pmod 5.$$

Since $t_1 \equiv 2 \pmod 5$ and $t_2 \equiv -1 \pmod 5$, evidently $N = 2$ will suffice. We then observe that 5 does indeed divide $k_2b + 2$. In fact,

$$
\begin{aligned}
k_2b + 2 &= 2(k_2 + 1) = 2(4t_2(t_2 + s_2) + 1) \\
&= 2(4\cdot 23184\cdot 98209 + 1) = 2\cdot 9107509825 \\
&= 2\cdot 5\cdot 1821501965 \ .
\end{aligned}
$$

Setting $p_2 = k_2a = k_2$ and $q_2 = k_2b + 1 = 2k_2 + 1$, we have

$$
\begin{aligned}
p_2^2 - 4q_2 &= k_2^2 - 4(2k_2 + 1) \\
&= 5k_2^2 - 4(k_2 + 1)^2 = 5\cdot 4((k/2)^2 - 5((k_2+1)/5)^2)
\end{aligned}
$$

so that $F(N(p_2,q_2)) = R(\sqrt{5d_1})$ where $5 \nmid d_1$. Clearly we must also have $F(M(p_2,q_2)) = R(\sqrt{5})$. (We omit numerical verification of this last statement as a similar calculation was demonstrated in a previous example.) Evidently from this example, the method of calculation outlined is highly impractical.

III. ON THE COINCIDENCE OF F(M(p,q)) AND F(N(p,q))

The following known theorems will be of use in this chapter:

Theorem D. Let $f(x)$ be a polynomial of degree $n \geq 3$ with integral coefficients and distinct zeros, and let a be any non-zero integer. Then the equation

$$ay^2 = f(x)$$

has only finitely many integral solutions (x,y).∎

This is a special case of a theorem by C. L. Siegel, [5] . A proof resting on the Thue-Siegel-Roth Theorem was given by W. J. Leveque in [6] , pages 155-7.

Theorem E. The integer 2 is a quadratic residue of primes of the form $8N \pm 1$ and a quadratic non-residue of primes of the form $8N \pm 3$. ∎

A proof of this theorem can be found in [7] , Theorem 95, page 75.

Theorem F. Let D be a positive integer which is not a perfect square. If $u_1 + v_1\sqrt{D}$ is the fundamental solution of any class of solutions of the equation

$$u^2 - Dv^2 = N$$

and if $x_1 + y_1\sqrt{D}$ is the fundamental solution of the equation

$$x^2 - Dy^2 = 1$$

(which exists according to Theorem B), then

$$0 \leq v_1 \leq \frac{y_1}{\sqrt{2(x_1 + 1)}} \sqrt{N} \qquad \text{if} \quad N > 0,$$

and
$$0 < v_1 \leq \frac{y_1}{\sqrt{2(x_1 - 1)}} \sqrt{-N} \qquad \text{if} \quad N < 0. \blacksquare$$

A proof of this theorem can be found in [3], pages 205-7.

Computations for pairs of integers (p,q) satisfying the inequalities

$$0 \leq |p| \leq 600, \quad 0 \leq |q| \leq 800$$

revealed five pairs (p,q) with $q \neq -1$, $pq \neq 0$, such that the fields $F(M(p,q))$ and $F(N(p,q))$ coincide. In the case $q = -1$, we have

$$\Delta(p,q) = p^2(p^2 + 4), \quad \delta(p,q) = p^2 + 4$$

so that the fields coincide trivially for every p. (This fact is also evident from remarks in the Introduction.) Also, it is easy to see that

$$\Delta(p,0) = (p^2 + 1)^2, \quad \delta(p,0) = p^2,$$
$$\Delta(0,q) = (q^2 - 1)^2, \quad \delta(0,q) = -4q$$

so that $F(M(p,0)) = F(N(p,0))$ for all integers p and $F(N(0,q)) = F(M(0,q))$ if and only if $q = -\square$.

The five non-trivial pairs (p,q) such that the fields coincide are listed in Table I below with other pertinent information. Here we define $F(p,q) = F(M(p,q)) = F(N(p,q))$. Also we denote the fundamental unit in $F(p,q)$ by $u(p,q)$.

TABLE I

$F(p,q)$	p	q	$\delta(p,q)$	$p^2 + (q + 1)^2$	$p^2 + (q - 1)^2$
$R(\sqrt{2})$	6	7	$2 \cdot 2^2$	10^2	$2 \cdot 6^2$
$R(\sqrt{2})$	14	47	$2 \cdot 2^2$	50^2	$2 \cdot 17^2$
$R(\sqrt{17})$	11	-76	$17 \cdot 5^2$	$2 \cdot 17 \cdot 13^2$	$2 \cdot 55^2$
$R(\sqrt{17})$	141	-236	$17 \cdot 35^2$	$2 \cdot 17 \cdot 47^2$	$2 \cdot 195^2$
$R(\sqrt{41})$	40	31	$41 \cdot 6^2$	$41 \cdot 8^2$	50^2

TABLE II

p	q	$u(p,q)$	$\lambda^{+}_{N(p,q)}$	$\lambda^{+}_{M(p,q)}$
6	7	$1 + \sqrt{2}$	$-3 + \sqrt{2}$	$(-3 + \sqrt{2})^2(u(6,7))^4$
14	47	$1 + \sqrt{2}$	$-7 + \sqrt{2}$	$(7 + \sqrt{2})^2(u(14,47))^4$
11	-76	$4 + \sqrt{17}$	$\alpha\beta^2 u(11,-76)$ $\alpha = 6 + \sqrt{17}$ $\beta = (5 - \sqrt{17})/2$	$\bar{\alpha}^2\bar{\beta}\beta^3(u(11,-76))^4$
141	-236	$4 + \sqrt{17}$	$\bar{\beta}^2\gamma(\overline{u(141,-236)})^3$ $\gamma = 22 + 5\sqrt{17}$	$\bar{\beta}^3\beta\gamma^2$
40	31	$32 + 5\sqrt{41}$	$-20 + 3\sqrt{41}$	$(-20 + 3\sqrt{41})^2(u(40,31))^2$

In Table II above* the characteristic roots $\lambda_N^+(p,q)$ and $\lambda_M^+(p,q)$ are factored into primes in $F(p,q)$. This factorization is possible since the fields in question, $R(\sqrt{2})$, $R(\sqrt{17})$ and $R(\sqrt{41})$, are Euclidean fields.

We observe that one of the cases of coincidence of the fields $F(M(p,q))$ and $F(N(p,q))$ occurs when $(p,q) = (6,7)$. This brings to mind the question of whether there exists another pair (p,q) such that $q = p + 1$ and the two fields coincide. We have the following theorem:

Theorem 3.1. $F(M(p,p+1)) = F(N(p,p+1))$ if and only if $p = -1, -2$, or 6.

Proof: (Note that when $p = -1$ or -2 the fields in question coincide trivially.) We set $q = p + 1$. Then we have

$$(3.1) \qquad \delta(p,q) = p^2 - 4q = q^2 - 6q + 1 = k^2m$$

for some integers k and m such that m is square-free. Further,

$$p^2 + (q-1)^2 = 2p^2$$
$$p^2 + (q+1)^2 = 2(q^2+1)$$

so that

$$(3.2) \qquad \Delta(p,q) = 2^2p^2(q^2+1) \; .$$

Suppose $F(M(p,q)) = F(N(p,q))$. Then from equations 3.1 and 3.2:

$$(3.3) \qquad q^2 + 1 = m\cdot\square \, .$$

Then equation 3.1 becomes

* This table is not further used here. Since, however, it necessitates some lengthy computation, it is included as it may be of interest independently.

$$m\cdot\square - 6q = k^2m$$

so that $m \mid 6q$. But $(m,q) = 1$ from equation 3.1 so that $m \mid 6$. Hence by equation 3.3, $m = 1$ or 2.

If $m = 1$ then $0 = pq = p(p + 1)$ by Theorem 1.1, so that $p = 0$ or -1. In the case $p = -1$ the two fields do in fact coincide, whereas in the case $p = 0$ they do not.

If $m = 2$ then there exists an integer h such that

(3.4) $$q^2 + 1 = 2h^2,$$

by equation 3.3. Thus equation 3.1 becomes

$$2h^2 - 6q = 2k^2$$

or

(3.5) $$3q = h^2 - k^2.$$

From equation 3.4, we must have

$$9q^2 = 9(2h^2 - 1)$$

which we combine with equation 3.5 to have:

(3.6) $$(h^2 - k^2)^2 = 3^2(2h^2 - 1).$$

We will show that equation 3.6 has only two solutions which correspond to $p = -2, 6$. We may assume that both h and k are non-negative throughout our discussion. We first suppose that $h \geq 30$. Then if $|h - k| \geq 5$ we have:

$$x^2 = ((h - k)/3)^2(h + k)^2 \geq 25h^2/9 > 2h^2 > 2h^2 - 1$$

where we have defined

$$x = ((h^2 - k^2)/3) .$$

This inequality shows us that in this case equation 3.6 cannot be satisfied.

If $|h - k| = 4$, then $|h + k| = 2h \pm 4$ (since $h \geq 30$) and so

$$\begin{aligned} x^2 &= 16(2h \pm 4)^2/9 > (2h - 4)^2 \\ &> 2h^2 + (2h^2 - 16h) = 2h^2 + 2h(h - 8) \\ &> 2h^2 - 1, \end{aligned}$$

so that equation 3.6 cannot be satisfied.

If $|h - k| = 3$, then

$$x^2 \geq (2h - 3)^2 > 2h^2 + 2h(h - 6) > 2h^2 - 1$$

and again equation 3.6 cannot be satisfied.

In the case $|h - k| = 2$ we have

$$\begin{aligned} x^2 &= 4(2h \pm 2)^2/9 \leq 4(2h + 2)^2/9 \\ &= 16h^2/9 + 4(8h + 4)/9 \\ &= 2h^2 - 2(h^2 - 16h - 8)/9. \end{aligned}$$

Now it is clear that since $h \geq 30$ we must have:

$$h^2 - 16h - 8 = h(h - 16) - 8 > 30\cdot 1 - 8 > 9.$$

Hence $x^2 < 2h^2 - 2 < 2h^2 - 1$. Hence in this case also equation 3.6 cannot be satisfied.

Suppose now that $|h - k| = 1$. Then

$$\begin{aligned} x^2 &\leq (2h + 1)^2/9 = 4h^2/9 + 4h/9 + 1/9 \\ &= 2h^2 - (14h^2/9 - 4h/9 - 1/9) \\ &= 2h^2 - (2h(7h - 2) - 1)/9 \\ &< 2h^2 - 1 \end{aligned}$$

and we conclude as above that equation 3.6 cannot be satisfied. Obviously, equation 3.6 cannot be satisfied in the case $|h - k| = 0$ and so we have proven that for $h \geq 30$ there is no k such that equation 3.6 is satisfied.

Now we observe that equation 3.6 implies

$$n^2 - 2h^2 = -1 \tag{3.7}$$

where $n = \underline{+}(h^2 - k^2)/3$ so that $k^2 = h^2 \underline{+} 3n$. The positive solutions of equation 3.7 can of course be written down in order of increasing magnitude as in the table below. (The positive solutions of equation 3.7 are precisely the positive odd powers of $1 + \sqrt{2}$.)

h	n	$h^2 - 3n$	$h^2 + 3n$	k
1	1	-2	4	2
5	7	4	46	2
29	41	718	964	---
	⋮		⋮	

Thus we see that for $h < 30$ the possible solutions of equation 3.6 are $(h,k) = (1,2)$ and $(5,2)$. In the former case $q = (h^2 - k^2)/3 = -1$ and thus $p = -2$, whereas in the latter case $q = 7$ and thus $p = 6$. ▮

We observe that in three cases of coincidence of $F(M(p,q))$ and $F(N(p,q))$, two of which are non-trivial, the relation $\delta(p,q) = 8$ is satisfied. This leads us to inquire if there are any additional pairs (p,q) such that $F(M(p,q)) = F(N(p,q))$ and $\delta(p,q) = 8$. We have the following theorem:

<u>Theorem 3.2</u>. Suppose $F(M(p,q)) = F(N(p,q))$, $\delta(p,q) = 8$, and $p \geq 0$. Then $(p,q) = (2,-1)$, $(6,7)$, or $(14,47)$.

<u>Proof</u>: Under the above hypotheses,

$$p^2 + (q + 1)^2 = 4q + 8 + q^2 + 2q + 1 = (q + 3)^2$$

and $$p^2 + (q - 1)^2 = 8 + (q + 1)^2 .$$

Since $F(N(p,q)) = R(\sqrt{2})$ we must have

$$(3.8) \qquad (q + 1)^2 + 8 = 2k^2$$

for some integer k. We define $x = p/2$. Clearly x is integral. Also

$$x^2 = q + 2$$

so that

$$q + 1 = x^2 - 1 .$$

Substituting this result in equation 3.8 we have:

$$(3.9) \qquad (x^2 - 1)^2 + 8 = 2k^2.$$

From this equation we see that x is odd and k is even, so that $k/2$ is an integer which we denote by y. Equation 3.9 then becomes

$$(x^2 - 1)^2 = 8(y^2 - 1)$$

and thus

$$(3.10) \qquad ((x^2 - 1)/8)^2 = (y^2 - 1)/8.$$

Since x and y are odd we may write*

$$x = 2u - 1, \; y = 2v - 1$$

so that equation 3.10 becomes

$$\binom{u}{2}^2 = \binom{v}{2} .$$

The only solutions** of this equation are (u,v) = (1,1), (2,2) and (4,9), and these solutions correspond to

* I am indebted to H. Hasse for this transformation.

** For a proof of this assertion, see [8], pages 202-7. The problem was raised previously by several authors. (See [9], pages 27, 36, and 37.) A new proof by J. W. S. Cassels is forthcoming.

$(p,q) = (2,-1)$, $(6,7)$, and $(14,47)$, respectively. ∎

In Theorem 3.2 we considered only those cases of coincidence which occur when $\delta(p,q) = 8$. We suppose now that $\delta(p,q) = K$, where K is a constant. Then we have the following theorem:

Theorem 3.3. Let K denote an integral constant. Then there exist at most a finite number of pairs (p,q) such that $\delta(p,q) = K$ and $F(M(p,q)) = F(N(p,q))$.

Proof: We can easily see that there exists no pair (p,q) such that $\delta(p,q) = 0$ and $F(M(p,q)) = F(N(p,q))$. Hence we assume $K \neq 0$. We may also assume $K \neq 8$, in view of the previous theorem. We write $K = k^2Q$, where k and Q are integers and Q is square-free. We suppose that $F(M(p,q)) = F(N(p,q))$ coincide. Then we must have

(3.11) $\Delta(p,q) = (p^2 + (q+1)^2)(p^2 + (q-1)^2) = h^2Q$

for some integer h . Since $\delta(p,q) = p^2 - 4q = k^2Q$, we must have:

(3.12) $(k^2Q + 4q + (q+1)^2)(k^2Q + 4q + (q-1)^2) = h^2Q$.

The left-hand side of equation 3.12 is a polynomial of degree four in q with roots

$$q = -3 \pm (8 - k^2Q)^{\frac{1}{2}}, \quad -1 \pm k(-Q)^{\frac{1}{2}} .$$

Since $k^2Q = K \neq 8$ and $K \neq 0$ by hypothesis, these four roots are distinct. Thus by Theorem D we conclude that equation 3.12 has at most a finite number of solutions (h,q). This proves the theorem since K and q determine $|p|$ uniquely. ∎

We apply a similar argument to prove the following more interesting result:

Theorem 3.4. For any given integer $q \neq -1, 0$, there exist at most a finite number of integers p such that $F(M(p,q))$ and $F(N(p,q))$ coincide.

Proof: (Recall that when $q = -1$ or 0, the cases eliminated from this theorem, these fields coincide for all integers p.) Suppose first that q and Q are fixed integers satisfying the conditions that $q \neq 0, -1$, and Q is nonzero and square-free. Suppose also that

$$(3.13) \qquad F(M(p,q)) = R(\sqrt{Q}) = F(N(p,q)),$$

for some integer p. Then equation 3.12 must be satisfied for some pair of integers (h,k). The left side of this equation is a polynomial of degree four in k with roots given by

$$k = \pm ((-4q - (q \pm 1)^2)/Q)^{\frac{1}{2}}$$

for all four choices of signs. These four roots are distinct except if either

$$4q + (q + 1)^2 = 0,$$

$$4q + (q - 1)^2 = 0,$$

or

$$4q + (q + 1)^2 = 4q + (q - 1)^2.$$

The first of these equations is not satisfied for integral q, the second implies that $q = -1$, and the third implies that $q = 0$, so that under our hypotheses the four roots are distinct. Thus we can conclude by Theorem D that equation 3.12 has at most a finite number of solutions (h,k) for fixed q and Q satisfying these restrictions, so that for such q and Q equation 3.13 can be satisfied by at most a finite number of integers p (since k, q and Q determine $|p|$ uniquely). Clearly if $Q = 0$, $|p|$ is uniquely determined by q (in fact, $p^2 = 4q$). Thus we conclude that for any Q and any $q \neq 0, -1$, there exist at most a finite number of integers p such that equation 3.13 holds.

Now we observe that for $q \neq -1$ there exist at most a finite number of square-free integers Q such that equation 3.13 is satisfied. This is true since equation 3.13 implies that there exist integers k, N, a, b and M such that $Q = ab$, $MN = \square$, and the following equations are satisfied:

$$p^2 - 4q = k^2Q$$
$$p^2 + (q + 1)^2 = Na$$
$$p^2 + (q - 1)^2 = Mb \quad .$$

Combining these equations we see that

$$a \mid (q^2 + 6q + 1), \quad b \mid (q + 1)^2$$

so that

$$Q \mid (q + 1)^2(q^2 + 6q + 1).$$

Now the expression $(q + 1)^2(q^2 + 6q + 1)$ is not equal to zero for integral $q \neq -1$. Hence it follows that Q can assume only a finite number of square-free values, for fixed $q \neq -1$. Since Q may always be considered to be square-free or equal to zero in equation 3.13, we conclude from all of the above results that there exist at most a finite number of integers p such that $F(M(p,q)) = F(N(p,q))$, and thus the theorem is proven. ▮

We may simplify the above proof slightly with the use of the following lemma:

Lemma. There exists no integer p such that $F(M(p,1)) = F(N(p,1))$.

Proof: We let $q = 1$ and suppose that $F(M(p,q)) = F(N(p,q))$. Then we must have

$$(3.14) \qquad p^2 - 4q = p^2 - 4 = k^2Q$$

$$(3.15) \qquad (p^2 + (q+1)^2)(p^2 + (q-1)^2) = (p^2 + 4)p^2 = h^2Q$$

for some integers h, k, and Q, where Q is square-free or zero as usual, and $h, k \neq 0$. Equation 3.15 implies that h/p is an integer, say j. Thus from equations 3.14 and 3.15 we have

$$8 = j^2Q - k^2Q = (j^2 - k^2)Q \ .$$

If $Q = 1$ then from equation 3.14 we have $p^2 = k^2 + 4$ which is impossible since $k \neq 0$. The only remaining alternative is $Q = 2$, which implies $j^2 = k^2 + 4$ and this is also an impossibility. Thus there exists no Q, and hence no p, satisfying equations 3.14 and 3.15. ▮

In the proof of Theorem 3.4 we have shown that equation 3.13 has at most a finite number of solutions p for given integers q and Q, where $q \neq -1, 0$, and Q is either equal to zero or square-free. We may now give a different demonstration of this as follows:

We observe from the lemma that for $q = 1$, equation 3.13 is never satisfied. We therefore can assume that integers $q \neq \pm 1, 0$, and Q are fixed and observe that the equation $F(M(p,q)) = R(\sqrt{Q})$ has only a finite number of solutions p at most. This is true since the left-hand side of the equation

$$(p^2 + (q+1)^2)(p^2 + (q-1)^2) = h^2 Q$$

is a polynomial of degree four in p with roots given by the relation $p = \pm i(q \pm 1)$ (for all four choices of signs in this expression). Under our hypotheses these roots are distinct so that for $Q \neq 0$ we conclude again by Theorem D that $F(M(p,q)) = R(\sqrt{Q})$ has at most a finite number of solutions p, and for $Q = 0$ this equation has no solutions p. This is the desired result.

The proof of the following theorem proceeds along the same lines of reasoning employed in proving Theorem 3.4.

Theorem 3.5. For a fixed integer $p \neq 0$ there exist at most a finite number of integers q such that $F(M(p,q))$ and $F(N(p,q))$ coincide.

Proof: We observe that for fixed Q and $p \neq 0$ the equation

$$(3.16) \qquad \Delta(p,q) = k^2 Q$$

has at most a finite number of solutions (q,k). For, $\Delta(p,q)$ is a polynomial of the fourth degree in q with roots $q = \pm 1 \pm ip$ (for all four choices of signs). Under our hypotheses, these roots are distinct so that by Theorem D, equation 3.16 has at most a finite number of solutions

(q,k) for $Q \neq 0$ (and clearly it has no solutions q for $Q = 0$, since by hypothesis $p \neq 0$) so that equation 3.16 has at most a finite number of solutions q for any Q.

We now demonstrate that only a finite number of square-free integers Q can satisfy

$$F(M(p,q)) = F(N(p,q)) = R(\sqrt{Q}) \tag{3.17}$$

for fixed $p \neq 0$. For, if equation 3.17 is satisfied then there exist integers h and k such that:

$$4(q + 1) = p^2 - k^2Q + 4,$$

$$4(q - 1) = p^2 - k^2Q - 4,$$

$$(16p^2 + 16(q + 1)^2)(16p^2 + 16(q - 1)^2) = (16)^2h^2Q$$

and hence,

$$(24p^2 + p^4 + 16)(p^2 + 4) \equiv 0 (\mathrm{mod}\ Q).$$

Since this expression is never equal to zero, we conclude that Q belongs to a finite set of integers. These results yield the theorem. ∎

For two of the known non-trivial cases of coincidence of $F(M(p,q))$ and $F(N(p,q))$ we notice that

$$(p^2 + (q + 1)^2)(p^2 + (q - 1)^2) = 17 \cdot 130^2p^2. \tag{3.18}$$

In one case $(p,q) = (11,-76)$ and in the other $(p,q) = (141,-236)$.

Using computer-obtained data, it is possible to show that equations 3.18 and

$$p^2 - 4q = 17k^2, \tag{3.19}$$

which together imply that

(3.20) $\qquad F(M(p,q)) = F(N(p,q)) = R(\sqrt{17}),$

are satisfied for no other triples (p,q,k) (with $p \geq 0$ and $k \geq 0$) than $(11,-76,5)$, $(141,-236,35)$, and $(536,-1,130)$, the latter triple representing a trivial case of coincidence. From computations we know that this assertion is true for p, $|q| \leq 550$. If either p or $|q| > 550$ then

$$(p^2 + (q + 1)^2)(p^2 + (q - 1)^2) \geq (p^2 + (q + 1)^2)p^2$$
$$> 550^2p^2 > 17\cdot130^2p^2.$$

Hence equations 3.18 and 3.19 are satisfied for no other triples than those given.

One of the coinciding cases, namely $(p,q) = (40,31)$ gives us a solution of the system of equations:

(3.21) $\qquad (p^2 + (q + 1)^2)(p^2 + (q - 1)^2) = 41\cdot10^2p^2$

(3.22) $\qquad p^2 - 4q = 41\cdot k^2.$

There are no other triples except $(p,q,k) = (40,31,6)$ and $(64,-1,10)$ (with $p \geq 0$ and $k \geq 0$) satisfying equations 3.12 and 3.22. From computations we know that this assertion is true for p and $|q| \leq 65$. If either p or $|q| > 65$ then:

$$(p^2 + (q + 1)^2)(p^2 + (q - 1)^2) \geq (p^2 + (q + 1)^2)p^2$$
$$> 65^2p^2 > 4100p^2$$

and this proves our assertion.

We observe that both equation 3.21 and equation 3.18 have solutions (p,q) of the form $(p,-1)$. In general, the following remark is true:

<u>Remark 3.6</u>. Let K be a fixed integer. Suppose the equation $\Delta(p,q) = Kp^2$ has a solution (p_o,q_o), $p_o > 0$.

Then there exists an integer p_1 such that $\Delta(p_1,-1) = Kp_1^2$.

Proof: Write $K = h^2Q$, where Q is square-free. Then by hypothesis we have:

$$\Delta(p_o,q_o) = (1 + p_o^2 + q_o^2)^2 - 4q_o^2 = h^2p_o^2Q.$$

Hence $h^2Qp_o^2 - 4p_o^2 = (1 + p_o^2 + q_o^2)^2 - 4(q_o^2 + p_o^2)$

$$= (1 - (p_o^2 + q_o^2))^2$$

so that $h^2Q - 4 = p_1^2$ for some integer p_1, since $p_o \neq 0$. This integer p_1 satisfies our requirements. For,

$$\Delta(p_1,-1) = p_1^2(p_1^2 + 4) = h^2p_1^2Q = Kp_1^2 \ . \blacksquare$$

In the above discussion we considered systems of equations which included the equation

$$(3.23) \qquad (p^2 + (q + 1)^2)(p^2 + (q - 1)^2) = 4kp^2$$

with $k = 17\cdot65^2$ in one case and $k = 41\cdot5^2$ in the other. We noted some solutions (p,q) (indicated by † in Table III) in these cases. Let us now consider the solutions of equation 3.23 by itself. Clearly we need only mention non-negative pairs of solutions (p,q) (i.e., pairs such that $p, q \geq 0$). As solutions of equation 3.23 must satisfy the conditions

$$|q + 1| \leq \sqrt{2k} \ , \qquad |p| \leq \sqrt{2k} \ ,$$

it is easy to exhaust them with the aid of a computer, as has been done in the cases of those k noted above (see Table III below).

General properties of the solutions of equation 3.23 evidenced in these two cases are explained by the following

Table III

$k = 17\cdot 65^2$		$k = 41\cdot 5^2$	
p	q	p	q
0	1	0	1
3	40	1	8
8	65	7	20
† 11	76	12	25
21	104	24	31
32	127	31	32
53	160	33	32
60	169	† 40	31
77	188	52	25
80	191	57	20
99	208	63	8
108	215	† 64	1
† 141	236		
164	247		
192	257		
203	260		
228	265		
267	268		
269	268		
308	265		
333	260		
344	257		
372	247		
395	236		
428	215		
437	208		
456	191		
459	188		
476	169		
483	160		
504	127		
515	104		
525	76		
528	65		
533	40		
† 536	1		

remark.

<u>Remark 3.7</u>. Let $n(k)$ denote the number of non-negative pairs (p,q) which are solutions of equation 3.23 for a fixed positive integer k. Then*

$$n(k) = \begin{cases} 1, \text{ if } k \neq 1 + \square \\ 2(d_1(k) - d_3(k)), \text{ if } k = 1 \end{cases} .$$

Further, if $k = 1 + \square$ and $k \neq 1$, then $n(k) \geq 4$.

<u>Proof</u>: Since

$$\Delta(p,q) = (p^2 + q^2 - 1)^2 + 4p^2,$$

we can rewrite equation 3.23 as follows:

$$(3.24) \qquad (p^2 + q^2 - 1)^2 = 4p^2(k - 1).$$

Hence if $k - 1 \neq \square$, equation 3.23 has only the trivial solution $(p,q) = (0,1)$. Suppose now that there exists a non-negative integer h such that $k = 1 + h^2$. Then the non-negative solutions of equation 3.23 are precisely the pairs $(p,q) = (|s|, |t|)$, where (s,t) is a solution of

$$(3.25) \qquad s^2 + t^2 - 1 = 2sh$$

which can be written as

$$(3.26) \qquad x^2 + t^2 = h^2 + 1 = k$$

where $x = s - h$. Evidently for $h > 0$, $n(k)$ is the number of solutions (x,t) of equation 3.26 with $t \geq 0$ (we must count both (x,t) and $(-x,t)$ since $h > 0$ implies $x \neq 0$, and

* In [7], $d_1(n)$ and $d_3(n)$ are defined to be the number of divisors of n of the form $4N + 1$ and $4N + 3$, respectively.

hence the absolute values of the integers s corresponding to $+x$ and $-x$ are distinct) and this number is just* $r(k)/2$. It is known that**

$$r(k) = 4(d_1(k) - d_3(k)).$$

Thus $\quad n(k) = 2(d_1(k) - d_3(k)).$

Clearly this formula also holds if $h = 0$. For, in this case equation 3.24 becomes $(p^2 + q^2 - 1)^2 = 0$, so that $n(1) = 2$. Since $d_1(1) = 1$ and $d_3(1) = 0$, we have

$$n(1) = 2(d_1(1) - d_3(1))$$

as asserted. To complete the proof of the remark, we observe that for $k > 2$, four distinct solutions of equation 3.23 are given by $(p,q) = (0,1)$, $(h-1,h)$, $(h+1,h)$, and $(2h,1)$. (We note that according to Table III, $n(17 \cdot 65^2) = 36$ and $n(41 \cdot 5^2) = 12$. This agrees with Remark 3.7, since $d_1(17 \cdot 65^2) = 2 \cdot 3 \cdot 3 = 18$, $d_1(41 \cdot 5^2) = 2 \cdot 3 = 6$, and $d_3(17 \cdot 65^2) = d_3(41 \cdot 5^2) = 0$.) ▮

We observe that Table III includes the pair $(p,q) = (8,65)$, which is a solution of the equation

$$(3.27) \qquad (p^2 + (q + 1)^2)(p^2 + (q - 1)^2) = 4 \cdot 17 p^2 q^2.$$

Actually we can very simply describe all of the solutions of this equation as follows

<u>Remark 3.8</u>. The (non-negative) solutions of equation 3.27

* In [7], $r(n)$ is defined to be the number of representations of n as a sum of two ordered squares (variations in sign are taken into account).

** See [7], pages 241-2, for instance.

are precisely the pairs $(p,q) = (0,1)$, (p_n,q_n) and (p_n,q_{n+1}) where $p_n = x_n + 4q_n$, and x_n and q_n are defined by the equation

$$x_n + q_n\sqrt{17} = (4 + \sqrt{17})^{2n+1}, \qquad n = 0, 1, 2, \ldots .$$

<u>Proof</u>: Since

$$\Delta(p,q) = (p^2 - q^2 + 1)^2 + 4p^2q^2,$$

equation 3.27 becomes

$$(p^2 - q^2 + 1)^2 = (8pq)^2.$$

Thus the non-negative solutions of equation 3.27 are precisely the pairs $(|s|, |t|)$ such that (s,t) is a solution of

(3.28) $$s^2 + 8st - t^2 + 1 = 0.$$

We let $x = s - 4t$. Then equation 3.28 becomes

$$x^2 - 17t^2 = -1.$$

The solutions of this equation are the pairs $(x,t) = (\pm x_n, \pm t_n)$, $n = 0, 1, 2, \ldots$, (for all choices of signs) where x_n and t_n are defined by

$$x_n + t_n\sqrt{17} = (4 + \sqrt{17})^{2n+1} .$$

Hence the non-negative solutions of equation 3.27 are precisely the pairs $(p,q) = (p_n,q_n)$ and (p_n',q_n), $n = 0, 1, 2, \ldots,$ where

$$p_n = x_n + 4t_n, \qquad p_n' = |x_n - 4t_n|, \quad q_n = t_n.$$

We complete the proof by showing that p_n' is in fact equal to p_{n-1} for $n \geq 1$, and $(p_0',q_0) = (0,1)$. Thus

$$\begin{aligned} x_n + t_n\sqrt{17} &= (x_{n-1} + t_{n-1}\sqrt{17})(4 + \sqrt{17})^2 \\ &= 33x_{n-1} + 136t_{n-1} + \sqrt{17}(8x_{n-1} + 33t_{n-1}). \end{aligned}$$

Hence

$$\begin{aligned} p_n' &= |x_n - 4t_n| \\ &= |33x_{n-1} + 136t_{n-1} - 32x_{n-1} - 132t_{n-1}| \\ &= x_{n-1} + 4t_{n-1} = p_{n-1}. \quad \blacksquare \end{aligned}$$

Returning now to the question of coincidence of the fields $F(M(p,q))$ and $F(N(p,q))$ in its more general aspects, we are able to demonstrate that there exist an infinite number of integers q such that the fields coincide for no integers p.

Theorem 3.9. Suppose $F(M(p,q)) = F(N(p,q))$. Then $q \not\equiv 2 \pmod 4$.

Proof: Suppose $F(M(p,q)) = F(N(p,q))$ and $q \equiv 2 \pmod 4$. Then there exist integers Q, k, and m such that $k, m \neq 0$,

(3.29) $\delta(p,q) = p^2 - 4q = k^2Q$

(3.30) $\Delta(p,q) = (p^2 + (q+1)^2)(p^2 + (q-1)^2) = m^2Q$

where Q is equal to zero or a square-free product of primes congruent to one or two modulo four. Hence $Q \equiv 1, 2,$ or $5 \pmod 8$, or $Q = 0$. We show that Q is odd. For, combining equations 3.29 and 3.30 we have

(3.31) $(k^2Q + 4q + (q-1)^2)(k^2Q + 4q + (q+1)^2) = m^2Q,$

so that

$$(k^2Q + 1)(k^2Q + 1) \equiv m^2Q \pmod 2$$

since $q \equiv 0 \pmod 2$. Clearly from this equation we cannot have $Q \equiv 0 \pmod 2$. Hence $Q \equiv 1$ or $5 \pmod 8$. We assume now that $Q \equiv 5 \pmod 8$ and deduce a contradiction. From equation 3.29 we have

(3.32) $$p^2 \equiv 5k^2 (\text{mod } 8).$$

Hence $p^2 \equiv 0$ or $4(\text{mod } 8)$. In either case, we see that $\Delta(p,q) \equiv 1(\text{mod } 8)$, and since $m^2 Q \equiv 5m^2 \not\equiv 1(\text{mod } 8)$, we conclude that equation 3.30 cannot possibly be satisfied in the case $Q \equiv 5(\text{mod } 8)$. The remaining case is $Q \equiv 1(\text{mod } 8)$. We will also deduce a contradiction in this case. Assume then that $Q \equiv 1(\text{mod } 8)$. We can write

(3.33) $$p^2 + (q + 1)^2 = \beta_1^2 Q_1 n$$

(3.34) $$p^2 + (q - 1)^2 = \beta_2^2 Q_2 n$$

for some integers β_1, β_2, Q_1, Q_2, and n, where $Q_1 Q_2 = Q$ and n is square-free. It is clear that n is a product of primes of the form $4N + 1$, or twice such a product. Combining equations 3.33 and 3.29 we have

(3.35) $$4q + k^2 Q_1 Q_2 + (q + 1)^2 = \beta_1^2 Q_1 n$$

so that we conclude

(3.36) $$4q + (q + 1)^2 \equiv 0 \ (\text{mod } Q_1).$$

Similarly, from equations 3.29 and 3.34 we have

(3.37) $$4q + (q - 1)^2 = (q + 1)^2 \equiv 0(\text{mod } Q_2)$$

which implies that $Q_2 \mid q + 1$.

Now Q_1 is a product of primes, $\prod P_i$, where each $P_i \equiv 1(\text{mod } 4)$. We can show that in fact each $P_i \equiv 1(\text{mod } 8)$. For, suppose some $P_i \equiv 5(\text{mod } 8)$. Then, by equation 3.36,

$$4q + (q + 1)^2 \equiv 0(\text{mod } P_i),$$

or, setting $x = p/2$ (x is obviously integral),

(3.38) $$4x^2 + 4x + 8x + 1 \equiv 0(\text{mod } P_i).$$

Equation 3.38 can be rewritten as

$$(3.39) \qquad (2x + 3)^2 \equiv 8 (\text{mod } P_i).$$

But,
$$\left(\frac{8}{P_i}\right) = \left(\frac{2}{P_i}\right) = -1$$

by Theorem E, and hence we have a contradiction.

Hence $Q_1 = \prod P_i$, where each $P_i \equiv 1 (\text{mod } 8)$, and, in particular, $Q_1 \equiv 1(\text{mod } 8)$. Since $Q \equiv 1(\text{mod } 8)$ and $Q_1 Q_2 = Q$, we conclude that $Q_2 \equiv 1(\text{mod } 8)$ also.

Now, from equation 3.29 we have

$$p^2 \equiv k^2 Q + 8(\text{mod } 16)$$
$$\equiv k^2 + 8 \quad \text{or} \quad 9k^2 + 8 \quad (\text{mod } 16)$$

since $q \equiv 2(\text{mod } 4)$ and $Q \equiv 1(\text{mod } 8)$. Since the quadratic residues of 16 are 0, 1, 4, and 9, it is clear that

$$p^2 \equiv 1 \text{ or } 9 \ (\text{mod } 16).$$

Also, we observe that since $4 \nmid q$, we have

$$(q + 1)^2 \not\equiv (q - 1)^2 (\text{mod } 16).$$

Since q is even we conclude that there are four possible cases:

Case I: $(q + 1)^2 \equiv 1, \ (q - 1)^2 \equiv 9, \ p^2 \equiv 1(\text{mod } 16)$

Case II: $(q + 1)^2 \equiv 9, \ (q - 1)^2 \equiv 1, \ p^2 \equiv 1(\text{mod } 16)$

Case III: $(q + 1)^2 \equiv 1, \ (q - 1)^2 \equiv 9, \ p^2 \equiv 9(\text{mod } 16)$

Case IV: $(q + 1)^2 \equiv 9, \ (q - 1)^2 \equiv 1, \ p^2 \equiv 9(\text{mod } 16)$.

In Case I we have

$$p^2 + (q + 1)^2 \equiv 1 + 1 \equiv 2(\text{mod } 16)$$
$$p^2 + (q - 1)^2 \equiv 1 + 9 \equiv 10(\text{mod } 16)$$

and in Case IV we have

$$p^2 + (q + 1)^2 \equiv 9 + 9 \equiv 2(\text{mod } 16)$$

$$p^2 + (q - 1)^2 \equiv 9 + 1 \equiv 10(\text{mod } 16)$$

so that in both cases I and IV we have

$$(3.40) \qquad p^2 + (q + 1)^2 \equiv 2(\text{mod } 16)$$

$$(3.41) \qquad p^2 + (q - 1)^2 \equiv 10(\text{mod } 16) \quad .$$

Hence from equations 3.33, 3.34, 3.40 and 3.41 we have

$$(3.42) \qquad \beta_1^2 Q_1 n \equiv 2(\text{mod } 16)$$

$$(3.43) \qquad \beta_2^2 Q_2 n \equiv 10(\text{mod } 16) \ .$$

Similarly in cases II and III we have

$$p^2 + (q + 1)^2 \equiv 10(\text{mod } 16)$$

$$p^2 + (q - 1)^2 \equiv 2(\text{mod } 16)$$

so that

$$(3.44) \qquad \beta_1^2 Q_1 n \equiv 10(\text{mod } 16)$$

$$(3.45) \qquad \beta_2^2 Q_2 n \equiv 2(\text{mod } 16) \ .$$

We now show that the system of equations

$$(3.46) \qquad v^2 tA \equiv 2(\text{mod } 16)$$

$$(3.47) \qquad w^2 tB \equiv 10(\text{mod } 16)$$

cannot be satisfied for any integers v, w, and t, where A and B are integers such that $A \equiv B \equiv 1(\text{mod } 8)$ and are fixed. Then it will certainly follow that neither of the systems of equations 3.42 and 3.43 or 3.44 and 3.45 can be satisfied so that in all cases we have a contradiction.

Thus we assume that equations 3.46 and 3.47 are satisfied for some integers v, w, and t. Then since $A \equiv B \equiv 1(\text{mod } 8)$ we must have $v \equiv 1(\text{mod } 2)$ from equation

3.46, $w \equiv 1 \pmod 2$ from equation 3.47, and $t \equiv 0 \pmod 2$ from both of these equations. Hence

$$Av^2 \equiv 1 \equiv Bw^2 \pmod 8$$

so that

$$t(w^2B - v^2A) \equiv 0 \pmod{16}. \tag{3.48}$$

However, subtracting equation 3.46 from equation 3.47 we have

$$t(w^2B - v^2A) \equiv 10 - 2 \equiv 8 \pmod{16}$$

and this equation contradicts equation 3.48. Thus if we assume $Q \equiv 1 \pmod 8$ we arrive at a contradiction and this completes the proof of the theorem. ▮

We recall from the lemma following Theorem 3.4 that $F(M(p,1))$ and $F(N(p,1))$ cannot coincide for any integer p. For certain other odd integers q we can also demonstrate that $F(M(p,q))$ and $F(N(p,q))$ cannot coincide for any p. Thus we have

Theorem 3.10. Suppose $F(M(p,q))$ and $F(N(p,q))$ coincide. Then $q \neq 3, 5, 11, 13, 15, -3, -5,$ and -13.

Proof: By equation 3.31 of Theorem 3.9, we have

$$g(q) = (q + 1)((q + 1)^2 + 4q) \equiv 0 \pmod Q \tag{3.49}$$

where Q is a square-free integer or zero and we have assumed that $F(M(p,q)) = F(N(p,q)) = R(\sqrt{Q})$ ($g(q)$ is defined by this expression). From Table IV below and the fact that the prime divisors of Q are of the form 2 or $4N + 1$, it is clear that for each integer q listed in the statement of the theorem, we must have $Q = 1$ or 2. (Since $q \neq \pm 1$, we know that $Q \neq 0$.)

Table IV

q	$\lvert q+1 \rvert$	$\lvert ((q+1)/2)^2 + q \rvert$	$\lvert g(q)/4 \rvert$
3	2^2	7	$2^2 7$
5	$2 \cdot 3$	$2 \cdot 7$	$2^2 3 \cdot 7$
11	$2^2 3$	47	$2^2 3 \cdot 47$
13	$2 \cdot 7$	$2 \cdot 31$	$2^2 7 \cdot 31$
15	2^4	79	$2^4 79$
-3	2	2	2^2
-5	2^2	1	2^2
-13	$2^2 3$	23	$2^2 3 \cdot 23$

Now,

$$\delta(p,q) = p^2 - 4q = k^2 Q \tag{3.50}$$

for some integer k. This implies that $Q \neq 1$. For, if $Q = 1$, then $pq = 0$ by Theorem 1.1 and hence, since the integers q in question are non-zero, $p = 0$; then, from equation 3.50, we have $-4q = k^2$, which is impossible for the given q. Hence $Q = 2$ and thus equation 3.50 becomes

$$p_1^2 - 2k_1^2 = q \tag{3.51}$$

where $p_1 = p/2$, $k_1 = k/2$ are integers. Now the fundamental solution of the equation

$$x^2 - 2y^2 = 1$$

is $x_1 + y_1\sqrt{2} = 3 + 2\sqrt{2}$. Hence by Theorem F, if equation

3.51 has solutions for $q > 0$, one of them must satisfy the inequality

$$0 \leq k_1 \leq 2\sqrt{q}/\sqrt{8} = \sqrt{q/2} \ .$$

Also, by Theorem F, if equation 3.51 has solutions for $q < 0$, then one of them must satisfy

$$0 < k_1 \leq 2\sqrt{|q|}/\sqrt{4} = \sqrt{|q|}.$$

For each of the q involved in this theorem we test all possible k_1 and discover that indeed in each case equation 3.51 has no solutions, and thus the theorem is proven. ▮

In the case $q = 7$, we recall that there exists an integer p such that $F(M(p,q))$ and $F(N(p,q))$ coincide. We are able to show that in fact this p is unique (in absolute value). Thus

<u>Theorem 3.11</u>. $F(M(p,7)) = F(N(p,7))$ if and only if $|p| = 6$.

<u>Proof</u>: Assume p is an integer such that $F(M(p,7))$ and $F(N(p,7))$ coincide and $F(p,7) = R(\sqrt{Q})$, say, where Q is zero or square-free. Then we have

(3.52) $$\delta(p,7) = p^2 - 28 = k^2Q$$

(3.53) $$\Delta(p,7) = (p^2 + 36)(p^2 + 64) = m^2Q$$

for some integers k and m such that $k, m \neq 0$. Now from the previous theorem we see that we must have

$$Q \mid (7 + 1)((7 + 1)^2 + 28)$$

so that $$Q \mid 8 \cdot 2^2 23 \ .$$

Hence, in fact, $Q \mid 2$. We argue as in Theorem 3.10 and conclude that $Q = 2$. We note that if P is a prime such that

$$P \mid ((p^2 + (q+1)^2), (p^2 + (q-1)^2)),$$

then $P \mid 4q$. In this case $4q = 28$ so that P can only be equal to 2 or 7. However, we know that if

$$7 \mid (p^2 + (q \pm 1)^2),$$

then $$7^{2\alpha} \,\overline{|}\, (p^2 + (q \pm 1)^2)$$

for some integer α (where of course α depends on the choice of signs). Hence for a given integer p, one of the following systems of equations must be satisfied:

I	$p^2 + 36 = 4\cdot\Box$	II	$p^2 + 36 = 2\cdot\Box$
	$p^2 + 64 = 2\cdot\Box$		$p^2 + 64 = 4\cdot\Box$
III	$p^2 + 36 = 2\cdot\Box$	IV	$p^2 + 36 = \Box$
	$p^2 + 64 = \Box$		$p^2 + 64 = 2\cdot\Box$

Now from equation 3.52, $p^2 \equiv 2k^2 + 4 (\text{mod } 8)$ so that $p^2 \equiv 4 (\text{mod } 8)$. Hence $p^2 + 36 \equiv 0 (\text{mod } 8)$, and $p^2 + 64 \equiv 4 (\text{mod } 8)$. Hence neither system I nor system IV can hold.

In systems II and III we have $p^2 + 36 = 2n^2$, for some integer n, so that

$$(3.54) \qquad x^2 + 9 = 2y^2$$

where x and y are integers defined by $x = p/2$, $y = n/2$. Further, equation 3.52 yields:

$$(3.55) \qquad x^2 - 7 = 2z^2,$$

where $z = k/2$. Combining equations 3.54 and 3.55 we have

$$2z^2 - 2y^2 = -7 - 9 = -16$$

so that

$$y^2 - z^2 = 8. \tag{3.56}$$

The only solutions of equation 3.56 are $y = \pm 3$, $z = \pm 1$, and these solutions lead to $x = \pm 3$ (from equation 3.55), or $|p| = 6$ (and we recall that in this case the fields coincide). ∎

REFERENCES

1 Drazin, M. P., J. W. Dungey, and K. W. Gruenberg, Some Theorems on Commutative Matrices, J. London Math. Soc., (1951), 26, 221-8.

2 Hoffman, A. J., and O. Taussky, A Characterization of Normal Matrices, J. of Research of the National Bureau of Standards, (1954), 52, 17-19.

3 Nagell, T., Introduction to Number Theory, (1951).

4 Dirichlet, G. L., Zahlentheorie, (1863).

5 Siegel, C. L., The Integral Solutions of the Equation $y^2 = ax^n + bx^{n-1} + \ldots + k$, J. London Math. Soc., (1926), 6, 66-8.

6 LeVeque, W. J., Topics in Number Theory, (1956), II.

7 Hardy, G. H., and E. M. Wright, An Introduction to the Theory of Numbers, (1960).

8 Lundgren, Wilhelm, Solution Complète de Quelques Équations du Sixième Degre à Deux Indeterminées, Archiv for Math. og Naturv., (1946), 48, 177-211.

9 Dickson, L. E., History of the Theory of Numbers, (1920), II.