Pacific Journal of Mathematics

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

Lorraine L. Foster

Vol. 18, No. 1 March 1966

PACIFIC JOURNAL OF MATHEMATICS
Vol. 18, No. 1, 1966

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

LORRAINE L. FOSTER

This paper deals with a special case of the following problem: Let A, B be matrices of order n over the rational integers. Compare the algebraic number field generated by the characteristic roots of AB with those generated by A, B.

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

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

Further, if $c \in S$, there exists an infinite sequence $\{(r_n, s_n)\}$ of distinct pairs of integers such that $F(M(r_n, s_n)) = R(\sqrt{c})$ and $F(N(r_n, s_n)) = R(\sqrt{cd_n})$ for some integers d_n such that $(c, d_n) = 1$. If $c \in S$ and c is odd or $c = 2$, there exists an infinite sequence $\{(r'_n, s'_n)\}$ of distinct pairs of integers such that $F(N(r'_n, s'_n)) = R(\sqrt{c})$ and $F(M(r'_n, s'_n)) = R(\sqrt{cd'_n})$ for some integers d'_n such that $(c, d'_n) = 1$.

There are five known pairs of integers (r, s) with $rs \neq 0$ and $s \neq -1$ such that $F(M(r, s))$ and $F(N(r, s))$ coincide. For $s \equiv 2 \pmod 4$ and for certain odd integers s the fields $F(M(r, s))$ and $F(N(r, s))$ cannot coincide for any integers r.

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

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 $\bar{A}'A = A\bar{A}'$ where $\bar{A}' = (\overline{a_{ji}})$. It is known that if A is normal, with characteristic roots λ_i, $i = 1, \cdots, n$, then[1] the characteristic roots of $A\bar{A}'$ are given by $\lambda_i \cdot \bar{\lambda}_i$, $i = 1, \cdots, n$. Conversely, if the characteristic roots of $A\bar{A}'$ can be written as $\lambda_i \cdot \bar{\lambda}_{\delta_i}$, $i = 1, \cdots, n$, where $\{\delta_1, \cdots, \delta_n\}$ is some permuta-

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

tion of $\{1, \cdots, n\}$ then A is normal.[2] Hence it seems of interest to study the characteristic roots of $A\bar{A}'$ in comparison with the characteristic roots of A in the case of nonnormal 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, I, and the algebraic number fields in which the characteristic roots of A and $A\bar{A}'$ lie are compared.

Specifically, we let $M(r, s)$ denote the companion matrix of the polynomial $x^2 + rx + s$ and consider the set $\{M(r, s) \mid r, s \in I\}$. We define $N(r, s) = M(r, s)\cdot(M(r, s))'$. We observe that $M(0, 1)$ is normal and $M(r, -1)$ is normal (and in fact symmetric) for all $r \in I$. Otherwise, $M(r, s)$ is nonnormal.

We define functions $\delta(r, s)$ and $\Delta(r, s)$ as follows:

$$\begin{aligned}\delta(r, s) &= r^2 - 4s\\ \Delta(r, s) &= (r^2 + s^2 + 1)^2 - 4s^2 .\end{aligned}$$

We note that $\Delta(r, s)$ can also be expressed in the forms

$$(r^2 + (s + 1)^2)(r^2 + (s - 1)^2) , \quad 4r^2s^2 + (r^2 - s^2 + 1)^2 ,$$

and $4r^2 + (r^2 + s^2 - 1)^2$. We denote the fields which the characteristic roots of $M(r, s)$ and $N(r, s)$ generate over the rational number field, R, by $F(M(r, s))$ and $F(N(r, s))$, respectively. Then $F(M(r, s)) = R(\sqrt{\delta(r, s)})$ and $F(N(r, s)) = R(\sqrt{\Delta(r, s)})$. We definte $g_\delta(r, s)$ to be the square-free part of $\delta(r, s)$ if $\delta(r, s) \neq 0$, and $g_\delta(r, s) = 1$ otherwise. Similarly, we define $g_\Delta(r, s)$. This work is therefore concerned with the relationships between $g_\delta(r, s)$ and $g_\Delta(r, s)$. Clearly $F(M(r, s))$ and $F(N(r, s))$ coincide if and only if $g_\delta(r, s) = g_\Delta(r, s)$.

Many of the conjectures proven in this work were suggested by calculations performed on the IBM 7090 computer. The question of the number of pairs (r, s), with $s \neq -1$ and $rs \neq 0$, such that $F(M(r, s))$ and $F(N(r, s))$ coincide is still unanswered. (We can easily see that $g_\delta(r, -1) = g_\Delta(r, -1)$ and $g_\delta(r, 0) = g_\Delta(r, 0)$ for all $r \in I$. Also, $g_\delta(0, s) = g_\Delta(0, s)$ if and only if[3] $s = -\square$.) The computer data and a number of results lead us to conjecture that there exist only finitely many pairs (r, s) satisfying these conditions.

1. The Nature of $F(N(r, s))$. We will conclude in this section that the set of fields $\{F(N(r, s)) \mid rs \neq 0\}$ is precisely the set $\{R(\sqrt{c}) \mid c = a^2 + b^2 \neq 1\}$. We first note

---

[2] This was proven by A.J. Hoffman and 0. Taussky, [2].

[3] In this paper, "$\square$" will always denote an integral square.

THEOREM 1.1. *$g_\Delta(r, s) = 1$ if and only if $rs = 0$.*

Proof. Without restricting generality, we assume $r, s \geqq 0$. We observe that $\Delta(r, s) = (r^2 + s^2 - 1)^2 + 4r^2 = (r^2 + s^2)^2 + 2(r^2 - s^2) + 1$ and that $(r^2 + s^2 + 1)^2 = (r^2 + s^2)^2 + 2(r^2 + s^2) + 1$. Hence if $r > s > 0$ we have $(r^2 + s^2)^2 < \Delta(r, s) < (r^2 + s^2 + 1)^2$, while if $0 < r < s$ we have $(r^2 + s^2 - 1)^2 < \Delta(r, s) < (r^2 + s^2)^2$. Also, $\Delta(r, r) = 4r^4 + 1$. Hence $\Delta(r, s) \neq \square$ for $rs \neq 0$ and the necessity of the condition is proven. To prove sufficiency we observe that $\Delta(0, s) = (s^2 - 1)^2$ and $\Delta(r, 0) = (r^2 + 1)^2$.

Since $g_\Delta(r, s)$ is the square-free part of $4r^2s^2 + (r^2 - s^2 + 1)^2$, we conclude that $g_\Delta(r, s)$ is of the form $a^2 + b^2$, where a and b are relatively prime integers, and, $ab = 0$ if and only if $rs = 0$. The next theorem demonstrates that each form with $ab \neq 0$ is represented by some $g_\Delta(r, s)$. We prove, in fact, rather more. We first recall the following lemma:

LEMMA.[4] *Let $d > 1$ 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 $d = a^2 + b^2$ and $(a, b) = 1$.*

THEOREM 1.2. (i) *Let $c = a^2 + b^2 \neq \square$. Then there exists a sequence $\{(r_n, s_n)\}$, $1 \leqq n < \infty$, such that $r_n < r_{n+1}$, $s_n < s_{n+1}$, and $\Delta(r_n, s_n) = c \cdot \square$.*

(ii) *Further, if c is a product of primes of the form $4N + 1$, there exists a sequence $\{(r'_n, s'_n)\}$, $1 \leqq n < \infty$, such that*

$$r'_n < r'_{n+1},\ s'_n < s'_{n+1},\ \Delta(r'_n, s'_n) = c \cdot \square$$

and $\delta(r'_n, s'_n) = cd_n \cdot \square$, where d_n is some integer relatively prime to c.

Proof. Let $f_0 + g_0\sqrt{c}$ denote any solution of the equation $f^2 - cg^2 = 1, f_0, g_0 > 0$. Write $c = \prod_{i=1}^m P_i^{\beta_i}$ where the primes P_i are distinct and each $\beta_i > 0$. Further, write $g_0 = k \prod_{i=1}^m P_i^{\alpha_i}$, where each $\alpha_i \geqq 0$ and $(k, c) = 1$. Define $c' = g_0/k$ and $d = (c')^2 c$. Then we have

$$f_0^2 - k^2 d = f_0^2 - g_0^2 c = 1 . \tag{1.1}$$

We define $f_n + g_n\sqrt{d} = (f_0 + k\sqrt{d})^{2n}$ and $x_n + y_n\sqrt{d} = (f_n + g_n\sqrt{d})^2 = f_n^2 + g_n^2 d + 2f_n g_n\sqrt{d}$, $n \geqq 1$, so that $f_n^2 - g_n^2 d = 1 = x_n^2 - y_n^2 d$, $x_n = f_{2n}$, and $y_n = g_{2n}$. Clearly $x_n > x_{n-1}$ and $y_n > y_{n-1}$, $n > 1$. We can write $d = a_1^2 + b_1^2$ for some integers $a_1, b_1 > 0$. If each $P_i \equiv 1 \pmod 4$ then by the lemma we can choose a_1 and b_1 to be relatively prime. We

[4] A proof of this result can be found in [3], pp. 164-6.

now define

$$\begin{aligned} u_n + v_n\sqrt{d} &= (d + b_1\sqrt{d})(x_n + y_n\sqrt{d}) \\ &= d(x_n + b_1y_n) + (b_1x_n + dy_n)\sqrt{d},\ n \geqq 1 . \end{aligned}$$

It is clear that

$$u_n^2 - v_n^2d = d^2 - b_1^2d . \tag{1.2}$$

Further, $u_n \equiv 0$, $v_n \equiv b_1 \pmod{d}$, since $x_n \equiv f_n^2 \equiv 1 \pmod{d}$, $n \geqq 1$. It follows that $2u_n/d$, $2(v_n - b_1)/d$ are integers which we shall denote by m_n, k_n, respectively, $n \geqq 1$. Clearly $u_n > u_{n-1}$ so that $k_n > k_{n-1}$. From (1.2) we have $4d^2 - 4b_1^2d = dm_n^2 - d(dk_n + 2b_1)^2$. Simplifying and dividing by d^2, we get

$$dk_n^2 + 4b_1k_n + 4 = m_n^2 . \tag{1.3}$$

We now define

$$r_n = k_na_1,\ s_n = k_nb_1 + 1 ,\quad n \geqq 1.$$

Then $r_n < r_{n+1}$, $s_n < s_{n+1}$, $r_n^2 + (s_n - 1)^2 = k_n^2d$, and $r_n^2 + (s_n + 1)^2 = m_n^2$, from (1.3). Clearly $\Delta(r_n, s_n) = d\cdot\Box = c\cdot\Box$, $n \geqq 1$, so that (i) is proven.

Let us suppose that each $P_i \equiv 1 \pmod{4}$ and that we have chosen a_1, b_1 to be relatively prime. We observe that

$$f_n \equiv 1 \pmod{d} ,\quad n \geqq 1. \tag{1.4}$$

For, $f_1 = f_0 + k^2d = 2k^2d + 1 \equiv 1 \pmod{d}$ by (1.1). Also, if $f_{n-1} \equiv 1 \pmod{d}$, then $f_n = f_{n-1}f_1 + g_{n-1}g_1d \equiv 1 \pmod{d}$. We also observe that

$$(g_1, d) = (2f_0k, d) = (2f_0, d) = 1 , \tag{1.5}$$

by (1.1) and the fact that d is odd. Further, we show by induction that

$$g_n \equiv ng_1 \pmod{d} ,\quad n \geqq 1. \tag{1.6}$$

We assume that $g_{n-1} \equiv (n-1)g_1 \pmod{d}$, $n \geqq 2$. Then

$$g_n = g_{n-1}f_1 + f_{n-1}g_1 \equiv g_{n-1} + g_1 \equiv ng_1 \pmod{d}$$

by (1.4) and the induction is complete. We consider the equation $f(y) = y^2 + 1 \equiv 0 \pmod{P_i}$, $i = 1, \cdots, m$. Since each $P_i \equiv 1 \pmod{4}$, we can find a solution y_i to this equation, for each i. Then we can choose[5] integers y_i' such that $y_i' \equiv y_i \pmod{P_i}$, $f(y_i') = 0 \pmod{P_i^{2\alpha_i+\beta_i}}$, since $f'(y_i) \not\equiv 0 \pmod{P_i}$, $i = 1, \cdots, m$. By the Chinese Remainder Theorem we can choose z such that $z \equiv y_i' \pmod{P_i^{2\alpha_i+\beta_i}}$ for all i, and

[5] For a proof of this statement, see for instance [4], page 87.

hence

$$z^2 + 1 \equiv 0 \pmod{d} . \tag{1.7}$$

Since $(2b_1, d) = 1$, by (1.5) and (1.6) it is clear that the integers $2b_1 g_{td+i}$, $i = 1, \cdots, d$, represent a complete residue system modulo d, for any integer $t \geqq 0$. Hence we can choose an integer $N > 0$ such that $2b_1 g_N \equiv 2b_1 g_{td+N} \equiv z - 1 \pmod{d}$, for every $t \geqq 0$. Then

$$(2b_1 g_{td+N} + 1)^2 + 1 \equiv 0 \pmod{d}$$

by (1.7). Moreover

$$\begin{aligned} \delta(r_{td+N}, s_{td+N}) &= -(k_{td+N} b_1 + 2)^2 + k_{td+N}^2 d \\ &= -(k_{td+N} b_1 + 2)^2 \pmod{d} \end{aligned} \tag{1.8}$$

In general, we can show that

$$\begin{aligned} k_n &= 2(b_1 x_n + d y_n - b_1)/d \\ &= 2(b_1(f_n^2 + g_n^2 d - 1)/d + 2f_n g_n) \equiv 4(b_1 g_n^2 + g_n) \pmod{d}, \end{aligned}$$

using (1.4). Hence

$$k_{td+N} b_1 + 2 \equiv (2b_1 g_{td+N} + 1)^2 + 1 \equiv 0 \pmod{d} , \tag{1.9}$$

so that by (1.8), $\delta(r_{td+N}, s_{td+N}) \equiv 0 \pmod{d}$, $t \geqq 0$. We can show that $((\delta(r_{td+N}, s_{td+N}))/d, d) = 1$. For, assume the contrary. Then

$$P_i^{2\alpha_i+\beta_i+1} \mid \delta(r_{td+N}, s_{td+N}) ,$$

for some i. By (1.9) we know that $P_i^{2(\alpha_i+\beta_i)} \mid (k_{td+N} b_1 + 2)^2$. Hence, by (1.8), $P_i^{2\alpha_i+\beta_i+1} \mid k_{td+N}^2 d$ so that $P_i \mid k_{td+N}$. This is however a contradiction by (1.9). Hence $\delta(r_{td+N}, s_{td+N}) = dd'_{t+1} = cd_{t+1} \cdot \square$ where $(d'_{t+1}, c) = (d_{t+1}, c) = 1$, $t \geqq 0$. If we set $m = (n-1)d + N$, $r'_n = r_m$, $s'_n = s_m$, the proof of (ii) is complete.

2. Further relations between $F(M(r, s))$ and $F(N(r, s))$.

The following theorems are concerned with various comparisons of the fields $F(M(r, s))$ and $F(N(r, s))$. We observe from Theorem 1.2 (ii) that, for every square-free odd integer $c = a^2 + b^2$ there exist infinitely many pairs (r, s), $rs \neq 0$, $s \neq -1$, such that $g_\Delta(r, s) \mid g_\delta(r, s)$ and $g_\Delta(r, s) = c$. In this section we will demonstrate that if $c = a^2 + b^2$ is a square-free integer then there exist infinitely many pairs (r, s), $rs \neq 0$, $s \neq -1$, such that $g_\delta(r, s) \mid g_\Delta(r, s)$ and $g_\delta(r, s) = c$. We first prove the following theorem, which essentially states the conclusion of Theorem 1.2 (ii) for the case $c = 2$.

THEOREM 2.1. *There exists a sequence* $\{(r_n, s_n)\}$, $1 \leqq n < \infty$, *of* *pairs of integers such that* $g_\Delta(r_n, s_n) = 2$, $g_\delta(r_n, s_n) = 2d_n$, *where* d_n *is some odd integer and* $|s_n| < |s_{n+1}|$, $n \geqq 1$.

Proof. Define integers x_n, y_n by the relation $x_n + y_n\sqrt{2} = (1+\sqrt{2})^{2n-1}$, $n \geqq 1$. Then $x_n^2 - 2y_n^2 = -1$ and $x_n \equiv y_n \equiv 1 \pmod 2$. Also define integers f_n, s_n by the relations: $|f_n| = x_n$, $|s_n| = y_n$, $f_n \equiv s_n \equiv -1 \pmod 4$, $n \geqq 1$. Further define $r_n = f_n + s_n$. Then $r_n^2 - s_n^2 + 1 - 2r_ns_n = 0$ so that $\Delta(r_n, s_n) = (r_n^2 - s_n^2 + 1)^2 + 4r_n^2s_n^2 = 8r_n^2s_n^2$. Hence $g_\Delta(r_n, s_n) = 2$, $n \geqq 1$. Furthermore, $\delta(r_n, s_n) = 4((f_n + s_n)^2/4 - s_n)$, and since $f_n + s_n \equiv -2 \pmod 4$, we have $\delta(r_n, s_n)/4 \equiv 2 \pmod 4$. Hence $g_\delta(r_n, s_n) = 2d_n$, where d_n is odd, $n \geqq 1$.

We will prove the following theorem:

THEOREM 2.2. *Let* $c = a^2 + b^2$ *be a square-free integer. Then there exist infinite sequences* $\{r_n\}$, $\{s_n\}$, *and* $\{s'_n\}$, *such that* $r_n < r_{n+1}$, $s_n \neq 0, -1$, $g_\delta(r_n, s_n) = c$, $g_\Delta(r_n, s_n) = cc_n$, $g_\delta(r_n, s'_n) = -c$, *and* $g_\Delta(r_n, s'_n) = cc'_n$, *where* c_n *and* c'_n *are integers relatively prime to* c, $n = 1, 2, \cdots$.

We first prove three lemmas:

LEMMA 1. *Suppose* $c = t^2u > 0$, u *odd. Further suppose that* $c \mid r^2 + 4$, *for some integer* $r > 0$. *Then there exists an integer* $s \neq 0, -1$ *such that* $F(M(r, s)) = R(\sqrt{c})$ *and* $F(N(r, s)) = R(\sqrt{cc'})$, *where* c' *is some integer relatively prime to* c.

Proof. We define an integer f to be c or $c/4$ according as c is odd or even. Now $r^2 + 4 \not\equiv 0 \pmod{16}$ so that it is clear that $f \equiv 1 \pmod 4$. We define an integer $d = (r^2 + 4)/f$. Clearly $d \equiv 0$ or $1 \pmod 4$. We can therefore define a positive integer k as follows:

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

Observe that $k^2 \equiv d \pmod 4$. Define the integer $s = f((d - k^2)/4) - 1$. Evidently $s < -1$. Also, $\delta(r, s) = fk^2$. Furthermore, since $(f, rk) = 1$ it is clear that $\Delta(r, s) = fc_1$, where $c_1 = (k^2 + f((d - k^2)/4)^2)(r^2 + (s+1)^2)$ and $(c_1, f) = 1$. Hence $F(M(r, s)) = R(\sqrt{c})$, $F(N(r, s)) = R(\sqrt{cc_1})$, and if c is odd, $(c, c_1) = (f, c_1) = 1$ and the proof is complete. If c is even then $k^2 \equiv d \equiv 0 \pmod 4$, $(d - k^2)/4 \not\equiv 0 \pmod 2$ and $r^2 \equiv 0 \pmod 4$. Hence c_1 is odd and $(c, c_1) = 1$.

LEMMA 2. *Suppose* $c = t^2u > 0$, u *odd. Suppose also that* $c \mid r^2 + 4$

for some even integer $r > 0$. *Then there exists an integer* $s > 0$ *such that* $F(M(r, s)) = R(\sqrt{-c})$ *and* $F(N(r, s)) = R(\sqrt{cc_1})$ *for some integer* c_1 *relatively prime to* c.

Proof. (Observe that the requirement that r be even is necessary since $c > 0$, $c \mid r^2 + 4$, and $\delta(r, s) \equiv 0$ or $1 \pmod 4$.) We define an integer $r_1 = r/2$ and define integers f and d as in the preceding proof. We also define an integer $e = d/4$ and can choose an integer $j > 0$ such that $(j, f) = 1$ and $e \not\equiv j \pmod 2$, since f is odd. The reader may verify that if we choose $s = f(e + j^2) - 1$, the lemma is proven.

LEMMA 3. *Suppose* $c = 2t^2u > 0$ *where* u *is a square-free odd integer. Suppose also that* $c \mid r^2 + 4$ *and* $\varepsilon = \pm 1$. *Then:*

(i) *If* $r^2 + 4 \equiv 0 \pmod 8$ *there exists an integer* $s \neq 0, -1$ *such that* $F(M(r, s)) = R(\sqrt{\varepsilon c})$ *and* $F(N(r, s)) = R(\sqrt{cc_1})$ *where* c_1 *is some integer relatively prime to* c.

(ii) *If* $r^2 + 4 \equiv 4 \pmod 8$ *there exist no integers* s *and* c_1 *such that* $F(M(r, s)) = R(\sqrt{\varepsilon c})$, $F(N(r, s)) = R(\sqrt{cc_1})$ *and* $(c_1, c/t^2) = 1$.

Proof. We can define an integer $r_1 = r/2$. To prove (i) we suppose that $r^2 + 4 \equiv 0 \pmod 8$ and define integers d and e as in the proof of Lemma 2. We also define $f = c/4$ or c according as $c \equiv 0$ or $c \equiv 2 \pmod 4$. We can further define an odd integer $f_1 = f/2$ and choose an even integer $j > 0$ so that $(f_1, j) = 1$, $j > 2e$. To complete the proof of (i) we define $s = f(e - \varepsilon j^2) - 1$ and note that $f_1 \equiv 1 \equiv e \pmod 4$, $r_1 \equiv 1 \pmod 2$. Details are left to the reader.

To prove (ii) we assume that $r^2 + 4 \equiv 4 \pmod 8$, and assume the conclusion false. Then there exist integers s and c_1 (we may assume c_1 is square-free) such that

$$g_\delta(r, s) = 2\varepsilon u \tag{2.1}$$

$$g_\Delta(r, s) = 2c_1 u\,, \qquad (c_1, 2u) = 1. \tag{2.2}$$

Define an odd integer $g = (r^2 + 4)/4u$. Then, by (2.1),

$$\delta(r, s) = 4ug - 4(s + 1) = 2k^2 u\varepsilon\,,$$

for some integer $k > 0$. We conclude that $k/2$ is an integer, m say, since u is odd. We also conclude that

$$\Delta(r, s) = u(2k^2\varepsilon + u(g - 2m^2\varepsilon)^2)\cdot(4r_1^2 + u^2(g - 2m^2\varepsilon)^2) \equiv 1 \pmod 2\,,$$

which contradicts (2.2). Hence (ii) is proven.

Proof of Theorem 2.2. Write $c = \prod_{i=1}^{t} P_i$ where the P_i are distinct primes of the form $4N + 1$ or 2. Let x_i be an integer such that $x_i^2 + 1 \equiv 0 \pmod{P_i}$, $i = 1, \cdots, t$ and choose z such that $z \equiv x_i \pmod{P_i}$,

$i = 1, \cdots, t$. Also, define $r_n = 2(z + (n-1)c)$, $n \geqq 1$. Clearly $r_n^2 + 4 \equiv 4(z^2 + 1) \equiv 0 \pmod{c}$, $n \geqq 1$. Assume c is odd. Then by Lemma 1 there exists an integer $s_n \neq 0, -1$ such that $g_\delta(r_n, s_n) = c$ and $g_\Delta(r_n, s_n) = cc_n$, where c_n is some integer relatively prime to c. Further, since r_n is even, by Lemma 2 there exists an integer $s'_n > 0$ such that $g_\delta(r_n, s'_n) = -c$ and $g_\Delta(r_n, s'_n) = cc'_n$, where $(c, c'_n) = 1$. Hence if c is odd the theorem is proven. We assume c is even. Then z is odd so that $r_n/2 \equiv 1 \pmod{2}$ and hence $r_n^2 + 4 \equiv 0 \pmod{8}$, $n \geqq 1$. We take $\varepsilon = 1, -1$ sucessively in Lemma 3 and the theorem is proven.

Taking a different viewpoint we have:

THEOREM 2.3. *For every integer $r > 0$ there exist infinitely many distinct integers s such that $g_\delta(r, s) \mid g_\Delta(r, s)$, $\mid g_\delta(r, s) \mid \neq 1$.*

Proof. Assume first that $r \neq 2$. Then, since $r^2 + 4 \not\equiv 0 \pmod{16}$, we know that $r^2 + 4$ has an odd square-free divisor c, say, $c > 1$. We define $d = (r^2 + 4)/c$ and choose an integer $e > 0$ such that $e^2 \equiv d \pmod{4}$ and $(e, c) = 1$. We then define $k_n = 2cn + e$, $n \geqq 0$. Clearly $k_n^2 \equiv d \pmod{4}$ and $(k_n, c) = 1$. Hence we can define $s_n = (c(d - k_n^2)/4) - 1$, $n \geqq 0$, and, as in the proof of Lemma 1 (with $f = c$), we conclude that $g_\delta(r, s_n) = c$, $g_\Delta(r, s_n) = cc_n$, where c_n is some integer relatively prime to c. Hence if $r \neq 2$ the theorem is proven. In the case $r = 2$ we define $s_n = 1 - 2n^2$, $n \geqq 1$, and observe that $\Delta(2, s_n) = 32c'_n$, $\delta(2, s_n) = 2 \cdot \square$, where c'_n is odd.

3. On the coincidence of $F(M(r, s))$ and $F(N(r, s))$. The following known theorem, which is a special case of a theorem by C.L. Siegel [5], will be applied frequently in this section.[6]

THEOREM A. *Let $f(x)$ be a polynomial of degree $n \geqq 3$ with integral coefficients and distinct zeros and let A be a nonzero integer. Then the equation $f(x) = Ay^2$ has at most a finite number of integral solutions (x, y).*

Computations for pairs of integers (r, s) satisfying the inequalities $0 \leqq |r| \leqq 600$, $0 \leqq |s| \leqq 800$ revealed five pairs (r, s) with $rs \neq 0$, $s \neq -1$ such that the fields $F(M(r, s))$ and $F(N(r, s))$ coincide. These are: $(r, s) = (6, 7)$, $(14, 47)$, $(11, -76)$ $(141, -236)$ and $(40, 31)$. The corresponding values of $g_\Delta(r, s)$ are: 2, 2, 17, 17, 41. In this section we will prove several theorems which resulted from a study of these five pairs, and which in some sense, limit the number of pairs (r, s) for

[6] A proof of this theorem is given in [6], pp. 155-7.

which coincidence occurs.

We first observe that in three cases of coincidence we have $\delta(r, s) = 8$. This leads us to inquire if any additional pairs (r, s) exist with these properties. We find

THEOREM 3.1. *Suppose* $g_\delta(r, s) = g_\Delta(r, s)$, $\delta(r, s) = 8$, *and* $r \geqq 0$. *Then* $(r, s) = (2, -1)$, $(6, 7)$, *or* $(14, 47)$.

Proof. Under the above hypotheses, $r^2 - 4s = 8$, $r^2 + (s+1)^2 = (s+3)^2$, $r^2 + (s-1)^2 = (s+1)^2 + 8$, and $\Delta(r, s) = 2\cdot\square \neq 0$. Hence there exists an integer $k > 0$ such that $(s+1)^2 + 8 = 2k^2$. Define an integer $x = r/2$. Clearly $(x^2 - 1)^2 + 8 = 2k^2$ so that x is odd and k is even. Define $y = k/2$ and observe that

$$((x^2-1)/8)^2 = (y^2-1)/8\ . \tag{3.1}$$

We can then define[7] integers u and v by $x = 2u - 1$, $y = 2v - 1$ so that (3.1) becomes $\binom{u}{2}^2 = \binom{v}{2}$. The only solutions[8] of this equation are $(u, v) = (1, 1)$, $(2, 2)$ and $(4, 9)$ and these solutions correspond to $(r, s) = (2, -1)$, $(6, 7)$, and $(14, 47)$, respectively.

In the preceding theorem we required that $\delta(r, s) = 8$. We now suppose that $\delta(r, s) = K$, a constant. We have:

THEOREM 3.2. *There exist at most a finite number of pairs* (r, s) *such that* $g_\delta(r, s) = g_\Delta(r, s)$ *and* $\delta(r, s) = K$, *a constant.*

Proof. If $K = 0$ the fields coincide only for $(r, s) = (0, 0)$. Hence we assume $K \neq 0$. We may also assume $K \neq 8$, by Theorem 3.1. We write $K = k^2Q$ where Q is square-free. Suppose $g_\delta(r, s) = g_\Delta(r, s)$. Then we must have $\Delta(r, s) = h^2Q$ for some integer h. Since $\delta(r, s) = r^2 - 4s = k^2Q$, this implies

$$(k^2Q + 4s + (s+1)^2)\cdot(k^2Q + (s+1)^2) = h^2Q\ . \tag{3.2}$$

The left-hand side of (3.2) is a polynomial in s of degree four with roots $s = -3 \pm (s - k^2Q)^{1/2}$, $-1 \pm k\sqrt{-Q}$, and, under our hypotheses, these four roots are distinct. Hence by Theorem A we conclude that (3.2) has at most a finite number of solutions (s, h). This proves the theorem since K and s determine $|r|$ uniquely.

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

---

[7] The author is indebted to H. Hasse for this transformation.

[8] For a proof of this assertion, see [**7**], pages 202-7.

THEOREM 3.3. *For any integer $s \neq -1$, 0, there exist at most a finite number of integers r such that $g_\delta(r, s) = g_\Delta(r, s)$.*

We require the following lemma:

LEMMA. $g_\delta(r, 1) \neq g_\Delta(r, 1)$ *for all* r.

Proof. Suppose the lemma false. Then, for some $r > 0$ there exist integers h, k such that $r^2 - 4 = k^2Q$, $(r^2 + 4)r^2 = h^2Q$, where $Q = g_\delta(r, 1) = g_\Delta(r, 1) > 0$. We observe that we must have $hk \neq 0$, $r \neq 0$. Since Q is square-free, $r \mid h$. Hence we can define an integer $j = h/r$. Thus we conclude that $8 = (j^2 - k^2)Q$ and $Q = 1$ or 2. If $Q = 1$ then $r^2 = k^2 + 4$ and if $Q = 2$ then $j^2 = k^2 + 4$ and both equations are impossible since $k \neq 0$.

Proof of Theorem 3.3. By the lemma we may assume $s \neq 1$. Hence let s and Q be fixed integers such that $s \neq 0, \pm 1$ and $Q > 0$ is square-free. Observe that the equation $g_\Delta(r, s) = Q$ has at most a finite number of solutions r. For this equation implies that

$$\Delta(r, s) = h^2Q \ . \tag{3.3}$$

Now $\Delta(r, s)$ is a polynomial of degree four in r with distinct roots $r = \pm\, i(s \pm 1)$, $(i = \sqrt{-1})$ and hence for fixed $s \neq \pm\, 1, 0$, equation (3.3) has at most a finite number of pairs of solutions (r, h), by Theorem A.

Now observe that for fixed $s \neq -1$ there exist at most a finite number of square-free integers Q such that

$$g_\delta(r, s) = g_\Delta(r, s) = Q \ . \tag{3.4}$$

For this equation implies, by (3.2), that $(s + 1)^2(s^2 + 6s + 1) \equiv 0 \pmod{Q}$. Combining these results, we have the theorem.

A similar theorem for fixed r is true:

THEOREM 3.4. *For a given integer $r \neq 0$ there exist at most a finite number of integers s such that $g_\delta(r, s) = g_\Delta(r, s)$.*

Proof. We observe that for fixed square-free integers Q and $r > 0$ equation (3.3) has at most a finite number of solutions (s, h). For, the roots $s = \pm 1 \pm ir$ $(i = \sqrt{-1})$ are distinct and Theorem A applies. Further it is clear that if (3.4) is satisfied then $Q \mid (r^4 + 24r^2 + 16)(r^2 + 4)$. Hence, as above, the theorem is proven.

We observe that the pairs (r, s) such that $g_\delta(r, s) = g_\Delta(r, s)$ have the property that $s \not\equiv 2 \pmod 4$. This must always be the case as is seen by the following theorem

THEOREM 3.5. *Suppose* $g_\delta(r, s) = g_\Delta(r, s)$. *Then* $s \not\equiv 2 \pmod 4$.

Proof. Suppose the theorem is false, for some (r, s), $s \equiv 2 \pmod 4$. Then there exist integers h and k such that

$$\delta(r, s) = r^2 - 4s = k^2 Q \tag{3.5}$$

$$\Delta(r, s) = (r^2 + (s+1)^2)\cdot(r^2 + (s-1)^2) = h^2 Q \tag{3.6}$$

where $Q = g_\delta(r, s) = g_\Delta(r, s) > 0$. We can see by Theorem 1.1 and the fact that $s \equiv 2 \pmod 4$ that $hk \neq 0$. Now Q is a square-free product of primes of the form $4N + 1$ or twice such a product. Hence $Q \equiv 1$, 2 or $5 \pmod 8$. We show that Q is odd. For, (3.5) and (3.6) imply (3.2) which yields:

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

since s is even. Hence $Q \equiv 1$ or $5 \pmod 8$. We assume first that $Q \equiv 5 \pmod 8$. Equation (3.5) implies $r^2 \equiv 5k^2 \pmod 8$ so that r is even and $(r^2 + (s+1)^2)\cdot(r^2 + (s-1)^2 \equiv 1 \pmod 8$. This contradicts (3.6). Hence we can assume $Q \equiv 1 \pmod 8$. We can write

$$r^2 + (s+1)^2 = \beta_1^2 Q_1 n \tag{3.7}$$

$$r^2 + (s-1)^2 = \beta_2^2 Q_2 n \tag{3.8}$$

where $\beta_1, \beta_2, Q_1, Q_2, n$ are integers such that $Q_1Q_2 = Q$ and n is square-free. Combining (3.5) and (3.7) we have $4s + k^2Q_1Q_2 + (s+1)^2 = \beta_1^2Q_1n$ so that

$$4s + (s+1)^2 \equiv 0 \pmod{Q_1}\,. \tag{3.9}$$

Similarly, $(s+1)^2 \equiv 0 \pmod{Q_2}$ so that $Q_2 \mid s + 1$. Now $Q_1 = \prod P_i$, where the P_i are distinct primes of the form $4N + 1$. We assert that each $P_i \equiv 1 \pmod 8$. For, let x be the integer $s/2$ and observe that (3.9) implies $(2x + 3)^2 \equiv 8 \pmod{P_i}$.

Now[9] $\left(\frac{8}{P_i}\right) = \left(\frac{2}{P_i}\right) = -1$ if $P_i \equiv 5 \pmod 8$.

Hence $P_i \equiv 1 \pmod 8$ so that $Q_1 \equiv 1 \equiv Q_2 \pmod 8$. Now from (3.5) we have $r^2 \equiv k^2 + 8$ or $9k^2 + 8 \pmod{16}$ so that $r^2 \equiv 1$ or $9 \pmod{16}$. Clearly $(s+1)^2 \not\equiv (s-1)^2 \pmod{16}$. Hence there are four possible cases

1. $(s+1)^2 \equiv 1,\quad (s-1)^2 \equiv 9,\quad r^2 \equiv 1 \pmod{16}$
2. $(s+1)^2 \equiv 9,\quad (s-1)^2 \equiv 1,\quad r^2 \equiv 1 \pmod{16}$

[9] For a proof of this result see for instance [**9**], p. 75.

3. $(s+1)^2 \equiv 1, \quad (s-1)^2 \equiv 9, \quad r^2 \equiv 9 \pmod{16}$

4. $(s+1)^2 \equiv 9, \quad (s-1)^2 \equiv 1, \quad r^2 \equiv 9 \pmod{16}$

In cases 1 and 4 we have $r^2 + (s+1)^2 \equiv 2$, $r^2 + (s-1)^2 \equiv 10 \pmod{16}$. Hence from (3.7) and (3.8) we have

$$\beta_1^2 Q_1 n \equiv 2, \ \beta_2^2 Q_2 n \equiv 10 \pmod{16} . \tag{3.10}$$

Clearly β_1 and β_2 are odd and n is even so that $\beta_1^2 Q_1 \equiv 1 \equiv \beta_2^2 Q_2 \pmod 8$ and $n(\beta_1^2 Q_1 - \beta_2^2 Q_2) \equiv 0 \pmod{16}$ which is impossible by (3.10). Similarly in cases 2 and 4 we deduce a contradiction.

We recall from the lemma to Theorem 3.3 that $g_\delta(r, 1) \neq g_\Delta(r, 1)$ for all r. For certain other odd integers s we can also demonstrate that $g_\delta(r, s) \neq g_\Delta(r, s)$ for all r. We have

THEOREM 3.6. *Suppose* $g_\delta(r, s) = g_\Delta(r, s)$. *Then* $s \neq 1, 3, 5, 11, 15, -3, -5,$ *and* -13.

Proof. Let $s \neq 1$ be one of the values listed and assume the theorem is false. Then from (3.2),

$$g(s) = (s+1)((s+1)^2 + 4s) \equiv 0 \pmod Q$$

where $g_\delta(r, s) = g_\Delta(r, s) = Q > 0$ is square-free and $g(s)$ is defined by this equation. We tabulate $g(s)$ for each $s \neq 1$ in the statement of the theorem and find that in each case Q can only be 1 or 2. It is clear by (3.5) and Theorem 1.1 that $Q \neq 1$ for the given values of s. Hence Q can only be 2 so that (3.5) becomes

$$r_1^2 - 2k_1^2 = s \tag{3.11}$$

where $r_1 = s/2$ and $k_1 = k/2$ are integers. Now the fundamental solution of the equation $x^2 - 2y^2 = 1$ is $3 + 2\sqrt{2}$. Hence, if (3.11) has solutions,[10] one of them must satisfy

$$0 \leqq k_1 \leqq \sqrt{s/2} \text{ if } s > 0, \ 0 < k_1 \leqq \sqrt{|s|} \text{ if } s < 0 .$$

For each $s \neq 1$ listed we test all possible k and discover that in fact (3.11) has no solutions and thus the theorem is proven.

We recall that $g_\delta(6, 7) = g_\Delta(6, 7)$. We ask if there are other integers r such that $g_\delta(r, r+1) = g_\Delta(r, r+1)$ or such that $g_\delta(r, 7) = g_\Delta(r, 7)$. The following two theorems answer these questions.

THEOREM 3.7. $g_\delta(r, r+1) = g_\Delta(r, r+1)$ *if and only if* $r = -1$,

[10] Here we have used Theorems 108, 108a, [4].

-2 or 6.

Proof. Sufficiency is clear. Hence we assume

$$g_\delta(r, r+1) = g_\Delta(r, r+1) \tag{3.12}$$

for some $r \neq 0$. Let $s = r+1$. Then there exist positive integers h, k and Q such that Q is square-free and

$$\delta(r, s) = s^2 - 6s + 1 = k^2 Q \tag{3.13}$$

$$\Delta(r, s) = 2r^2(s^2+1) = 2r^2h^2Q\ . \tag{3.14}$$

Hence

$$s^2 + 1 = h^2 Q \tag{3.15}$$

$$6s = (k^2 - h^2)Q\ . \tag{3.16}$$

Equation (3.16), together with (3.13) and (3.14) implies $Q = 1$ or 2. If $Q = 1$ then $r = 0$ or -1 by Theorem 1.1. If $r = 0$, equation (3.12) is not satisfied.

Hence we assume $Q = 2$. Then, combining (3.15) and (3.16) we have

$$((h^2 - k^2)/3)^2 = 2h^2 - 1\ . \tag{3.17}$$

We will show that (3.17) has only two solutions which correspond to $r = -2, 6$. Let $y = |h - k|$, $x = (h^2 - k^2)/3$ and suppose $h \geqq 30$. We consider the cases $y \geqq 5$, $y = 4$, $y = 3$ and find that in each case $x^2 > 2h^2 - 1$. Also, if $y = 1$ or 2 then $x^2 < 2h^2 - 1$ so that for $h \geqq 30$ equation (3.17) has no solutions. Equation (3.17) implies that $2h^2 - 1 = \square$ and the solutions of this equation such that $h < 30$ are $h = 1, 5, 29$. Substituting in (3.17) we find solutions $(h, k) = (1, 2)$, $(5, 2)$, so that $r = -2, 6$.

THEOREM 3.8. *$g_\delta(r, 7) = g_\Delta(r, 7)$ if and only if $|r| = 6$.*

Proof. Suppose $g_\delta(r, 7) = g_\Delta(r, 7) = Q$ for some $r > 0$. Then there exist positive integers h and k such that

$$\delta(r, 7) = r^2 - 28 = k^2 Q \tag{3.18}$$

$$\Delta(r, 7) = (r^2 + 36)(r^2 + 64) = h^2 Q \tag{3.19}$$

so that $Q \mid 32 \cdot 23$. Hence $Q = 1$ or 2. By Theorem 1.1, $Q = 2$. By (3.18), $r^2 \equiv 4 \pmod 8$ so that $r^2 + 64 \equiv 4 \pmod 8$. Hence from (3.19) we can easily see that $r^2 + 64 = \square$ and $r^2 + 36 = 2 \cdot \square$. Hence $r/2$ is an integer, x, and $x^2 + 9 = 2y^2$ for some $y > 0$. Hence, from (3.18), $y^2 - z^2 = 8$, where z is the integer $k/2$. Hence $y = 3$, $z = 1$ so that

$r = 6$.

This research is part of the author's doctoral thesis submitted April, 1964 at California Institute of Technology. The author is indebted to Dr. Olga Taussky Todd for suggesting the problem and for her helpful guidance in preparation of the thesis. Further, the author is indebted to the National Science Foundation and the California Institute of Technology for financial assistance.

REFERENCES

1. M. P. Drazin, J. W. Dungey, and K. W. Gruenberg, *Some theorems on commutative matrices*, J. London Math. Soc. **26** (1951), 221-8.
2. A. J. Hoffman, and O. Taussky, *A Characterization of Normal Matrices*, J. of Research of the National Bureau of Standards, **52** (1954), 17-19.
3. G. L. Dirichlet *Zahlentheorie*, (1863)
4. T. Nagell, *Introduction to Number Theory*, New York, (1951).
5. C. L. Siegel, *The Integral Solutions of the Equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. London Math. Soc., **6** (1926), 66-8.
6. W. J. LeVeque, *Topics in Number Theory*, II, Reading, (1956).
7. Wilhelm Lundgren, *Solution Complète de Quelques Équations du Sixième Degré à Deux Indeterminées*. Archiv for Math. og Naturv., **48**, 177-211.
8. L. E., Dickson, *History of the Theory of Numbers*, II, New York, (1920).
9. G.H., Hardy, and E. M. Wright *An Introduction to the Theory of Numbers*, New York, (1960).

Received September 22, 1964.

Printed in Japan by International Academic Printing Co., Ltd., Tokyo Japan

Pacific Journal of Mathematics
Vol. 18, No. 1 March, 1966