Mathematical Journal of Okayama University

Volume 27, *Issue* 1 1985 *Article* 20

JANUARY 1985

Some arithmetical properties on 2×2 integral matrices

Takeo Funakura* Nobuaki Morimoto†

*Okayama University of Science

†Tosa Women's High School

Math. J. Okayama Univ. 27 (1985), 135—146

SOME ARITHMETICAL PROPERTIES ON 2×2 INTEGRAL MATRICES

TAKEO FUNAKURA and NOBUAKI MORIMOTO

0. Introduction. We use $\mathbf{Z}$ for the set of all integers and $M_2(\mathbf{Z})$ for the set of all 2×2 integral matrices. A matrix A in $M_2(\mathbf{Z})$ is called a quadratic residue modulo a prime number p if the congruence

$$(*) \qquad X^2 \equiv A \pmod{p}$$

has a solution in $M_2(\mathbf{Z})$. Let $|A|$ and $tr\,A$ be the determinant and the trace of A respectively. We denote the zero matrix by O and the unit matrix by E. We define the functions χ_p on $\mathbf{Z}$ by

$$\chi_p(n) = \begin{cases} \left(\frac{n}{p}\right) & \text{if } p \nmid n \\ 0 & \text{if } p \mid n \end{cases} \qquad \text{for any odd prime number } p,$$

$$\chi_2(n) = \begin{cases} 1 & \text{if } 2 \nmid n \\ 0 & \text{if } 2 \mid n, \end{cases}$$

where $\left(\frac{-}{p}\right)$ is the Legendre symbol. In this paper, an integer n is called a quadratic residue modulo p if $x^2 \equiv n \pmod{p}$ has a solution in $\mathbf{Z}$. Namely n is a quadratic residue if and only if $\chi_p(n) = 0$ or 1.

The aim of this paper is to study some analogies on $M_2(\mathbf{Z})$ to some arithmetical properties on $\mathbf{Z}$ related to quadratic residues. To the question "Does the Hasse principle apply in $M_2(\mathbf{Z})$?", we shall answer in Section 2.

If an integer is a quadratic residue modulo p for almost all prime numbers p, then it is a square of an integer. We shall show in Theorem 3 that if a 2×2 integral matrix is a quadratic residue modulo p for almost all prime numbers p, then it is a square of a rational matrix but not always a square of an integral matrix. Every integer is congruent to a sum of two squares modulo p for all prime numbers p; this result remains true if "integer" is replaced by "2×2 integral matrix". See Theorem 6. Corresponding to the Lagrange theorem that every positive integer can represented as a sum of four squares of integers, it will be proved in Theorems 7, 8, and 10 that every 2×2 integral matrix can be represented as a sum of two squares of rational regular matrices, as a sum of three squares of integral matrices, and also as a sum of four squares of integral regular matrices.

Theorem 8 already occurs in Carlitz [1], Griffin-Krusemeyer [3], and Newmann [4]. Our proof is somewhat simpler than the previous proofs. Furthermore we shall give in Theorem 9 a necessary and sufficient condition that a 2×2 integral matrix can be represented as a sum of two squares of integral matrices. Also, as to products of squares, we shall obtain some results in Corollary 2 and Theorem 5.

1. The summary of Rosenfeld's result.

Theorem 1. *Let p be any prime number. The number of incongruent solutions of $(*)$ is as follows.*

(i) *If A is congruent to a scalar matrix, that is, $A \equiv nE \pmod p$ for some n in $\mathbf{Z}$, then the number is*

$$p^2+\chi_p(2\ tr\ A)p+\chi_p(2\ tr\ A)+\chi_2(p).$$

(ii) *Otherwise, the number is*

$$\sum_{\substack{n \pmod p \\ n^2 \equiv |A|}} \chi_p(tr\ A+2n)(\chi_p(tr\ A+2n)+\chi_2(p)).$$

Proof. The assertion (i) is Proposition 1 of [6]. The assertion (ii) follows from Propositions 2, 3 and 4 of [6].

Theorem 1 yields a criterion for quadratic residues on $M_2(\mathbf{Z})$. This criterion appears in [2].

Corollary 1. *Let p be any prime number. A 2×2 integral matrix A is a quadratic residue modulo p if and only if either* (i) *or* (ii) *holds.*

(i) *A is congruent to a scalar matrix modulo p.*

(ii) *There exists an integer n such that*

$$|A| \equiv n^2 \pmod p \quad \text{and} \quad \chi_p(tr\ A+2n) = 1.$$

Corollary 2. *Let p be any odd prime number. A 2×2 integral matrix is congruent to a product of two squares of integral matrices modulo p if and only if its determinant is a quadratic residue modulo p.*

Proof. If there exist X, Y such that $A \equiv X^2Y^2$, then $|A| \equiv |X|^2|Y|^2$, which implies $\chi_p(|A|) \neq -1$.

Conversely we assume that there exists an integer n with $|A| \equiv n^2$. If

$m_+ = tr\,A+2n$ does not vanish then m_+A satisfies (ii) of Corollary 1, so that $m_+A \equiv X^2$ for some X in $M_2(\mathbf{Z})$. Putting $Y = \begin{pmatrix} 0 & y \\ 1 & 0 \end{pmatrix}$, where $ym_+ \equiv 1$, we get $A \equiv X^2Y^2$. The case when $m_- = tr\,A-2n$ does not vanish is similar to the above. If both m_+ and m_- vanish, then $tr\,A \equiv 0$ and $|A| \equiv n^2 \equiv 0$. Then both the $(1,2)$-entry and the $(2,1)$-entry do not vanish if $A \not\equiv 0$. Suppose now that the $(1,2)$-entry denoted by b does not vanish. Putting $B = \begin{pmatrix} 1 & 0 \\ 4b & 1 \end{pmatrix}$, we have $|BA| \equiv 0$ and $tr\,BA \equiv (2b)^2$, so that by Corollary 1 there exists Y such that $BA \equiv Y^2$. Since $B^{-1} = \begin{pmatrix} 1 & 0 \\ -2b & 1 \end{pmatrix}^2 = X^2$, we have $A \equiv X^2Y^2$. If the $(2,1)$-entry does not vanish, then applying the above to the transposed matrix ${}^tA$, we obtain ${}^tA \equiv X^2Y^2$, that is, $A \equiv ({}^tY)^2({}^tX)^2$.

Corollary 3. *Let p be an odd prime number. The set of squares in the general linear group $GL(2,p)$ over the finite field $\mathbf{Z}/p\mathbf{Z}$ generates a subgroup of index 2.*

Proof. This follows from Corollary 2.

Remark. It follows from Proposition 5 and Lemma 1 of [6] that the ratio of the number of squares in $GL(2,p)$ to the cardinal number of $GL(2,p)$ is $3/8+O(1/p)$ and that such a ratio in $M_2(\mathbf{Z})/pM_2(\mathbf{Z})$ is also $3/8+O(1/p)$, where $O(\ )$ is the Landau symbol.

2. The Hasse principle on quadratic residues. As to this notion, see pages 76 and 112 of LeVeque [8].

Theorem 2. *Let a be an integer.*

(i) *The density of prime numbers p with $\chi_p(a) = 1$ is 1 if a is a square of an integer, and $1/2$ otherwise.*

(ii) *The density of prime numbers p with $\chi_p(a) = -1$ is 0 if a is a square of an integer, and $1/2$ otherwise.*

Proof. See Proposition 14 of Chapter VI of Serre [7].

Theorem 3. *A 2×2 integral matrix is a quadratic residue modulo p for almost all prime numbers p if and only if it is a square of a rational matrix.*

Proof. The sufficiency is clear.

The necessity : If there are infinitely many prime numbers p such that (i) of Corollary 1 holds, then there exists an integer n such that $A = nE$, and so $A = \begin{pmatrix} 0 & n \\ 1 & 0 \end{pmatrix}^2$. Suppose now that (i) of Corollary 1 holds for only finitely many prime numbers. Then (ii) of Corollary 1 holds for almost all prime numbers. Since $\chi_p(|A|) = 0$ or 1 for almost all prime numbers p, we see that there exists an integer n such that $|A| = n^2$. We put

$$P_+ = \{p : \chi_p(m_+) = 1, \ (p, m_+m_-) = 1\}$$
$$P_- = \{p : \chi_p(m_-) = 1, \ (p, m_+m_-) = 1\},$$

where $m_+ = tr\,A + 2n$ and $m_- = tr\,A - 2n$. If neither m_+ nor m_- is a square of an integer, it follows from Theorem 2 that P_+ and P_- have density $1/2$. On the other hand, the union $P_+ \cup P_-$ has density 1 since either $\chi_p(m_+) = 1$ or $\chi_p(m_-) = 1$ for almost all prime numbers p. Therefore the intersection $P_+ \cap P_-$ has density 0. Hence the symmetric difference $P_+ \Delta P_-$ has density 1. But we have

$$\chi_p(m_+m_-) = \chi_p(m_+)\,\chi_p(m_-) = -1$$

for all p in $P_+ \Delta P_-$. Since the density of all prime numbers p with $\chi_p(m_+m_-) = -1$ is 0 or $1/2$, we obtain a contradiction. Hence either m_+ or m_- is a square. Such an integer is denoted by m^2. Then we get

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} (m^2+a-d)/2m & b/m \\ c/m & (m^2-a+d)/2m \end{pmatrix}^2,$$

which implies the necessity.

The following lemmas assert that we can not replace "for almost all prime numbers p" by "for all prime numbers p" and "a rational matrix" by "an integral matrix" in Theorem 2.

Lemma 1. *Let p_0 be any prime number. There exist infinitely many integral matrices which are quadratic residues modulo p for all prime numbers $p \neq p_0$ but not modulo p_0.*

Proof. We consider

$$A = \begin{pmatrix} 1 & p_0 - q \\ p_0 + q & p_0^2 - 2q + 1 \end{pmatrix}.$$

Then

$$tr\,A = p_0^2-2q+2 \text{ and } |A| = (q-1)^2.$$

Putting $n = q-1$, we see

$$|A| = n^2,\ tr\,A+2n = p_0^2,\ \text{and } tr\,A-2n = p_0^2-4q+4.$$

By Corollary 1, A is a quadratic residue modulo p for all prime numbers $p \neq p_0$. Now

$$\chi_{p_0}(tr\,A+2n) = 0 \text{ and } \chi_{p_0}(tr\,A-2n) = \chi_{p_0}(-4q+4),$$

so that integers q with $\chi_{p_0}(-q+1) = -1$ give this lemma if p_0 is odd. If $p_0 = 2$, then A is a quadratic residue modulo 2 or not according as q is even or odd.

Lemma 2. *There exist infintely many matrices which are quadratic residues modulo p for all prime numbers p but not squares of integral matrices.*

Proof. Let A be as in Proof of Lemma 1 and p_0 an odd prime number. Then integers q prime to p_0 which satisfy both $q > (p_0^2+3)/4$ and $\chi_{p_0}(1-q) = 1$ give this lemma. Indeed A is also a quadratic residue modulo p_0. Furthermore assuming that $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}^2$ in $M_2(\mathbf{Z})$, we have

$$x^2+yz = 1 \tag{1}$$
$$(x+w)y = p_0-q \tag{2}$$
$$(x+w)z = p_0+q \tag{3}$$
$$w^2+yz = p_0^2-2q+1. \tag{4}$$

Calculating (2)+(3), (2)−(3) and (1)−(4), we get

$$(x+w)(y+z) = 2p_0,\ (x+w)(y-z) = -2q,$$
$$(x+w)(x-w) = 2q-p_0^2.$$

The greatest common divisor of $2p_0$, $-2q$, $2q-p_0^2$ is 1, so that $x+w = \pm 1$. Therefore

$$y+z = \pm 2p_0,\ y-z = \mp 2q,\ x-w = \pm(2q-p_0^2),$$

which lead to

$$x = \pm(1-p_0^2+2q)/2,\ y = \pm(p_0-q),$$
$$z = \pm(p_0+q),\ w = \pm(1-p_0^2+2q)/2.$$

Substituting these into (1), we obtain

$$(p_0^2-1)(p_0^2-4q+3) = 0.$$

This contradicts to our assumption on p_0 and q.

Summing up Theorem 3 and Lemmas 1 and 2, we obtain

Theorem 4. *Let $M_2(\mathbf{Z})^2$ and $M_2(\mathbf{Q})^2$ be the sets of all squares of integral matrices and of rational matrices respectively. Let $M_2(\mathbf{Z})_p^2$ be the set of all quadratic residues modulo a prime number p. Then the following relation of inclusion holds* ;

$$M_2(\mathbf{Z})^2 \subsetneqq \bigcap_p M_2(\mathbf{Z})_p^2 \subsetneqq M_2(\mathbf{Q})^2 \cap M_2(\mathbf{Z}) \subsetneqq M_2(\mathbf{Z}),$$

where p runs over all prime numbers.

Applying Theorem 3 to Proof of Corollary 2, we obtain

Theorem 5. *A 2×2 integral matrix is represented as a product of two squares of rational matrices if and only if its determinant is a square of an integer.*

In the case of modulo 2, the matrices $\begin{pmatrix}0&0\\0&0\end{pmatrix}$, $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, $\begin{pmatrix}0&0\\0&1\end{pmatrix}$, $\begin{pmatrix}1&1\\0&0\end{pmatrix}$, $\begin{pmatrix}1&0\\1&0\end{pmatrix}$, $\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\begin{pmatrix}0&1\\0&1\end{pmatrix}$, $\begin{pmatrix}0&0\\1&1\end{pmatrix}$, $\begin{pmatrix}1&1\\1&0\end{pmatrix}$, $\begin{pmatrix}0&1\\1&1\end{pmatrix}$ form a representation system of the quadratic residue classes. These generate a multiplicative semi-group of order 13 in $M_2(\mathbf{Z})/2M_2(\mathbf{Z})$. The semi-group contains classes of $\begin{pmatrix}0&1\\0&0\end{pmatrix}$, $\begin{pmatrix}0&0\\1&0\end{pmatrix}$, $\begin{pmatrix}1&1\\1&1\end{pmatrix}$ but not of $\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $\begin{pmatrix}1&0\\1&1\end{pmatrix}$, $\begin{pmatrix}0&1\\1&0\end{pmatrix}$. We remark that for every integer n, the matrix $\begin{pmatrix}2n+1&1\\0&2n+1\end{pmatrix}$, whose determinant is equal to a square $(2n+1)^2$, can not be represented as any product of squares of integral matrices.

3. Some analogies of the Lagrange theorem. Let p be an odd prime number. If $p\equiv 1 \pmod 4$ and $p \neq 5$ then every integer modulo p is congruent to a sum of two incongruent squares of integers prime to p, and if $p\equiv 3 \pmod 4$ and $p \neq 3, 7$ then so is every integer prime to p. In the case of $M_2(\mathbf{Z})$, we have

Theorem 6. *Let p be an odd prime ≥ 5. Every 2×2 integral matrix modulo p is congruent to a sum of two incongruent squares of integral matrices whose determinants do not vanish modulo p.*

Proof. We have two identities

$$A^2-(tr\,A)A+|A|E=O$$
$$A^2+2xA+x^2E-(A+xE)^2=O.$$

Their difference yields

$$(2x+tr\,A)A=(A+xE)^2+(|A|-x^2)E. \tag{1}$$

If there exists an integer x such that

$$\chi_p(2x+tr\,A)=1,\quad x^2-|A|\not\equiv 0,\quad \text{and}\quad |A+xE|\not\equiv 0, \tag{2}$$

then putting

$$X=y\begin{pmatrix}0 & |A|-x^2\\ 1 & 0\end{pmatrix},\quad Y=y(A+xE),$$

where $y^2(2x+tr\,A)\equiv 1$, we obtain

(3) $A\equiv X^2+Y^2 \pmod p$, where $|X|$, $|Y|$ are prime to p and $X^2\not\equiv Y^2$. We note that $X^2\equiv Y^2$ if and only if $(A+xE)^2\equiv(|A|-x^2)E$ if and only if A is congruent to a scalar matrix. Let $m(p)$ be the number of $x \pmod p$ such that $x^2\equiv|A|$ or $|A+xE|\equiv 0$ and let $n(p)$ be the number of $x \pmod p$ such that $\chi_p(2x+tr\,A)=1$. If $p\geq 11$, then $m(p)\leq 4$ and $n(p)=(p-1)/2\geq 5$, so that $m(p)<n(p)$. Therefore there exists x satisfying (2). In the case of $p=7$: If $A \pmod 7$ satisfies one of the following properties ; (i) $\chi_7(|A|)=0$ or -1, (ii) the eigenvalues do not belong to $\mathbf{Z}/7\mathbf{Z}$, (iii) the eigenvalues are equal to each other, then $m(7)\leq 2$ and $n(7)=3$. Thus the rest is similar. Otherwise the eigenvalues of $A \pmod 7$ are given by $a \pmod 7$, $b \pmod 7$ such that $a\not\equiv b \pmod 7$ and $\chi_7(ab)=1$. Here if A is not a quadratic residue, then $A\equiv 3A+5A$ gives (3). If A is a quadratic residue, say $A\equiv B^2$, then one of $A\equiv\left(2B+\begin{pmatrix}0&0\\ i&0\end{pmatrix}\right)^2+\left(2B-\begin{pmatrix}0&0\\ i&0\end{pmatrix}\right)^2$ for $i=1, 2, 3$ gives (3). In the case of $p=5$: If $|A+E|\not\equiv 0$, $|A-E|\not\equiv 0$ and $A^2+E\not\equiv O$ then we can take $X=A-E$, $Y=2(A+E)$ in (3). If $|A-E|\equiv 0$ then the eigenvalues of $A \pmod 5$ belong to $\mathbf{Z}/5\mathbf{Z}$ and one

eigenvalue is congruent to 1. If the other is congruent to 1, 2, or 3, then we can take $x \equiv 2$, 4, or 1 in (2) respectively. If the other is congruent to 4 then $A \equiv 2A+4A$ gives (3), and if the other is congruent to 0 then $A \equiv (A+3B)^2+(B+E)^2$, where $(2E+A)B \equiv 4E$, gives (3). If $|A+E| \equiv 0$, then $|(-A)-E| \equiv 0$, and so $-A \equiv X^2+Y^2$, that is, $A \equiv (2X)^2+(2Y)^2$. If $A^2+E \equiv O$ then $3A$ is a quadratic residue, say $3A \equiv B^2$, and so one of $A \equiv \left(B+\begin{pmatrix}0 & 0\\ i & 0\end{pmatrix}\right)^2+\left(B-\begin{pmatrix}0 & 0\\ i & 0\end{pmatrix}\right)^2$ for $i = 1, 2$ gives (3).

In the case of $p = 3$, (3) holds if and only if A is not congruent to any one of E, $\pm\begin{pmatrix}0 & 2\\ 1 & 0\end{pmatrix}$, $\pm\begin{pmatrix}1 & 1\\ 1 & 2\end{pmatrix}$, $\pm\begin{pmatrix}1 & 2\\ 2 & 2\end{pmatrix}$. But they are congruent to twice squares with determinants prime to 3. In the case of $p = 2$, every integral matrix is congruent to a sum of two squares of integral matrices. But an integral matrix is congruent to a sum of squares with odd determinants if and only if it is congruent to O, E, $\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$, $\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$. In parallel with Proof of Theorem 6 in the case of $p \geq 11$, we can prove

Theorem 7. *Every 2×2 integral matrix is represented as a sum of two distinct squares of rational regular matrices.*

We shall see from Theorem 9 that "rational matrices" can not be replaced by "integral matrices" in Theorem 7 even if the restriction "distinct and regular" is removed. Also, see [3] and [5]. By(1) in Proof of Theorem 4, we get

Lemma 3. $A = (A-mE)^2+\begin{pmatrix}0 & |A|-m^2\\ 1 & 0\end{pmatrix}^2$, *where* $m = (tr\,A-1)/2$.

Lemma 4. *If* $A = B^2+C^2$ *then* $2A = (B+C)^2+(B-C)^2$.

Lemma 5. *If* $A \equiv O \pmod 4$ *then* $A = B^2+C^2$ *for some* $B, C \in M_2(\mathbf{Z})$.

Proof. Put $A' = \frac{1}{4}A$, then A' belongs to $M_2(\mathbf{Z})$. By Lemma 3, we get

$$A = (2A'-mE)^2+\begin{pmatrix}0 & 4\\ 1 & 0\end{pmatrix}^2 \begin{pmatrix}|A'|-m^2\\ \end{pmatrix},$$

where $m = tr\,A'-1$.

Theorem 8. *Every* 2×2 *integral matrix is represented as a sum of three distinct squares of integral matrices.*

Proof. The case of $tr\,A \equiv 1 \pmod 2$ is obvious from Lemma 3. If $tr\,A \equiv 0 \pmod 2$ then $tr(A-X^2) \equiv 1 \pmod 2$, where $X = \begin{pmatrix} 2l+1 & 0 \\ 0 & 0 \end{pmatrix}$. By applying Lemma 3 to $A-X^2$, we get $A-X^2 = Y^2+Z^2$ for some Y, Z in $M_2(\mathbf{Z})$, that is, $A = X^2+Y^2+Z^2$.

Theorem 9. *An* 2×2 *integral matrix* A *is represented as a sum of two squares of integral matrices if and only if* A *is not congruent modulo* 4 *to any one of*

$$\begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}.$$

Proof. We divide the proof into nine cases.

(i) $tr\,A \equiv 1 \pmod 2$. Then it is obvious from Lemma 3.

(ii) $tr\,A \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & (b+1)/2 \\ e & 0 \end{pmatrix}^2 + \begin{pmatrix} (a-d)/2 & (b-1)/2 \\ c-e & 1-(a-d)/2 \end{pmatrix}^2$$

where $e = a-1-(a-d)^2/4-(b-1)c/2$.

(iii) $tr\,A \equiv 0 \pmod 2$ and $c \equiv 1 \pmod 2$. Then the transposed matrix ${}^tA$ satisfies (ii).

(iv) $tr\,A \equiv 2 \pmod 4$ and $a \equiv b \equiv c \equiv d \equiv 0 \pmod 2$. Then $A' = \frac{1}{2}A$ belongs to $M_2(\mathbf{Z})$ and satisfies (i). Therefore this case follows from Lemma 4.

(v) $tr\,A \equiv 2 \pmod 4$, $a \equiv d \equiv 1 \pmod 2$ and $b \equiv c \equiv 0 \pmod 2$. Then

$$\begin{pmatrix} a & d \\ c & d \end{pmatrix} = \begin{pmatrix} 1+(a-d)/2 & -1+b/2 \\ e & -(a-d)/2 \end{pmatrix}^2 + \begin{pmatrix} 0 & 1+b/2 \\ c-e & 1 \end{pmatrix}^2,$$

where $e = (a-d)^2/8-(d-1)/2+bc/4+c/2$.

(vi) $tr\,A \equiv 0 \pmod 4$ and $a \equiv b \equiv c \equiv d \equiv 0 \pmod 4$. This case follows from Lemma 5.

(vii) $tr\,A \equiv 0 \pmod 4$, $a \equiv c \equiv d \equiv 0 \pmod 4$, and $b \equiv 2 \pmod 4$. Then $A' = \frac{1}{2}A$ belongs to $M_2(\mathbf{Z})$ and satisfies (ii). Therefore this case follows from Lemma 4.

(viii) $trA \equiv 0 \pmod 4$, $a \equiv b \equiv d \equiv 0 \pmod 4$, and $c \equiv 2 \pmod 4$. Then ${}^tA$ satisfies (vii).

(ix) The remainder case that $trA \equiv 0 \pmod 4$, $a \equiv d \equiv 1 \pmod 2$, and $b \equiv c \equiv 0 \pmod 2$ is equivalent to $(a, b, c, d) \equiv (1,0,0,3)$, $(1,0,2,3)$, $(1,2,0,3)$, $(1,2,2,3)$, $(3,0,0,1)$, $(3,0,2,1)$, $(3,2,0,1)$, or $(3,2,2,1) \pmod 4$. We assume now that for some x_i, x_j in $\mathbf{Z}$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}^2 + \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}^2.$$

Since $x_1^2 + y_1^2 - x_4^2 - y_4^2 = a - d \equiv 2 \pmod 4$, we must have either $x_1 \equiv y_1 \equiv 1$, $x_4 \equiv y_4 \equiv 0 \pmod 2$ or $x_1 \equiv y_1 \equiv 0$, $x_4 \equiv y_4 \equiv 1 \pmod 2$, so that $x_1 + x_4 \equiv y_1 + y_4 \equiv 1 \pmod 2$. Therefore it holds from $b \equiv c \equiv 0 \pmod 2$ that $x_2 \equiv y_2$, $x_3 \equiv y_3 \pmod 2$. We obtain a contradiction

$$1 \equiv a = x_1^2 + y_1^2 + x_2x_3 + y_2y_3 \equiv 0 \pmod 2.$$

The proof is completed.

We see from Theorem 9 that the "three" in Theorem 8 is the best possible value.

Every positive integer greater than 169 is represented as a sum of five squares of non-zero integers. Analogously we have

Theorem 10. *Every 2×2 integral matrix is represented as a sum of four distinct squares of integral regular matrices.*

Proof. Suppose now that $trA \equiv 1 \pmod 2$. Put $m = (trA - 1)/2$ and $n = |A| - m^2$. These are integers. If $|A - mE| \neq 0$ and $n \neq 0$ then by Lemma 3, we obtain partitions of A into squares of integral regular matrices,

$$\begin{aligned} A &= (A - mE)^2 + \begin{pmatrix} 0 & n \\ 1 & 0 \end{pmatrix}^2 \\ &= (A - mE)^2 + \begin{pmatrix} 0 & 2n \\ 1 & 0 \end{pmatrix}^2 + \begin{pmatrix} 0 & -n \\ 1 & 0 \end{pmatrix}^2 \\ &= (A - mE)^2 + \begin{pmatrix} 0 & n \\ 1 & 0 \end{pmatrix}^2 + \begin{pmatrix} 0 & l \\ 1 & 0 \end{pmatrix}^2 + \begin{pmatrix} 0 & -l \\ 1 & 0 \end{pmatrix}^2. \end{aligned}$$

If $|A - mE| = 0$ and the $(1,2)$-entry of A denoted by b is not 0, we set $B = A - \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}^2$, where k is a fixed integer such that $k \neq (trA - 1)/2b$. Put

$m' = (tr\,B-1)/2$ and $n' = |B| - m'^2$. These are integers as $tr\,B = tr\,A - 2 \equiv 1 \pmod 2$. Applying Lemma 3 to B, we obtain partitions of A into squares of integral regular matrices,

$$\begin{aligned} A &= B+\begin{pmatrix}1 & 0\\ k & 1\end{pmatrix}^2 \\ &= (B-m'E)^2+\begin{pmatrix}0 & n'\\ 1 & 0\end{pmatrix}^2+\begin{pmatrix}1 & 0\\ k & 1\end{pmatrix}^2 \\ &= (B-m'E)^2+\begin{pmatrix}0 & 2n'\\ 1 & 0\end{pmatrix}^2+\begin{pmatrix}0 & -n'\\ 1 & 0\end{pmatrix}^2+\begin{pmatrix}1 & 0\\ k & 1\end{pmatrix}^2, \end{aligned}$$

because $|B-m'E| = -2b \neq 0$ and $n' = 2bk - tr\,A+1 \neq 0$. If the $(2,1)$-entry is not 0, then applying the above consideration to the transposed matrix ${}^tA$ we get a similar result. If both the $(1,2)$-entry and the $(2,1)$-entry are 0, then $A = \begin{pmatrix}a & 0\\ 0 & a+1\end{pmatrix}$ or $\begin{pmatrix}a & 0\\ 0 & a-1\end{pmatrix}$ for some integer a. Then we have

$$\begin{aligned} \begin{pmatrix}a & 0\\ 0 & a+1\end{pmatrix} &= \begin{pmatrix}0 & a-17\\ 1 & 0\end{pmatrix}^2+\begin{pmatrix}4 & 0\\ 0 & 3\end{pmatrix}^2+\begin{pmatrix}1 & 0\\ 0 & 3\end{pmatrix}^2 \\ &= \begin{pmatrix}0 & a-18\\ 1 & 0\end{pmatrix}^2+\begin{pmatrix}4 & 0\\ 0 & 3\end{pmatrix}^2+\begin{pmatrix}1 & 0\\ 0 & 3\end{pmatrix}^2+\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}^2 \\ &= \begin{pmatrix}0 & a-25\\ 1 & 0\end{pmatrix}^2+\begin{pmatrix}3 & 0\\ 0 & 1\end{pmatrix}^2+\begin{pmatrix}4 & 0\\ 0 & 5\end{pmatrix}^2 \\ &= \begin{pmatrix}0 & a-26\\ 1 & 0\end{pmatrix}^2+\begin{pmatrix}3 & 0\\ 0 & 1\end{pmatrix}^2+\begin{pmatrix}4 & 0\\ 0 & 5\end{pmatrix}^2+\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}^2. \end{aligned}$$

Substituting $a-1$ for a and exchanging the $(1,1)$-entry and the $(2,2)$-entry in the above equality, we obtain similar partitions of $\begin{pmatrix}a & 0\\ 0 & a-1\end{pmatrix}$.

Therefore if $tr\,A \equiv 1 \pmod 2$, then A can be represented as sums of three and also four distinct squares of integral regular matrices.

If $tr\,A \equiv 0 \pmod 2$, then $A-\begin{pmatrix}2l & 0\\ 0 & 2l+1\end{pmatrix}^2$ has an odd trace, so that the matrix is represented as a sum of three squares, that is, A is represented as a sum of four distinct squares of integral regular matrices.

The proof is completed.

References

[1] L. Carlitz: Solution to Problem 140 (proposed by I. Connel), Canad. Math. Bull. 11 (1968), 615–619.

[2] T. FUNAKURA, N. MORIMOTO, N. TOYOIZUMI, and N. KAMIYA: On some properties of 2×2 integral matrices, Bull. Okayama Univ. of Sci. 15 (1979), 9−14.
[3] M. GRIFFIN and M. KRUSEMEYER: Matrices as sums of squares, Linear and Multilinear Algebra 5 (1977), 33−44.
[4] M. NEWMANN: Sums of squares of matrices, Pacific J. Math. 118 (1985), 497−506.
[5] D. R. RICHMAN: Matrices as sums of squares: A cojecture of Griffin and Krusemeyer, Linear and Multilinear Algebra 17 (1985), 289−294.
[6] A. ROSENFELD: A note on matrix quadratic residues, Amer. Math. Monthly 74 (1967), 804−810.
[7] J.-P. SERRE: A Course in Arithmetic, Springer-Verlag, New York-Heidelberg-Berlin, 1973.
[8] W. J. LEVEQUE: Fundamentals of Number Theory, Addison-Wesley, Massachusetts, 1977.

DEPARTMENT OF GENERAL EDUCATION
OKAYAMA UNIVERSITY OF SCIENCE
1-1 RIDAI-CHO, OKAYAMA 700, JAPAN
and
TOSA WOMEN'S HIGH SCHOOL
3-1 OUTESUJI 2-CHOME, KOCHI 780, JAPAN

(*Received July 20, 1985*)

SOME ARITHMETICAL PROPERTIES ON 2×2 INTEGRAL MATRICES

(This Journal, Vol. 27, pp. 135－146)

TAKEO FUNAKURA and NOBUAKI MORIMOTO

Page 136, line 12. For "$p^2+\chi_\rho(2trA)p+\chi_\rho(2trA)+\chi_2(p)$",
read "$p^2+\chi_\rho(2trA)p$".