EasyChair Preprint

№ 11692

2 x 2 Integer Matrices: Composition of Binary Quadratic Forms

Rama Garimella

January 5, 2024

2 x 2 INTEGER MATRICES: COMPOSITION OF BINARY QUADRATIC FORMS

Garimella Rama Murthy,
Professor, Mahindra University,
Hyderabad, INDIA

ABSTRACT

In this research paper, we consider 2 x 2 integer matrices and identify interesting binary quadratic forms which naturally arise. Specifically, we consider such symmetric integer matrices and derive compositions of pure binary quadratic forms naturally arising in association with determinant of such matrices. We also, discover number-theoretic results associated with trinary quadratic forms naturally arising in connection with 2 x 2 symmetric integer matrices. We formulate a "generalized Waring problem" using real quadratic algebraic numbers. We also discuss composition of binary quadratic forms naturally arising in other interesting structured 2 x 2 integer matrices. We explore representation of integers using trinary as well as binary quadratic forms.

1. INTRODUCTION:

Ever since the dawn of civilization, integers stimulated the curiosity of several mathematicians. Algebraic symbolism helped defining negative numbers based on the concept of "ZERO". Also, linear algebraic equation in one variable with integer coefficients enabled the introduction of rational numbers. Similarly, quadratic equations naturally led to the proposal of novel class of numbers, called "complex numbers".

Diophantus considered linear algebraic equations in two variables that are constrained to be integers. The so called simplest linear Diophantine equation is of the form

$$a\,x + b\,y = c$$

was solved using the Greatest Common Divisor (GCD of the integers { a, b }) algorithm. The book "Arithmetica" by Diophantus and some volumes of Euclid's elements contained interesting results related to integers and specifically prime numbers, perfect numbers (among other number-theoretic results). Fermat acquired a copy of Arithmetica and contributed several interesting number-theoretic theorems that survived passage of time. For instance, Fermat proved that a prime number of the form { 4 l + 1, l=1,2,… } (i.e. $p \equiv 1\,(mod)\,4$) can be expressed uniquely as the sum of squares of two integers. Further, a prime of the form { 4 l + 3, l=1,2,…….. } (i.e. $p \equiv 1\,(mod)\,4$) can never be expressed as the sum of squares of two integers. This result was combined with the following algebraic identity

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 - x_2y_2)^2 + (x_1y_2 + x_2y_1)^2$$
$$= (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$$

resulting in the so called GENUS theorem in algebraic number theory.

The author in his research efforts became interested in 2 x 2 integer matrices. Several interesting results were documented in the technical report [3]. The results reported in this research paper deal with number-theoretic concepts/ideas applied to 2 x 2 integer matrices.

This research paper is organized as follows. In Section 2, composition of binary quadratic forms arising in the case of 2 x 2 symmetric integer matrices are discussed. In Section 3, trinary quadratic forms naturally arising in association with symmetric 2x 2 integer matrices are identified and interesting results are derived. In Section 4, composition of binary quadratic forms naturally arising in association with certain structured quadratic forms arising in structured 2 x 2 matrices is discussed. The research paper concludes in Section 5.

2. 2 x 2 Symmetric Integer Matrices: Sums of Squares of Two Integers: Compositions:

Consider a symmetric 2 x 2 integer matrix of the form $X = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$ $where\ \{\ a,b,c\ \}\ are\ integers$. It readily follows that $X^2 = \begin{bmatrix} a^2+b^2 & b(a+c) \\ b(a+c) & b^2+c^2 \end{bmatrix}$. Thus, we have

$Det(X^2)$ = (Det(X))^2 = $(a^2+b^2)(b^2+c^2) - b^2(a+c)^2$.
Using the fact that Trace (X) = a + c , we have that

(Det(X))^2 = $(a^2+b^2)(b^2+c^2) - b^2(\ Trace(X)\ )^2$.

Hence,
(Det (X))^2 + (b ($Trace(X)$))^2 = $(a^2+b^2)(b^2+c^2)$.
Using the standard identity on product of sum of squares of two integers, we have thata

$$(a^2+b^2)(b^2+c^2) = (\ ab+bc\ )^2 + (\ ac-b^2)^2 = (\ ab-bc\ )^2 + (\ ac+b^2)^2.$$

Thus, genus theorem from algebraic number theory readily applies. Let X_1, X_2 be two symmetric integer matrices with elements $\{\ a_1,b_1,c_1\ \}$; $\{\ a_2,b_2,c_2\ \}$ respectively. Using the above discussion, we have that

$$(Det(X_1))^2 + (\ b_1(Trace(X_1))^2 = \ (a_1^2+b_1^2)(b_1^2+c_1^2)$$
$$(Det(X_2))^2 + (\ b_2(Trace(X_2))^2 = \ (a_2^2+b_2^2)(b_2^2+c_2^2)$$

Since the LHS as well as RHS of the above two expressions are binary quadratic Forms, genus theorem can be readily invoked. The binary quadratic form associated with the symmetric matrix, X is based on the quantity

(Det (X))^2 + (b ($Trace(X)$))^2 = $(\ \mu_1\mu_2)^2 + b^2(\mu_1+\mu_2)^2$, where

$\mu_1, \mu_2\ are\ eigenvalues\ of\ X.$

3. 2 x 2 Symmetric Integer Matrices: Sum of Squares of 3 integers (Trinary Quadratic Form): Equivalence of Trinary and Binary Quadratic Forms:

We now consider another interesting quantity associated with a 2 x 2 symmetric integer matrix: $X = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$. We readily have that

$$X^2 = \begin{bmatrix} a^2 + b^2 & b(a+c) \\ b(a+c) & b^2 + c^2 \end{bmatrix}.$$

$Thus,\ Trace(X^2) = \ a^2 + 2\,b^2 + c^2 = \ \mu_1^2 + \mu_2^2$, where

μ_1, μ_2 *are eigenvalues of* X, *which are in general quadratic algebraic numbers.*

Note: We thus have a trinary quadratic form in integers equal to the binary quadratic form in eigenvalues of symmetric 2 x 2 integer matrix. Since X is symmetric, its eigenvalues are real numbers. We now determine the nature of eigenvalues under some conditions on the integers a, b, c.

CASE I : Eigenvalues are rational numbers/integers:

$\mu_1 + \mu_2 = \ a + c$ and $\mu_1 \mu_2 \ = \ ac - b^2$.

Also, $(\mu_1 - \mu_2)^2 = (a-c)^2 + \ (2\,b\,)^2 = \Delta^2$

Hence, we have that $\mu_1,\ \mu_2 \ = \ \frac{(a+c) \mp \sqrt{(a-c)^2 + \ (2\,b\,)^2}}{2}$.

Thus, if { (a-c), (2b), Δ } form a Pythagorean triple, the eigenvalues of X are rational Numbers i.e. $\mu_1,\ \mu_2 \ = \ \frac{(a+c) \mp \ \Delta}{2}$. If { (a+c), Δ } are even integers, then the both the eigenvalues are integers.

Note: { (a+c), (a-c) } are both even/odd integers. Hence, if { a, c } are both even/odd, the eigenvalues will be integers.

CASE (ii): $(a-c)^2 + \ (2\,b\,)^2$ = p, a prime number.

By Fermat's Theorem, $p \equiv 1(mod)\ 4$.

For any given p, (a-c)= k is unique by Fermat's Theorem.

In such case, a+c = k + 2 c. Thus, $\mu_1,\ \mu_2 \ = \ \frac{(k+2c) \mp \sqrt{p}}{2}$.

Hence, in this case, $\mu_1,\ \mu_2$ are real algebraic numbers.

Note: A related case is the one, where$(a-c)^2 + \ (2\,b\,)^2 = q$, an integer which is not a perfect square (even or odd number). Even in this case the eigenvalues are

algebraic numbers.

- INTERESTING TRINARY QUADRATIC FORM:
  We now focus on the following equation from the above discussion:

$$, \quad Trace(X^2) = a^2 + 2\,b^2 + c^2 = \mu_1^2 + \mu_2^2$$

We reduce the above equality of trinary and binary quadratic forms (with $\mu_1,\ \mu_2$ being real algebraic numbers) to the case of equality between two binary quadratic forms under some conditions:

(I) { a, c, d } form a Pythagorean triple

$$Trace(X^2) = a^2 + 2\,b^2 + c^2 = d^2 + 2\,b^2 = \mu_1^2 + \mu_2^2.$$

If the eigenvalues $\{\ \mu_1,\ \mu_2\ \}$ are integers, then the genus Theorem associated

With binary quadratic forms can be invoked. Also, letting X_1, X_2 be two such 2 x 2

Symmetric integer matrices, we have

$$Tr(X_1^2) = d_1^2 + 2b_1^2 \ ; \ Tr(X_2^2) = d_2^2 + 2b_2^2\ .$$

We can readily invoke Brahmagupta's identity for the composition of such

quadratic forms

- Bramhagupta's Identity:
  For a given n, the product of two numbers of the form $a^2 + nb^2$ is itself a number of that form i.e.

$$(a^2 + nb^2)(c^2 + nd^2) = (ac - nbd)^2 + n(ad + bc)^2$$
$$= (ac + nbd)^2 + n(ad - bc)^2$$

The identity holds in any commutative ring.

We now invoke the Brahmagupta's identity:

$$Tr(X_1^2)\ Tr(X_2^2) = (\ d_1^2 + 2b_1^2\ )(d_2^2 + 2b_2^2\ ) = (d_1d_2 - 2b_1b_2)^2 + 2\,(d_1b_2 + d_2b_1)^2$$
$$= (d_1d_2 + 2b_1b_2)^2 + 2\,(d_1b_2 - d_2b_1)^2$$

Note: The other interesting cases which lead to composition of binary quadratic forms are

$$a^2 + 2b^2 = e^2 \ \ or \ \ c^2 + 2b^2 = f^2, \ \ for \ \ suitable \ \ integers \ \{\ e, f\ \}.$$

- From linear algebra, we readily have that

$$Tr(X^{2m}) = \mu_1^{2m} + \mu_2^{2m} \ \ for \ \ m \geq 1.$$

As in the case of m=1, the above expression reduces to interesting polynomial in { a, b, c }

Now, we consider representation of a prime number, p using the specific trinary quadratic form considered above.

$$Trace(X^2) = \ a^2 + 2\,b^2 + c^2 = p = \mu_1^2 + \mu_2^2.$$

We provide some examples which illustrate the fact that $p \equiv 1(mod)4 \ or \ \ p \equiv 3\,(mod)4$. It readily follows (from Fermat's Theorem) that, if $Trace(X^2) = q, \ a \ prime \ with \ q \equiv 3\,(mod)\,4$, then, $\{\ \mu_1, \mu_2\ \}\ are\ real\ quadratic\ algebraic\ numbers$ ($quadratic\ surds$) $and\ not\ integers.$

Example 1: $\bar{X} = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix}$. We have that $Trace(X^2) = 13 \equiv 1\ (mod)\ 4.\ Also$

$$Trace(X) = \mu_1 + \ \mu_2 \ = 3 \ \ and \ \ determinant\ (\ X\ ) = \mu_1\mu_2 \ = -2.$$

$$\mu_1 = \frac{3 + \sqrt{17}}{2}, \qquad \mu_2 = \frac{3 - \sqrt{17}}{2}$$

i.e. eigenvalues are quadratic surds

Example 2: $\bar{X} = \begin{bmatrix} 1 & 3 \\ 3 & 2 \end{bmatrix}$. We have that $Trace(X^2) = 23 \equiv 3(mod)\ 4.\ Also$

$$Trace(X) = \mu_1 + \ \mu_2 \ = 3 \ \ and \ \ determinant\ (\ X\ ) = \mu_1\mu_2 \ = -7.$$

$$\mu_1 = \frac{3 + \sqrt{37}}{2}, \qquad \mu_2 = \frac{3 - \sqrt{37}}{2}$$

Note: In both the examples, the eigenvalues are NOT integers.

- Suppose the 2 x 2 symmetric integer matrix, $\bar{X}$ is singular (i.e. $b^2 = ac$). In this case, we have that Det($\bar{X}$) $= \ \mu_1\mu_2\ 0.$ $Furthermore,$
  $Trace(X^2) = \ a^2 + 2\,b^2 + c^2 = \mu^2.$
  $Note$: We can call such 4 integers { a,b,c, μ | as Pythagorean Quadruples.

Note: If $Trace(\ \bar{X}^2\ ) = p, a\ prime\ number$, then $\bar{X}$ cannot be singular.

The following Theorem deals with { $Trace(\ \bar{X}^s\ )\ for\ s\ \geq 2$ }.

THEOREM: Let $\bar{X} = \begin{bmatrix} a & b \\ b & c \end{bmatrix}$ be a 2 x 2 symmetric integer non-singular matrix (i.e. $b^2 \neq ac$) and let { a, c } are both even or both are odd. Also, let { (a-c), 2 b, K } form a Pythagorean triple i.e. $(a-c)^2 + \ (\ 2\ b\ )^2 = k^2$. Let $Trace(\ \bar{X}^s\ ) \ = \ f_s(\ a, b, c\ )\ be\ a\ trivariate\ polynomial\ in\ \{\ a, b, c\ \}.$

Under these conditions,

(i) we have that $Trace(\ \bar{X}^s\ ) \neq \mu^s\ \ for\ any\ integer\ s\ \geq 2.$
(ii) Also, $Det\ (\ \bar{X}^s\ ) = \beta^s \ = \ (\ Det(\bar{X}\ )^s = \ (\ ac - b^2)$ for all s.
(iii) If $\bar{X}$ is singular, then $Trace(\ \bar{X}^s\ ) = \ \delta^s\ for\ all\ s$
$(\ where\ \delta\ is\ the\ non-zero\ eigenvalue\ of\ \bar{X}.$

PROOF: From the conditions in the statement of theorem (based on earlier discussion) that the eigenvalues of $\bar{X}\ are\ \ integers\ and\ \ Trace(\bar{X}^s) = \ \mu_1^s + \mu_2^s\ \ for\ all\ \ s \geq 1.$

From Fermat's Last Number Theorem, we have that

$$Trace(\ \bar{X}^s\ ) \neq \mu^s\ \ for\ any\ integer\ s\ \geq 3.$$

Now, let us consider the case of s=2. It readily follows that (for $\bar{X}$ non-singular)

$$\mu_1^2 + \mu_2^2 \; = \; \frac{(a+c)^2 + k^2}{2}.$$

The RHS in the above equation cannot be an even or odd integer (based on properties of even/odd integers). Thus, the result in (i) follows.

The claims in (ii), (iii) follow from basic linear algebra results Q. E. D.

Note: $f_2(a,b,c) \; = \; a^2 + 2\,b^2 + c^2$, $f_3(a,b,c) = \; a^3 + \; 3\,a\,b^2 + 3b^2c + c^3$ and

$$f_4(a,b,c) = \; (a^2 + b^2)^2 + 2\,(b\,(a+c))^2 + (c^2 + b^2)^2$$

In view of the above results, we formulate an interesting generalization of Waring problem.

GENERALIZED WARING PROBLEM:

- In the simplest case, determine the number of ways in which an integer, f (from natural numbers) can be expressed as sum of squares of two real quadratic algebraic numbers, μ_1, μ_2 (quadratic surds) i.e

$$\mu_1^2 + \mu_2^2 = f\,.$$

More generally, we are interested in number of representations of the following form:,

$$\mu_1^2 + \mu_2^2 + \cdots . + \mu_M^2 = f\,.$$

with μ_i'*s being quadratic algebraic numbers*.

In the spirit of above generalization, we can consider weighted sum of squares. Most generally, we consider number of representations of an integer as a general multi-variate polynomial (could be homogeneous) in quadratic algebraic numbers. Generalizations in the spirit of Hilbert's 10th problem are possible (with the variables being quadratic surds instead of integers from the natural numbers).

4. **Structured 2 x 2 Integer Matrices: Composition of Binary Quadratic Forms:**

We now consider structured 2 x 2 integer matrices. First we consider a 2 x 2 integer matrix, X of the following form:

$$\bar{X} = \begin{bmatrix} a & -\alpha\, b \\ b & a \end{bmatrix}\,, \qquad where\ \alpha\ is\ an\ integer.$$

Such class of matrices reduce to the 2 x 2 matrices representing complex numbers when $\alpha = 1$.

It readily follows that the determinant of such a structured matrix is an interesting binary quadratic form:

$$Det(\bar{X}) = \; a + \alpha\, b^2.$$

Given two such integer matrices $\{\bar{X}_1, \bar{X}_2\}$, it readily follows that

$$Det(\bar{X}_1\bar{X}_2) = Det(\bar{X}_1)\,Det(\bar{X}_2).$$

Thus, the RHS in the above equation can be expressed as the interesting binary quadratic form using the Bramhagupta's identity. Details are avoided for brevity.

Now, we consider a structured 2 x 2 integer matrix of the following form:

$\bar{X} = \begin{bmatrix} a & b \\ b & -a \end{bmatrix}$. It readily follows that $\bar{X}^2 = \begin{bmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{bmatrix} = (a^2+b^2)\, I$.

It readily follows that compositions of binary quadratic forms can be readily invoked in association with two diagonal matrices $\bar{X}^2, \bar{Y}^2$ (associated with structured matrices $\bar{X}, \bar{Y}$).

Infact several number- theoretic results (such as MATRIX PYTHAGORAM THEOREM, MATRIX GENUS THEOREM) can be readily invoked in association with such structured 2 x 2 integer matrices.

5. CONCLUSIONS:

In this research paper, several interesting results related to composition of binary quadratic forms arising in connection with 2 x 2 integer matrices are explored. It is expected that these results have interesting implications to algebraic number theory based on quadratic surds.

REFERENCES:

[1] G. Andrews," Number Theory," Dover Publications, New York

[2] Harvey Cohn,"Advanced Number Theory," Dover Publications, New York

[3] G. Rama Murthy,"NP Hard Problems: Many Linear Objective Function Optimization Problem: Integer/Rational Matrices," IIIT-Hyderabad Technical report: IIIT/TR/2016/23, MAY 2016