A GENERALIZATION OF GAUSS THEOREM ON QUADRATIC FORMS

Nicolae I. Bratu and Adina N. Cretan
Department of Math. - Craiova University, Romania

ABSTRACT

An original result concerning the extension of Gauss's theorem from the theory of binary quadratic forms over forms with more unknowns was presented by Bratu in 1994.
The result did not appear in world-wide publications and it was not sufficiently exemplified in applications. This is the purpose of the actual paper.
Keywords: Representation of elements; quadratic forms; Gauss's theorem; automorphic transformation; the Pell's equation, Lagrange's Four-Square Theorem.

1. Actual theory

A quadratic form over an arbitrary field K of characteristic not 2 is a homogeneous polynomial having the coefficients in K :

$$f = \sum a_{ij} x_j x_i \ (a_{ij} = a_{ji}) \text{ or}$$
$$f = X' A X \qquad (1)$$

The representation of elements of K implies the solvability of the equation f =0 and the finding of an algorithm for the representation of zero. Theorem Minkowski-Hasse responses to the first condition [1]. The theory solves the case of quadratic forms of rank 2 for the second condition. There is an isomorphism between the set of classes of similar modules and the set of classes of binary quadratic primitive and self equivalent forms. The fundamental notion is the automorphic transformation, defined as the linear transformation of determinant D = 1, which transforms a quadratic form into itself. In the case of rational fields, Gauss stated a remarkable result, which defines the coefficients of the unimodular matrix of the transformation.

Gauss's Theorem For a binary quadratic form: $f(x, y) = ax^2 + bxy + cy^2$, where we suppose $(a,b,c) = 1$, if the linear transform of matrix $G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is automorphic, then:

$$\alpha = \frac{t - bu}{2} \quad ; \quad \beta = -cu$$
$$\gamma = au \quad ; \quad \delta = \frac{t + bu}{2} \qquad (2)$$

where $t, u \in Z$, such that they verify the Pell's diophantic equation:

$$t^2 - du^2 = 4 \qquad (3)$$

and d is the discriminant of the form. The converse of this theorem holds too

The proof of it showed in [2]

Gauss's theorem reduces the quest for solution of the diophantic equation $f(x,y) = m$, to the finding of a solution of the Pell's equation (3).

For the applications, [2], we have defined the minimal integer positive solution different from the ordinary solution ($t = 2$, $u = 0$), as being the ordered pair (x, y), with $x>0$ and $y>0$, for which, for any other solution (x`, y`), we have $x<x`$, or, if $x=x`$, then $y<y`$.

2. A general theorem of the Gauss type

In [4], we showed that we could affirmatively respond to Dickson's problem [3] for the second-degree equations with several unknowns proposing a generating method for rational solutions. The completion concerning the numeric representation is given in [5]. One of the applications of the generalized theorem was discussed in [6]. The result appeared in [4] is developed and exemplified in the present paper.

Let f be a quadratic form of several unknowns, which is easier to be written in the canonical form:

$$f = a_1 x_1^2 + \ldots\ldots + a_i x_i^2 - a_{i+1} x_{i+1}^2 - \ldots\ldots - a_n x_n^2 \qquad [4]$$

where $a_1, a_2 \ldots\ldots a_n \in N$. The determinant will be: $d = (-1)^{n-i} a_1 a_2 \ldots\ldots a_n$ and the algebraic sum of the coefficients will be called "the trace" of the diagonal quadratic form: $S = a_1 + \ldots\ldots + a_i - \ldots\ldots - a_n$

Remark 1. S = 0, if S = 0, a variable change is made, so that we have S =0

General Theorem (*Bratu*) *For any rational quadratic form [4], brought to the canonical form, one can determine an automorphic linear transformation defined by the unimodular matrix below:*

$$B = -\frac{1}{S}\begin{Vmatrix} 2a_1 - S & 2a_2 & .... & 2a_{i+1} & .... & 2a_n \\ 2a_1 & 2a_2 - S & .... & 2a_{i+1} & .... & 2a_n \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 2a_1 & 2a_2 & .... & 2a_{i+1} + S & .... & 2a_n \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 2a_1 & 2a_2 & .... & 2a_{i+1} & .... & 2a_n + S \end{Vmatrix}$$

where a_1 , ,…….$a_n \in N$, the coefficients of the form, and $S \in \mathbf{Z}$ is the trace of the quadratic form. For the binary quadratic form, the matrix B is identical to Gauss's matrix G, built for the rational solution of Pell's equation attached to the form. If the equation f = m, with d positive and m rational, has a solution, then the matrix B generates the set of rational solutions.

Proof. The matrix B comes from the matricial writing of the generating relations of a positive increasing solution for the x variable, from a natural solution (x_1,…..x_n.):

$$\begin{aligned} x_1' &= -x_1 + \frac{2}{S}(a_1 x_1 + \ldots\ldots a_i x_i - a_{i+1} x_{i+1} - \ldots\ldots - a_n x_n) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n' &= -x_n + \frac{2}{S}(a_1 x_1 + \ldots\ldots a_i x_i - a_{i+1} x_{i+1} - \ldots\ldots - a_n x_n) \end{aligned} \qquad (6)$$

Changing the sign in the columns i +1,…..,n of the matrix we write:

$$B = I - \frac{2}{S}A \qquad (7)$$

with $\det B_1 = (-1)^{n-i} \det B$ and $\det^2 B_1 = \det^2 B$ (8)

where I is the unit matrix of n-order, det B is the determinant of the matrix B and A is a degenerate matrix of the form:

$$A=\begin{Vmatrix} a_1 & a_2 & .... & a_n \\ a_1 & a_2 & .... & a_n \\ . & . & . & . \\ . & . & . & . \\ a_1 & a_2 & .... & a_n \end{Vmatrix}$$

In order to show that B is unimodular, we take:

$$B_1^2 = \frac{1}{S^2}(S^2\, I - 4\, S\, I\, A + 4\, A^2)$$

and we get $B_1^2 = I$, i. e. $\det B^2 = 1$

For the second part of the theorem let

$$ax^2 - by^2 = m \qquad (9)$$

be a quadratic equation, with $ab > 0$.

We have:

$$d = 4\, a\, b \qquad \text{and} \qquad S = a - b \qquad (10)$$

The matrix B is written :

$$B = -\frac{1}{S}\begin{Vmatrix} 2a - S & 2b \\ 2a & 2b + S \end{Vmatrix} \qquad (11)$$

and

$$B = \frac{1}{b - a}\begin{Vmatrix} a + b & 2b \\ 2a & a + b \end{Vmatrix} \qquad (11`)$$

with $\det^2 B = 1$

A rational solution of Pell's equation is:

$$t_o = 2\frac{a + b}{b - a} \qquad \text{and} \qquad u = \frac{2}{b - a}$$

Gauss's matrix built from this solution:

$$G = \frac{1}{b-a}\begin{Vmatrix} a+b & 2b \\ 2a & a+b \end{Vmatrix} \qquad (12)$$

We get: $G \equiv B$ q.e.d. (12`)

Remark 2. In applications, for the generating of another natural solution {x'} from one that is given {x}, it is necessary and sufficient that the term:

$$t = -\frac{2}{S}\,(\,a_1 x_1 + \ldots\ldots\ldots - a_n x_n\,) \qquad (13)$$

has at least an integer value among the $2^{\underline{n-1}}$ possible values. A sufficient condition is that S, the trace of the quadratic form, to have the values ± 1 or ± 2

If not, we use a power matrix B, which is still unimodular. It is necessary an extension of the previous definition of the minimal solution.

Definition 1**.** For the equation attached to the n-degree quadratic form, we call minimal positive solution the ordered $(x_1, \ldots x_n)$ which is a solution of the equation in which all variables are integers and nonnegative and at least one is not null and verifies:

for any other ordered $\{x_i^{'}\}$, rational integer nonnegative solution,

we have $x_1 < x_1^{'}$, if $x_1 = x_1^{'}$, then $x_2 < x_2^{'}$, ……and if $x_{n-2} = x_{n-2}^{'}$, then $x_{n-1} < x_{n-1}^{'}$.

Consequence. The multitude of the integer solutions of the equation (1) can be represented by the nodes of a lattice. The automorphic transformation of matrix B generates the multitude of solutions:

$$X_{i+1} = X_i * B \qquad (14)$$

The signs for the integers x_i are choose so that integer solutions can be obtained x_{i+1} .

3. Examples

3. 1 The equation $x^2 - 2y^2 = 7$

In the literature, the equation is an example for the solving method of binary equations with positive determinant, by the actual method; we have Pell's equation:

$$t^2 - 8u^2 = 4 \qquad \text{and Gauss's matrix} \qquad G = \begin{Vmatrix} 3 & 4 \\ 2 & 3 \end{Vmatrix}$$

We consider the couples (3, 1) and (5, 3) as the minimal positive solutions and by recurrent formulas:

$$x_{i+1} = 3x_i + 4y_i$$
$$y_{i+1} = 2x_i + 3y_i$$

we get two infinities of natural solutions.

By the proposed method, we apply the transformation defined by B matrix, where S = - 1:

$$B = \begin{Vmatrix} 3 & 4 \\ 2 & 3 \end{Vmatrix} = G$$

According to definition 1, the minimal positive solution is unique, namely (3,1). The graphic representation of the solution set is a chain, the top being the minimal solution. From the minimal solution –the chain top- (3,1) there can be obtained two major solutions: (5,3) and (13,9), etc.

3. 2. The equation $x^2 - 5y^2 = 1$

In literature, this equation of type Pell is solved through the finding of the minimal positive solution, using the method of continues fractions [2]. In our method, Pell's equation does not have a special role anymore. Starting from the ordinary solution (1,0), the use of the matrix B, where S = -4, will generate fractional solutions. We look for a natural number p, so that the matrix B could have only integer elements. We have:

$B_1 = B^3 = \begin{pmatrix} 9 & 20 \\ 4 & 9 \end{pmatrix}$ and the integer solutions will be generated by this matrix B_1: $(x_1, y_1) = (9,4)$, etc.

3. 3. The equation $x^2 + 2y^2 + 3z^2 - 5w^2 = 15$

A ordinary equation where S = 1

Matrix B is written:

$$B=\begin{Vmatrix} 1 & 4 & 6 & 10 \\ 2 & 3 & 6 & 10 \\ 2 & 4 & 5 & 10 \\ 2 & 4 & 6 & 11 \end{Vmatrix}$$

Starting from a certain solution S = (3, 2, 1, 1), other 5 new solutions can be obtained: (5, 4, 1. 3), etc.

3. 4. The equation $x^2 + y^2 + z^2 = 89$

The equation has solutions, the number 89 being not equal to $4^l (8k + 7)$.

Let S = (9,2,2) be the given solution and we check if there is at least a rational integer value t among the possible four:

$$t = \frac{2}{3}(\pm 9 \pm 2 \pm 2)$$

We build the matrix B:

$$B= \frac{1}{3}\begin{Vmatrix} 1 & -2 & 2 \\ -2 & 1 & 2 \\ -2 & -2 & 1 \end{Vmatrix}$$

and we determine the solutions : (3,4.8), (0,5.8), (6,2,7), which are all the decomposition in sum of three squares. We notice that 89 is a prime number having a unique decomposition in sum of two squares.

3. 5. The equation $x^2 + y^2 + z^2 = w^2$

This equation was discussed in [6]. The matrix B is written:

$$S_{i+1} = S_i * B \quad \text{and} \quad B = \begin{Vmatrix} 0 & -1 & -1 & 1 \\ -1 & 0 & -1 & 1 \\ -1 & -1 & 0 & 1 \\ -1 & -1 & -1 & 2 \end{Vmatrix}$$

The multitude of solutions is represented through the nodes of a graph, with the top the ordinary solution (1,0,0,1)

In [7], we showed that, using the function "quadratic combination", we find the general solution of the diophantine equation, type Euler-Carmichael-Mordell: $x^2 + b\,y^2 + c\,z^2 = w^2$ $(b, c) \in Z$

We enunciated a theorem, which is stronger than the Lagrange's Four Square Theorem:

Theorem *(Bratu) For any natural number z, there are at least three integer numbers (u,v,w), or/and (a,b,c), in order to have representations:*

$$z = u^2 + v^2 + w^2 \quad (\alpha)$$
$$z = a^2 + b^2 + 2c^2 \quad (\beta) \qquad (15)$$

For $z = z_1 = 2^{2k}(8l + 7)$ *we have only the representation* (β)*,*
for $z = z_2 = 2^{2k+1}(8l + 7)$ *we have only the representation* (α) *and*
for $z \neq z_1 \neq z_2$ *we have, in the same time, the representations* (α) *and* (β)

Examples: $z = 15$ *we have* $z = 3^2 + 2^2 + 2 * 1^2$ (β)

$z = 30$ *we have* $z = 5^2 + 2^2 + 1^2$ (α)

$z = 21$ *we have* $z = 4^2 + 2^2 + 1^2$ (α) *and*

$z = 3^2 + 2^2 + 2 * 2^2$ (β).

Conclusion The proposed method, for the determination of the solutions of quadratic equations, is different from the ones that exist in literature, from Fermat, Lagrange, Gauss.

# # #

REFERENCES

1. H.HASSE Uber die Darstelabarkeit von Zahlen durch quadratische Formen in Korper der rationalen Zahlen. J. reine. angew. Math. 152 (1922) p.129-148
2. L.J.MORDELL Diophantine Equations (1909)-Academic Press London And New York , cap.7-8, p.49-57
3. L.E.DICKSON History of theory of numbers t.3, p.37-39, Chelsea Publ. Comp.(1954)
4. N.I.BRATU Eseu asupra ecuatiilor diofantice-1- Editura Adel Craiova (1994) p.3-17
5. N.I.BRATU Note de analiza diofantica- Editura Dutescu Craiova (1996) p.21-26
6. N.I.BRATU Diophantine equations The first internat. conf. in numbers theory. American Res. Press (1997) p.147-151
7. N.I.BRATU and B.N.BRATU On the quaternary quadratic diophantine equations (1) (2000) Bulletin of Pure and Applied Sciences Vol. 19E/ 2, p.307-310