ON THE QUATERNARY QUADRATIC DIOPHANTINE EQUATIONS

NICOLAE BRATU[1]
ADINA CRETAN[2]

ABSTRACT

This paper has been updated and completed thanks to suggestions and critics coming from Dr. Mike Hirschhorn, from the University of New South Walles. We want to express our highest gratitude.

The paper appeared in an abbreviated form [6]. The present work is a complete form.

For the homogeneous diophantine equations: $x^2 + by^2 + cz^2 = w^2$ there are solutions in the literature only for particular values of the parameters b and c. These solutions were found by Euler, Carmichael, Mordell. They proposed a particular solution for this equation in [3]. This paper presents the general solution of this equation as functions of the rational parameters b, c and their divisors. As a consequence, we obtain the theorem that every positive integer can be represented as the sum of three squares, with at most one of them duplicated, which improves on the Fermat –Lagrange theorem.

Keywords: diophantine equations, parametric solutions, Lagrange's Four Square Theorem

In this paper, we present the parametric solutions for the homogeneous diophantine equations:

$$x^2 + by^2 + cz^2 = w^2 \tag{1}$$

where b, c are rational integers.

I. <u>Present theory</u>

Case 1: b = c =1.

Carmichael [2] showed that the solutions are expressions of the form:

$$w = p^2 + q^2 + u^2 + v^2 \qquad y = 2pq + 2uv \tag{2}$$
$$x = p^2 - q^2 + u^2 - v^2 \qquad z = 2pv - 2qu$$

where p, q, u, v are rational integers.

Mordell showed that these are the equations' only solutions by applying the arithmetic theory of the Gaussian integers.

Case 2: b = 1; c = -1.

Mordell [3] showed that the only solutions are the expressions:

$$2x = ad - bc \qquad 2y = ac + bd \tag{3}$$
$$2z = ac - bd \qquad 2w = ad + bc$$

where a, b, c, d are integer parameters.

---

[1] Dep. of Mathematics Craiova, Romania
[2] *Nicolae Titulescu* University of Bucharest, Romania

Case 3: b, c are rational integers.

Mordell [3] considered the particular solutions with three parameters, proposed by Euler:

$$w = p^2 + bq^2 + cu^2 \qquad y = 2pq \tag{4}$$
$$w = p^2 - bq^2 - cu^2 \qquad z = 2pu$$

II. Results

In [4] we describe a new method for solving quaternary equations using the notion of "quadratic combination". If by G_2^2 we denote the complete set of solutions of the equation: $x^2 + y^2 = z^2$ and by G_3^2 the complete set of solutions of the equation: $x^2 + y^2 + z^2 = w^2$, we can make the following definition:

Definition 1: Quadratic combination is a numerical function _Q _ which associates to a pair of solutions in G_2^2 four solutions in G_3^2. Symbolically we have:

$$Q : G_2^2 \times G_2^2 \to G_3^2$$

Observation

From the quadratic combination of the equation's solutions of the form: $x^2 + by^2 = z^2$, we shall obtain [4] the solutions for the equation: $x^2 + by^2 + cz^2 = w^2$

1. **Case b = c = 1**

From the quadratic combination, we find again the solution (2). We can present another demonstration for Mordell's solutions. [4] (*)

If by E_3^2 we denote an equation: $x^2 + y^2 + z^2 = w^2$ and F_3^2 is a graph, from [4] we have:

Theorem 1.

For the equation E_3^2, the solutions are the expressions (2) and only these.

The first part of the demonstration results from verification. For the second part, we can use the property demonstrated in [4].

Lemma 2.

The set of solutions of equation E_3^2 can be thought of as a graph F_3^2, where the arcs are given by the "t" functions:

$$t = w \pm x \pm y \pm z$$

and the vertices are:

(1,0,0,1), the ordinary solution, then, through the functions t, another four solutions: (3,0,4,5), (3,6,2,7), (7,4,4,9), (7.6,6,11), etc., an infinity of positive solutions (and symmetrically).

The solutions are generated by the relation $S_i = S_{i-1} B$, where B is the matrix:

(*) In annex we present an extract from the paper [4]

$$S_{i+1} = S_i \text{ times } B, \qquad B = \begin{bmatrix} 0 & -1 & -1 & 1 \\ -1 & 0 & -1 & 1 \\ -1 & -1 & 0 & 1 \\ -1 & -1 & -1 & 2 \end{bmatrix} \tag{5}$$

Lemma 3. Any solutions from the equation (2) are on the graph F_3^2 and, conversely, any solutions from F_3^2 can be written in the form (2).

We defined by $t_1 = x + y + z - w$; a term, which diminishes, where variables are natural numbers [4]. We show that from any solution in natural numbers we can obtain a solution with smaller (positive) w; $w_{i+1} < w_i$.

The parameter's correspondence ($p>q$ and $u>v$) will be:

$$p_1 = p - q - v \qquad u_1 = u + q - v$$
$$q_1 = q \qquad v_1 = v$$

It is obtained a number of decreasing value w_1, having as limit the ordinary solution (1,0,0,1). Conversely, using of tj, which enlarges, for every solution w_i from the graph F_3^2 are obtained other larger solutions, $w_{i+1} > w_i$, with positive w.

2. Case b =1, c = -1. Solutions result from quadratic combination:

$$\begin{aligned} w &= p^2 + q^2 - u^2 - v^2 \\ x &= p^2 - q^2 + u^2 - v^2 \\ y &= 2pq + 2uv \\ z &= 2pv - 2qu \end{aligned} \tag{6}$$

It can be shown that the Mordell's solutions (3) are equivalent with solutions (6); the relations between Mordell's parameters and ours are:

$$a = p + v \qquad b = p - v$$
$$c = q - u \qquad d = q + u$$

3. **Case b, c are rational integers**. For simplicity, we shall treat two subcases:

3a) b, c prime numbers. The quadratic combination will require the solutions:

$$\begin{aligned} w &= p^2 + bq^2 + cu^2 + bcv^2 \\ w &= p^2 - bq^2 - cu^2 + bcv^2 \\ y &= 2pq + 2cvu \\ z &= 2pu - 2bqv \end{aligned} \tag{7}$$

3b) b and c are composite. For any decomposition: b = i times j and c = l times h, where i, j, l, h are rational integers, we have the general solutions with four parameters of the equation (1) :

$$w = ihp^2 + jhq^2 + jlu^2 + ilv^2$$
$$x = ihp^2 - jhq^2 + jlu^2 - ilv^2$$

$$y = 2hpq + 2luv \tag{8}$$

$$z = 2ipv – 2jqu$$

Here we assume that x, w are odd, and y, z are even; permutations can be made to obtain analogous solutions.

Verification

For the equation:

$$x^2 – 6y^2 + 15z^2 = w^2 \tag{9}$$

with the particular solution: x = z = 1, y = 0, w = 4

For a decomposition: b = - 6 = (-3) times2 and c = 15 = 3 times 5, we can identify the four parameters i, j, k, l and find another solution of the form (8): x = 37; y = 32; z = 20 and w = 35, that satisfy the equation (9).

III. Applications

It is well known that

2. Theorem of Lagrange
Every number is the sum of four squares:

$$z = u^2 + v^2 + w^2 + t^2 \tag{10}$$

and a later

3. *Theorem of Legendre*:
Every number, not of the form 2^{2k} (81 + 7), is the sum of three squares.

$$z = u^2 + v^2 + w^2 \tag{11}$$

In [4] we proved the stronger theorem:

4. *Theorem of Bratu*

Every number is the sum of three squares, or of three squares with one duplicated. Further, numbers of the form 2^{2k} (8 l + 7) are only of the second type, numbers of the form 2^{2k+1} (81 + 7) are only of the first type, while numbers of neither of these two forms are of both types.

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:

$$z = u^2 + v^2 + w^2 \quad (\alpha) \tag{12}$$

$$z = a^2 + b^2 + 2c^2 \quad (\beta)$$

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 $z \neq z_1$ and $z \neq z_2$, we have in the same time the representation (α) and (β).

Examples: $z_1 = 15$, we have $z_1 = 3^2 + 2^2 + 2$ times 1^2 (β)

$z_2 = 30$, we have $z_2 = 5^2 + 2^2 + 1^2$ (α)

$z_3 = 21$, we have $z_3 = 4^2 + 2^2 + 1^2$ (α) and

$z_3 = 3^2 + 2^2 + 2$ times 2^2 (β).

The proof results using the function "quadratic combination", lemma 2 and noticing the graph F_3^2.

We can enunciate a general theorem [4]:

5. *Theorem of Bratu*

For any natural number Z, there are, simultaneously, at least 7 representations as algebraic sums of three squares of integer numbers:

$$Z = X_i^2 \pm Y_i^2 \pm bT_i^2 \quad \text{where } i=1,\dots 7 \text{ and } b=1,2 \qquad (13)$$

* ANNEX- Extract of [4], pag 39,40,41

"3.2.1 Combinarea patratica.

Am notat cu E_2^2 ecuatia ternara omogena $x^2 + y^2 = z^2$ *(1), cu S o solutie oarecare si F_2^2 arborele solutiilor reduse. Daca renuntam la conditia restrictiva (x,y)=1, obtinem sistemul complet de solutii G_2^2 . Vom nota analog ecuatia cuaternara omogena:* $x^2 + y^2 + z^2 = w^2$ *(2) cu E_3^2 si sistemul complet de solutii G_3^2 .*

Metoda se bazeaza pe urmatoarea lemma:

Lemma Pentru orice doua solutii din sistemul complet de solutii G_2^2 al ecuatiei E_2^2 se pot genera solutii pentru ecuatia cuaternara omogena $x^2 + y^2 + cz^2 = w^2$ *(3), unde c este un numar intreg, prin utilizarea "combimarii patratice".*

Daca $S_1=(x_1, y_1, z_1)$ *si* $S_2=(x_2, y_2, z_2)$ *sunt doua solutii oarecare din sistemul G , iar daca aceste solutii sunt scrise funvtie de solutiile reduse* S'_1 *si* S'_2 *si de coeficientii numerici h si l, atunci exista patru termeni X,Y,Z,W, definiti prin relatiile:*

$X= x_1 \pm x_2$; $Y= y_1 \pm y_2$; $W= z_1 \pm z_2$;

$Z^2= 2 (z'_1 z'_2 \pm x'_1 x'_2 \pm y'_1 y'_2)$, *astfel incat sa avem:*

$X^2 + Y^2 \pm hl Z^2 = W^2$

Reciproca este de asemeni adevarata" etc.

Definitia 1 se refera la functia "quadratic combination"

"3.2.2. <u>Ecuatia</u> $x^2 + y^2 + z^2 = w^2$ *(9)*

Aceasta ecuatie este rezolvata de teorie prin rezultatele lui Mordell, dupa cum am aratat in cap 2. Avem:

$$X = p^2 - q^2 + u^2 - v^2$$
$$Y = 2pq + 2uv \qquad (10)$$
$$Z = 2pv - 2qu$$
$$W = p^2 + q^2 + u^2 + v^2$$

Prin combinarea patratica am regasit aceste rezultate.

Se poate demonstra usor ca daca exista solutie a ecuatiei (9), pentru orice w numar intreg (teorema Hurwitz), exista solutie pentru ecuatia (10) pentru orice w intreg (teorema Lagrange) si reciproc. Vom demonstra in continuare cateva propozitii, etc,

In cazul solutiilor reduse F am convenit ca sa presupunem ca X si W sunt impare si Y si Z sunt pare. Prin combinarea patratica se poate arata ca multimea solutiiilor ecuatiei (9) este data de (10), dar si ca, printr-o dubla combinare a lui S_1 *cu* S_2 *(pare si impare), solutie cu defect, avem multimea solutiilor data de reuniunea a doua submultimi:*

$$X = p^2 - q^2 + u^2; \quad Y = 2pq;$$
$$Z = 2qu \text{ sau } 2pu \quad W = p^2 + q^2 + u^2 \qquad (15a)$$

si

$$X = p^2 - q^2; \quad Y = 2pq + 2u^2;$$
$$Z = 2pu - 2qu; \quad W = p^2 + q^2 + 2u^2 \qquad (15b)$$

Etc

<u>Propozitia</u> 3

Pentru orice numar natural z, care nu este de forma $2^k(8l+7)$*, exista cel putin doua moduri de reprezentare, una ca suma de trei patrate simple si alta ca suma de trei patrate, in care unul dintre patrate este dublat, adica:*

$$z = u^2 + v^2 + w^2 \quad (\alpha)$$
$$z = a^2 + b^2 + 2c^2 \quad (\beta) \qquad (22)$$

pentru $z = 2^{2k}(8l+7)$ *vom avea numai representarea (*β*),*

pentru $z = 2^{2k+1}(8l+7)$ *vom avea numai reprezentarea (*α*)*

Aceasta este o teorema mai tare decat "teorema celor patru patrate"a lui Fermat-Lagrange. Etc.

3.3.5 Teorema generala de reprezentare prin suma algebrica de patrate.

Pentru orice numar natural Z exista cel putin 7 reprezentari prin triplete de patrate de numere intregi:

$$Z = Xi^2 \pm Yi^2 \pm bTi^2, \text{ unde } i=\{1,\dots 7\} \text{ si } b=\{1, 2\} \qquad (26)$$ "

References

1. BOREVICI I. Z., SAFAREVICI I.K. - *Teoria cisel*, Moscova 1964, Iz. Nauka
2. CARMICHAEL R. D. - *Diophantine Analysis*, New-York 1915, Add. John Wiley & Sons
3. MORDELL L. K. - *Diophantine Equations*, London 1969, Academic Press
4. BRATU I.N. - *Note de analiza diofantica*, Craiova 1996, Ed .M. Dutescu
5. DICKSON L. E. - *History of the Theory of Numbers*, Washington 1920, Add. Washington Press
6. BRATU I .N. and BRATU N. B. - *On the quaternary quadratic diophantine equations (1)* , New Delhi 2000, Bulletin of Pure and Applied Sciences, vol. 19E/ 2, p.307-310