МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2007
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2007
Proceedings of the Thirty Sixth Spring Conference of
the Union of Bulgarian Mathematicians
St. Konstantin & Elena resort, Varna, April 2–6, 2007

ALGORITHM FOR FINDING MAXIMAL DIOPHANTINE FIGURES*

Andrey R. Antonov, Maria N. Brancheva

Diophantine figures have been studied by different authors [1, 2, 3, 4, 5, 6] and others. Here we consider Diophantine figures modulo p, where p is a prime number of the kind $p = 4k+3$, $k \in \mathbf{N}$. In fact, these figures are defined as special subsets of the finite field $\mathbb{Z}_p[i]$. The points of the mentioned special subsets are called Gauss-Pythagorean points. Diophantine figure is a subset of Gauss-Pythagorean points such that all the distances between pair of points of the figure are quadratic remainders. An algorithm for finding maximal Diophantine figures modulo p is given. A conjecture in general case is announced.

1. Some recalls. Denote by $Z_p[i]$ the ring of remainders modulo p of Gauss integer numbers, i.e. $n+im$, where $n, m \in Z_p$ ($\mathbb{Z}_p$ is the ring of remainders modulo p, $p \in \mathbb{Z}$). It is well known that for $p = 4k+3$ the ring $\mathbb{Z}_p[i]$ is a field with well defined pairwise distance between its points. Let $P(a, b)$ and $Q(c, d)$ are two points in $\mathbb{Z}_p[i]$, (a, b) corresponds to the Gauss integer number $a + ib$, and (c, d) – to $c + id$. The distance between P and Q is defined by the ordinary Cartesian coordinate formula

$$\mathrm{Dist}^2\left[P, Q\right] = (a-c)^2 + (b-d)^2 .$$

In the case when it is a quadratic remainder in the finite field Z_p, we say that the distance $\mathrm{Dist}\left[P, Q\right]$ between the point P and the point Q is an *integer distance in* $\mathbb{Z}_p[i]$.

A point $P(a, b)$ is called *Gauss-Pythagorean point* in $Z_p[i]$ (or Gauss-Pythagorean point modulo p) if the distance between this point and the origin $O(0, 0)$ is an integer distance in $\mathbb{Z}_p[i]$.

A subset Φ of $\mathbb{Z}_p[i]$ is called a Diophantine figure in $\mathbb{Z}_p[i]$ if all pairwise distances in Φ are integer distances in $\mathbb{Z}_p[i]$. We call it also Diophantine figure modulo p. Let us remark also that we consider only Diophantine figures which contain the origin O. Under this condition all points (vertices) of a Diophantine figure modulo p are Gauss-Pythagorean points modulo p.

A Diophantine figure modulo p is called a *maximal Diophantine figure* modulo p if there is no other strictly larger Diophantine figure Ψ modulo p such that $\Phi \subset \Psi$.

---

*[*]***2000 Mathematics Subject Classification:** 52-04, 52C10, 68U05, 65D18, 51N99

Key words: Diophantine figure, Gauss-Pythagorean points, Structural group of Gauss-Pythagorean homomorphisms, Diophantine invariance, Maximal Diophantine figures, Orbits and their computer programme realization

The set of all Gauss-Pythagorean points modulo $p = 4k + 3$ without the origin is a group with respect to the multiplication in the field $\mathbb{Z}_p[i]$. We denote this set by $GP_p[i]$ – the *group of all Gauss-Pythagorean points modulo p*. Clearly, $GP_p[i] \subset \mathbb{Z}_p[i]$.

The following theorem was announced in [4]:

Theorem 1. *The mapping $\xi \to \alpha\xi$:$Z_p[i] \to \mathbb{Z}_p[i]$ induces a bijective homomorphism on the group of Gauss-Pythagorean points $GP_p[i]$ of $\mathbb{Z}_p[i]$, $\xi \in Z_p[i]$, $\alpha \in GP_p[i]$.*

The set of all Gauss-Pythagorean homomorphisms is a group denoted by $\mathrm{MapGP}_p[i]$. This group is the structural group of the geometry of Diophantine figures. It means that the set of Diophantine figures is invariant determined with respect to Gauss-Pythagorean homomorphisms.

2. Algorithm for finding maximal Diophantine figures in $\mathbb{Z}_p[i]$. We follow all the necessary steps to find maximal Diophantine figures in $\mathbb{Z}_p[i]$. First we find the set GPP[1] of all Gauss-Pythagorean points in $\mathbb{Z}_p[i]$. Let us recall, e.g., that quadratic remainders modulo 7 are 0, 1, 2, 4. Let us denote the set of quadratic reminder with added 0 by **rem**. So rem={0,1,2,4} for the prime number p=7.

Algorithm for finding GPP [1]:

```
begin
GPP={empty list}
   for i from 0 to p-1 do
          for j from 0 to p-1 do
             if Dist(i,j)**2 in rem do
                GPP.append(i,j)
          end
   end
return GPP
```

We already have mentioned that GPP[1] without the origin (0,0) is a group $GP_p[i]$. The cardinality of this group is $(p^2 - 1)/2$.

Next, we go on with finding Diophantine pairs consisting of 2 Gauss-Pythagorean points. Let us mention that the origin is always a vertex in all Diophantine figures but for the simplicity in computations, we *remove* the origin from the further constructions. Let us denote the set of Diophantine pairs without origin by GPP[2]. Going ahead by induction, suppose that we have a set GPP $[n-1]$ of Diophantine figures each one containing $n-1$ Gauss-Pythagorean points from GPP[1] without the origin. Next we follow the intuitive idea for trying to append to a figure Φ from GPP $[n-1]$ a point from GPP[1] in order to obtain a Diophantine figure. If all attempts of appending over *all* points from GPP[1] to Φ fail, then Φ is a maximal Diophantine figure. Let us denote the set of all maximal Diophantine figures where each one consists of $n-1$ points with GPPmax $[n-1]$. The idea is simple, but it needs an exhaustive search.

Algorithm for finding GPP[n]:

```
begin
GPP[n]={empty list}
GPPmax [n − 1] ={empty list}
   for Figure in GPP [n − 1] do
          count=0
```

```
        for Point in GPP[1] do
           if (Figure and Point) is a DiophantineFigure do
              count=count+1
                 GPP[n].append(Figure,Point)
           if count=0 do
              GPPmax[n − 1].append(Figure)
           end
        end
return GPP[n],GPPmax[n − 1]
```

Following these steps, we found all maximal Diophantine figures modulo $p = 7$ and $p = 11$. Some of the results are explained below. Maximal Diophantine figures are divided into two subsets. The first subset contains all figures with $(p + 3)/2$ vertices, the second subset consists of Maximal Diophantine figures with maximal length. The tables below clear out the situation for $p = 7$ and $p = 11$.

Case $p = 7$:

Diophantine figure	GPP[1]	GPP[2]	GPP[3]	GPP[4]	GPP max[4]	GPP[5]	GPP[6]	GPP max[6]
Number of figures	24	132	200	90	30	24	4	4

Case $p = 11$:

Diophantine figure	GPP[1]	GPP[2]	GPP[3]	GPP[4]	GPP[5]	GPP[6]	GPP max[6]	GPP[7]	GPP[8]
Number of figures	60	870	3920	6060	4032	1680	420	720	270
Diophantine figure	GPP[9]	GPP[10]	GPP max[10]						
Number of figures	60	6	6						

We give some illustrations for the case $p = 7$. For the sake of simplicity, in all figures the origin is not drawn.

3. Group action of $\mathbf{GP}_p[i]$ and orbits of maximal Diophantine figures. We shall skip recalling some basic group notions from textbooks. Consider the action of $GP_p[i]$ on the set DF_p of Diophantine figures modulo p. Viewing each $\Phi \in DF_p$ as a set of points, we define the formula of $GP_p[i]$ on DF_p by $g \to r_g$: $g \in GP_p[i]$, where $r_g(\Phi)$ consists of the vertices of Φ, multiplied by g. We consider the figure Φ as a set of points, so that the action of $GP_p[i]$ on Φ is well defined by multiplication of all vertices of Φ with a given element g from $GP_p[i]$. This action is interesting from the point of view of finding all orbits of all already found maximal Diophantine figures. In this case we should consider as equivalent all the figures in one orbit. We have made computations for the cases $p = 7$ and $p = 11$.

For the case $p = 7$ the maximal Diophantine figures in GPPmax[4] (like the upper in Figure 2) are divided into two orbits of lengths 6 and 24. All maximal Diophantine figures in GPPmax[6] belong to one orbit, or all the “line” figures in Figure 3 could be obtained from each other by multiplication with a suitable point from GPP[1].

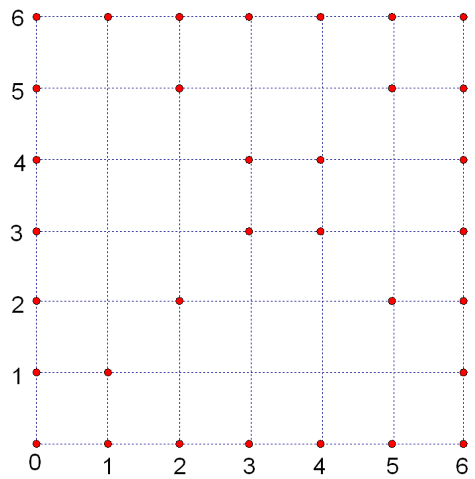

Figure 1. All Gauss-Pythagorean points in case $p = 7$:

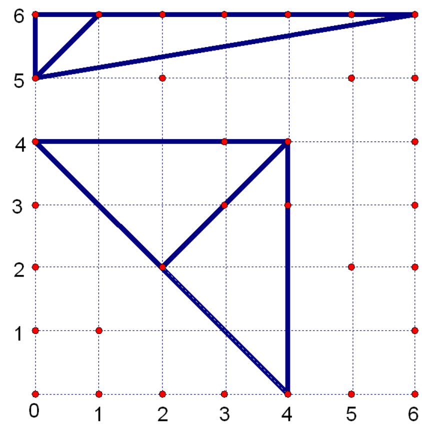

Figure 2. Two nonlinear maximal Diophantine figures in case $p = 7$ first – [(0;5),(0;6),(1;6),(6;6)]; second – [(0;4),(4;4),(2;2),(4,0)]

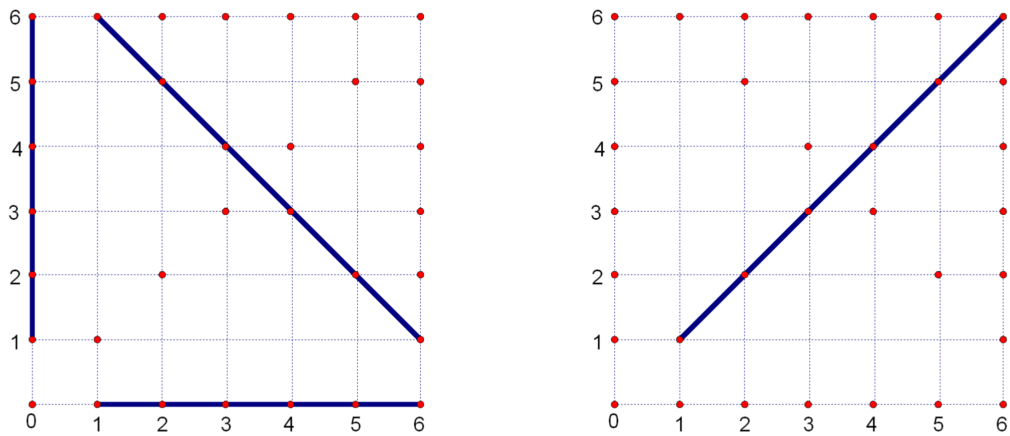

Figure 3. All four maximal Diophantine figures with maximal length – all are linear

For the case $p = 11$ the maximal Diophantine figures in GPPmax[6] are divided into: 6 orbits of length 60, 1 orbit of length 30, 1 orbit of length 20, and 1 orbit of length 10.

All maximal Diophantine figures in GPPmax[10] are linear and belong to one and the same orbit as in the case $p = 7$.

From computational observation we come to the:

Conjecture. For all $p = 4k + 3$ maximal Diophantine figures modulo p exist and are divided into two types (including the origin): the first – from nonlinear figures with number of vertices $(p + 3)/2$, and the second – of linear figures belonging to one and the same orbit with p vertices.

REFERENCES

[1] S. Dimiev, Iv. Tonov. Diophantine figures, *Math. and Education in Math.*, **15** (1986), 383–390.

[2] S. Dimiev, Kr. Markov. Gauss Integers and Diophantine Figures, *Math. and Education in Math.*, **31** (2002), 88–95.

[3] A. Cohnert, S. Kurz. A note on Erdos-Diophantine graphs and Diophantine carpets. *Mathematica Balkanica*, **20** (3-4), 2006.

[4] S. Dimiev (to appear in the Proceeding of the 3th Congress of Macedonian Mathematicians).

[5] A. Cohnert, S. Kurz. Preprint, 2006.

[6] S. Kurz. Konstruktion und Eigenschaften Ganzzahliger Punktmengen. Bayreuther Mathematische Schriften, Heft **76**, 2006.

Andrey R. Antonov
University of Chemical Technology and Metallurgy
8, St. Kliment Ohridski Blvd
1756 Sofia, Bulgaria
e-mail: andrio@uctm.edu

Maria Brancheva
Plovdiv University
Filial Smolyan
32, Dicho Petrov Str.
2700 Smolyan, Bulgaria
e-mail: mbrancheva@yahoo.com

АЛГОРИТЪМ ЗА НАМИРАНЕ НА МАКСИМАЛНИ ДИОФАНТОВИ ФИГУРИ

Андрей Антонов, Мария Бранчева

Диофантовите фигури са изследвани от различни автори $[1, 2, 3, 4, 5]$ и други. В тази статия разглеждаме подмножества на крайното поле $\mathbb{Z}_p[i]$, където p е просто число от вида $p = 4k + 3$, $k \in N$, а i е имагинерната единица. Чрез подходящо дефинирано разстояние между елементите на това поле се въвежда понятието Гаус-Питагорова точка. Диофантова фигура се нарича подмножество на $\mathbb{Z}_p[i]$ състоящо се от Гаус-Питагорови точки такива, че разстоянието между всеки две точки от фигурата да е квадратичен остатък в полето $\mathbb{Z}_p$. След въвеждане на понятията, в статията е описан ефективен алгоритъм за намиране на Диофантови фигури. Посочени са и някои нови свойства на Диофантовите фигури. Някои от резултатите са онагледени за $p = 7$ и $p = 11$.