DIOPHANTINE QUADRUPLES AND QUINTUPLES MODULO 4

Andrej Dujella

Abstract: A Diophantine m-tuple with the property $D(n)$ is a set $\{a_1, a_2, \dots a_m\}$ of positive integers such that for $1 \le i < j \le m$, the number $a_i a_j + n$ is a perfect square. In the present paper we give necessary conditions that the elements a_i of a set $\{a_1, a_2, a_3, a_4, a_5\}$ must satisfy modulo 4 in order to be a Diophantine quintuple.

Let n be an integer. A set of positive integers $\{a_1, a_2, \dots, a_m\}$ is called *a Diophantine m-tuple with the property* $D(n)$, or P_n*-set of size* m, if $a_i a_j + n$ is a perfect square for all $1 \le i < j \le m$. A P_n-set X will be termed *extendable* if, for some integer d, $d \notin X$, the set $X \cup \{d\}$ is a P_n-set.

The problem of extending P_n-sets is an old one, dating from the time of Diophantus (see [4, 5]). The first P_1-set of size 4 was found by Fermat, and it was $\{1, 3, 8, 120\}$. The most famous result on P_n-sets is due to Baker and Davenport [2], who proved that if $\{1, 3, 8, d\}$ is a P_1-set, then d has to be 120.

In 1985, Brown [3], Gupta and Singh [8] and Mohanty and Ramasamy [9] proved independently that if $n \equiv 2 \pmod 4$, then there does not exist a P_n-set of size 4. In 1993, the author proved that if $n \not\equiv 2 \pmod 4$ and $n \notin \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exists at least one P_n-set of size 4 (see [6]). P_n-sets of size 5 were studied in [1, 7, 10].

The purpose of the present paper is to characterize congruence types modulo 4 of Diophantine quadruples and quintuples. We will say that a set $X = \{a_1, \dots, a_m\}$ has *a congruence type* $[b_1, \dots, b_m]$, where $b_i \in \{0, 1, 2, 3\}$, if $a_i \equiv b_i \pmod 4$ for $i = 1, \dots, m$.

[0] *Mathematics Subject Classification (1991):* 11A07, 11B75, 11D79

Keywords and Phrases: Diophantine m-tuple, P_n-set, congruences

Our starting point is the following result of Mootha and Berzsenyi [11, Theorems 1, 2 and 3].

Theorem 1 **(a)** *If all of the elements of a P_n-set of size $m \geq 3$ are odd, then they are congruent to one another, modulo* 4*.*

(b) *If only one of the elements of P_n-set of size $m \geq 3$ is odd, then all of the others are congruent to* 0*, modulo* 4*.*

(c) *P_n-sets of the congruence type $[1, 2, 3]$ are not extendable.*

Proof: **(a)** Let $\{a, b, c\}$ be a P_n-set. Assume that a, b, c are odd and $a \equiv b \equiv c - 2 \pmod 4$. Since square of an integer is congruent to 0 or 1 modulo 4, $ab + n = \square$ implies $n \equiv 0, 3 \pmod 4$, and $ac + n = \square$ implies $n \equiv 1, 2 \pmod 4$. Contradiction.

(b) Assume that $\{a, b, c\}$ is a P_n-set, a is odd, b is even and $c \equiv 2 \pmod 4$. Then $ac + n = \square$ implies $n \equiv 2, 3 \pmod 4$, and $bc + n = \square$ implies $n \equiv 0, 1 \pmod 4$. Contradiction.

(c) Assume that $\{a, b, c, d\}$ is a P_n-set, $a \equiv 1 \pmod 4$, $b \equiv 2 \pmod 4$ and $c \equiv 3 \pmod 4$. Applying **(a)** on the set $\{a, c, d\}$ we see that d cannot be odd, and applying **(b)** on the set $\{a, b, d\}$ we see that d cannot be even. ∎

Theorem 2 *A P_n-set of size* 4 *has one of the following congruence types:*

$$[0, 0, 0, 0], \quad [0, 0, 0, 2], \quad [0, 0, 2, 2], \quad [0, 2, 2, 2], \quad [2, 2, 2, 2],$$

$$[0, 0, 0, 1], \quad [0, 0, 0, 3], \quad [0, 0, 1, 1], \quad [0, 0, 1, 3], \quad [0, 0, 3, 3],$$

$$[0, 1, 1, 1], \quad [0, 3, 3, 3], \quad [2, 1, 1, 1], \quad [2, 3, 3, 3], \quad [1, 1, 1, 1], \quad [3, 3, 3, 3],$$

and all of these congruence types are indeed possible.

Proof: The first part of the theorem follows directly from Theorem 1, and the second part will follow from Theorem 4 below. ∎

Theorem 3 *A P_n-set of size* 5 *has one of the following congruence types:*

$$[0,0,0,0,0],\quad [0,0,0,0,2],\quad [0,0,0,2,2],\quad [0,0,2,2,2],\quad [0,2,2,2,2],$$

$$[2,2,2,2,2],\quad [0,0,0,0,1],\quad [0,0,0,0,3],\quad [0,0,0,1,1],\quad [0,0,0,1,3],$$

$$[0,0,0,3,3],\quad [0,0,1,1,1],\quad [0,0,3,3,3],\quad [0,1,1,1,1],\quad [2,1,1,1,1],$$

$$[0,3,3,3,3],\quad [2,3,3,3,3],\quad [1,1,1,1,1],\quad [3,3,3,3,3].$$

Proof: The theorem is a direct consequence of Theorem 2. ∎

Theorem 4 *For all congruence types from Theorem 3, apart from maybe* $[1,1,1,1,1]$ *and* $[3,3,3,3,3]$*, there exists a nonzero integer* n *and a* P_n*-set of size* 5 *with that congruence type.*

Proof: The theorem follows from the following table:

n	P_n-set of size 5	Congruence type
-1196	$\{28, 44, 60, 84, 180\}$	$[0, 0, 0, 0, 0]$
-455	$\{8, 72, 102, 148, 492\}$	$[0, 0, 0, 0, 2]$
1600	$\{8, 42, 250, 768, 22272\}$	$[0, 0, 0, 2, 2]$
1024	$\{2, 66, 210, 640, 36480\}$	$[0, 0, 2, 2, 2]$
14400	$\{26, 200, 266, 506, 9450\}$	$[0, 2, 2, 2, 2]$
-299	$\{14, 22, 30, 42, 90\}$	$[2, 2, 2, 2, 2]$
1024	$\{4, 33, 2660, 5520, 245760\}$	$[0, 0, 0, 0, 1]$
9216	$\{12, 99, 7980, 16560, 737280\}$	$[0, 0, 0, 0, 3]$
400	$\{4, 21, 125, 384, 11136\}$	$[0, 0, 0, 1, 1]$
-255	$\{8, 32, 77, 203, 528\}$	$[0, 0, 0, 1, 3]$
-476	$\{20, 31, 75, 96, 192\}$	$[0, 0, 0, 3, 3]$
400	$\{4, 21, 69, 125, 384\}$	$[0, 0, 1, 1, 1]$
400	$\{7, 12, 63, 128, 375\}$	$[0, 0, 3, 3, 3]$
3600	$\{13, 100, 133, 253, 4725\}$	$[0, 1, 1, 1, 1]$
-3185325	$\{1113, 2958, 3417, 3993, 4725\}$	$[2, 1, 1, 1, 1]$
1296	$\{11, 35, 128, 243, 315\}$	$[0, 3, 3, 3, 3]$
-353925	$\{371, 986, 1139, 1331, 1575\}$	$[2, 3, 3, 3, 3]$

■

Corollary 1 *For all congruence types from Theorem 3, there exists an integer* n *and a* P_n*-set of size* 5 *with that congruence type.*

Proof: The statement follows directly from Theorem 4, using the fact that $\{1, 9, 25, 49, 81\}$ and $\{3, 27, 75, 147, 243\}$ are P_0-sets. ■

References

[1] J. Arkin, V. E. Hoggatt, E. G. Strauss, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. **17**(1979), 333–339.

[2] A. Baker, H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2) **20**(1969), 129–137.

[3] E. Brown, *Sets in which* $xy + k$ *is always a square*, Math. Comp. **45**(1985), 613–620.

[4] L. E. Dickson, *History of the Theory of Numbers, Vol. 2*, Chelsea, New York, 1992, pp. 513–520.

[5] Diophantus of Alexandria, *Arithmetics and the Book of Polygonal Numbers*, (I. G. Bashmakova, Ed.), Nauka, Moscow, 1974 (in Russian), pp. 103–104, 232.

[6] A. Dujella, *Generalization of a problem of Diophantus*, Acta Arith. **65**(1993), 15–27.

[7] A. Dujella, *On Diophantine quintuples*, Acta Arith. **81**(1997), 69–79.

[8] H. Gupta, K. Singh, *On* k*-triad sequences*, Internat. J. Math. Math. Sci. **5**(1985), 799–804.

[9] S. P. Mohanty, A. M. S. Ramasamy, *On* $P_{r,k}$ *sequences*, Fibonacci Quart. **23**(1985), 36–44.

[10] V. K. Mootha, *On the set of numbers* $\{14, 22, 30, 42, 90\}$, Acta Arith. **71**(1995), 259–263.

[11] V. K. Mootha, G. Berzsenyi, *Characterizations and extendibility of* P_t*-sets*, Fibonacci Quart. **27**(1989), 287–288.

Andrej Dujella
Department of Mathematics, University of Zagreb,
Bijenička cesta 30, 10000 Zagreb, CROATIA

E-mail: `duje@math.hr`