Diophantine m-tuples with elements in arithmetic progressions

A. Dujella and N. Saradha

Abstract

In this paper, we consider the problem of existence of Diophantine m-tuples which are (not necessarily consecutive) elements of an arithmetic progression. We show that for $n \geq 3$ there does not exist a Diophantine quintuple $\{a, b, c, d, e\}$ such that $a \equiv b \equiv c \equiv d \equiv e \pmod{n}$. On the other hand, for any positive integer n there exist infinitely many Diophantine triples $\{a, b, c\}$ such that $a \equiv b \equiv c \equiv 0 \pmod{n}$.

Keywords Diophantine m-tuples, arithmetic progressions, Pellian equations
Mathematics Subject Classification (2010) 11D09, 11B25

1 Introduction.

A set of m positive integers $\{a_1, a_2, ..., a_m\}$ is called a Diophantine m-tuple if $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. The first Diophantine quadruple, the set $\{1, 3, 8, 120\}$, was found by Fermat. Euler proved that there are infinitely many Diophantine quadruples. On the other hand, it is known that there does not exist a Diophantine sextuple, and there are only finitely many Diophantine quintuples (see [3]). The folklore conjecture is that there does not exist a Diophantine quintuple. There is a stronger version of this conjecture.

Conjecture 1. *All Diophantine quadruples $\{a, b, c, d\}$ are regular, i.e. satisfy the relation $(a + b - c - d)^2 = 4(ab + 1)(cd + 1)$.*

This stronger conjecture implies that the extension of a Diophantine triple to a Diophantine quadruple is essentially unique, namely if $d > \max\{a, b, c\}$, then $d = a + b + c + 2abc + 2\sqrt{(ab + 1)(ac + 1)(bc + 1)}$.

Consider the Diophantine triple $\{1, 8, 15\}$. Its elements are consecutive elements in an arithmetic progression. It is easy to find infinitely many such triples (see [1, 4]). Moreover, by using the fact that in a Diophantine triple $\{a, b, c\}$ with $a < b < c$ either $c = a + b + 2\sqrt{ab+1}$ or $c > 4ab$ (see [6, Lemma 4]), we see that there does not exist a Diophantine quadruple with elements which are consecutive elements in an arithmetic progression.

In this paper, we consider the problem of existence of Diophantine m-tuples which are elements of an arithmetic progression, but not necessarily consecutive elements. More precisely, we fix integers $n \geq 2$ and k and ask for Diophantine m-tuples with all elements congruent to k modulo n.

It is easy to see that there does not exist a Diophantine triple with odd elements. Indeed, if we have three odd numbers, then there exist two of them, say a_1 and a_2, which are congruent modulo 4, but then $a_1a_2 + 1 \equiv 2 \pmod 4$ cannot be a square. On the other hand, there are infinitely many Diophantine quadruples with even elements, e.g.

$$\{2k, 2k+2, 8k+4, 128k^3 + 192k^2 + 88k + 12\} \tag{1}$$

is a Diophantine quadruple for any positive integer k. We conjecture that for $n \geq 3$ there does not exist a Diophantine quadruple $\{a, b, c, d\}$ such that $a \equiv b \equiv c \equiv d \pmod n$. However we can show that this conjecture is true under Conjecture 1. See Remark 1 for details. On the other hand, we can prove unconditionally that there is no Diophantine quintuple with this property in Theorem 1 below.

2 Diophantine quintuples in arithmetic progressions

Theorem 1. *Let k and n be integers and $n \geq 3$. There does not exist a Diophantine quintuple $\{a, b, c, d, e\}$ such that $a \equiv b \equiv c \equiv d \equiv e \equiv k \pmod n$.*

Proof. Assume that $\{a, b, c, d, e\}$ is a Diophantine quintuple with $a < b < c < d < e$ and $a \equiv b \equiv c \equiv d \equiv e \equiv k \pmod n$. Then, by [5], the Diophantine quadruple $\{a, b, c, d\}$ is regular. Therefore,

$$d = a + b + c + 2abc + 2rst,$$

where $ab + 1 = r^2$, $ac + 1 = s^2$, $bc + 1 = t^2$. First we consider the case $n = 4$ (or more generally $4|n$). From $k^2 + 1 \equiv r^2 \pmod 4$, we see that k cannot be odd, while for $k \equiv 2 \pmod 4$ we get $r^2 \equiv 5 \pmod 8$, a contradiction. Finally, if $a \equiv b \equiv c \equiv 0 \pmod 4$, then $d \equiv 2 \pmod 4$. Thus we have shown that $4 \nmid n$.

Now without loss of generality we can assume that n is an odd prime (since n certainly has such factor). From $a \equiv b \equiv c \equiv d \equiv k \pmod n$ and $r^2 \equiv s^2 \equiv t^2 \equiv k^2 + 1 \pmod n$, we get

$$4r^2s^2t^2 = (d-a-b-c-2abc)^2 \equiv (-2k-2k^3)^2 = 4k^6+8k^4+4k^2 \pmod n.$$

On the other hand, $4r^2s^2t^2 \equiv 4(k^2+1)^3 = 4k^6 + 12k^4 + 12k^2 + 4 \pmod n$. Hence $4(k^2+1)^2 \equiv 0 \pmod n$ which implies that $k^2 + 1 \equiv 0 \pmod n$.

Now, we claim that there does not exist a Diophantine triple $\{a, b, c\}$ such that $a \equiv b \equiv c \equiv k \pmod n$, where n is an odd prime and $k^2 + 1 \equiv 0 \pmod n$.

Assume that such triple exists and that, for fixed k and n, $\{a, b, c\}$ is such triple with minimal value of $a+b+c$. From $r^2 \equiv k^2+1 \equiv 0 \pmod n$, we get $r \equiv 0 \pmod n$. From $ac + 1 = s^2$ and $bc + 1 = t^2$, we get

$$bs^2 - at^2 = b - a. \tag{2}$$

Consider the Pellian equation

$$bx^2 - ay^2 = b - a. \tag{3}$$

Its corresponding Pell equation $u^2 - abw^2 = 1$ has fundamental solution $(u, v) = (r, 1)$. By [2, Lemma 1], there is a finite set $(x_0^{(i)}, y_0^{(i)})$ of solutions of (3) such that all solutions of (3) are given by

$$x\sqrt{b} + y\sqrt{a} = (x_0^{(i)}\sqrt{b} + y_0^{(i)}\sqrt{a})(r + \sqrt{ab})^m, \quad m \ge 0, \tag{4}$$

where, for all i,

$$\begin{cases} 0 < x_0^{(i)} < \sqrt{\frac{r+1}{2}} \\ 0 < |y_0^{(i)}| < \sqrt{\frac{b\sqrt{b}}{2\sqrt{a}}}. \end{cases} \tag{5}$$

Denote the solution (x, y) defined by (4) as $(x_m^{(i)}, y_m^{(i)})$. Then

$$x_m^{(i)} = 2rx_{m-1}^{(i)} - x_{m-2}^{(i)}.$$

We know that $r \equiv 0 \pmod n$. Hence by induction we get

$$\begin{cases} x_{2j}^{(i)} \equiv \pm x_0^{(i)} \pmod n \\ x_{2j+1}^{(i)} \equiv \pm k y_0^{(i)} \pmod n). \end{cases} \tag{6}$$

We also know that $r^2 \equiv 1 \pmod{a}$. By comparing the coefficients of $\sqrt{b}$ in (4), we get

$$\begin{cases} x_{2j}^{(i)} \equiv x_0^{(i)} \pmod{a} \\ x_{2j+1}^{(i)} \equiv r x_0^{(i)} \pmod{a}, \end{cases} \tag{7}$$

so that

$$(x_m^{(i)})^2 \equiv (x_0^{(i)})^2 \pmod{a}.$$

It is clear from (3) that $(x_0^{(i)})^2 \equiv 1 \pmod{\frac{a}{\gcd(a,b)}}$. We will show that $(x_0^{(i)})^2 \equiv 1 \pmod{a}$. By (2), there exist i, m such that $s = x_m^{(i)}$. Since $s^2 = ac + 1 \equiv 1 \pmod{a}$, we conclude from (7) that $(x_0^{(i)})^2 \equiv 1 \pmod{a}$. Moreover, from $s \equiv 0 \pmod{n}$ and (6), we get

$$x_0^{(i)} \equiv 0 \pmod{n} \text{ or } y_0^{(i)} \equiv 0 \pmod{n}. \tag{8}$$

Hence, $x_0^{(i)} \geq n$ or $|y_0^{(i)}| \geq n$. In particular, $x_0^{(i)} > 1$.

Consider the first possibility in (8), viz., $x_0^{(i)} \equiv 0 \pmod{n}$. Define an integer c_0 by

$$c_0 = \frac{(x_0^{(i)})^2 - 1}{a}.$$

Then $c_0 > 0$ and $ac_0 + 1 = (x_0^{(i)})^2$. Since $(x_0^{(i)}, y_0^{(i)})$ is a solution of (3), we also get $bc_0 + 1 = (y_0^{(i)})^2$. Since $x_0^{(i)} \equiv 0 \pmod{n}$, we have $ac_0 + 1 \equiv k^2 + 1 \pmod{n}$, and so $c_0 \equiv k \pmod{n}$. On the other hand, by (5),

$$c_0 < \frac{r-1}{2a} < \sqrt{\frac{b}{a}} < b < c.$$

Hence, $\{a, b, c_0\}$ is a Diophantine triple with $a + b + c_0 < a + b + c$ which contradicts the minimality of $a + b + c$.

It remains to consider the second case in (8) when $y_0^{(i)} \equiv 0 \pmod{n}$. In this case we take $x_1 = x_0^{(i)} r - a|y_0^{(i)}|$ and $x_1' = x_0^{(i)} r + a|y_0^{(i)}|$. Observe that

$$x_1 \equiv x_1' \equiv 0 \pmod{n}.$$

As $(x_0^{(i)}, y_0^{(i)})$ satisfies (3), we find that

$$\begin{aligned} x_1 x_1' &= (x_0^{(i)})^2 r^2 - a^2 |y_0^{(i)}|^2 = (ab+1)(x_0^{(i)})^2 - a^2 (y_0^{(i)})^2 \\ &= a(b-a) + (x_0^{(i)})^2. \end{aligned} \tag{9}$$

Then $x_1' > 0$ and $x_1 \equiv 0 \pmod{n}$ give

$$x_1 > 1.$$

Also

$$x_1^2 \equiv (x_0^{(i)})^2 r^2 \equiv r^2 \equiv 1 \pmod{a}.$$

Define an integer c_1 by

$$c_1 = \frac{(x_1^2 - 1)}{a}.$$

Since $x_1 > 1$, we get $c_1 > 0$. Thus $ac_1 + 1 = x_1^2$ and using the fact that $(x_1^{(i)}, y_1^{(i)})$ satisfies (3), we get $bc_1 + 1 = (bx_0^{(i)} - r|y_0^{(i)}|)^2$. Further $y_0^{(i)} \equiv 0 \pmod{n}$ gives $ac_1 + 1 = x_1^2 \equiv (x_0^{(i)})^2 r^2 \equiv 0 \pmod{n}$, so that $ac_1 + 1 \equiv k^2 + 1 \pmod{n}$ which shows that

$$c_1 \equiv k \pmod{n}.$$

From (9) and (5), we get

$$x_1 x_1' < ab + (x_0^{(i)})^2 \leq r^2 - 1 + \frac{r+1}{2} < \frac{2r^2 + r}{2}.$$

Since $x_1' > x_0^{(i)} r \geq 2r$, we have

$$x_1 < \frac{2r^2 + r}{2x_1'} < \frac{r+1}{2},$$

and hence

$$ac_1 + 1 < \frac{(r+1)^2}{4} < r^2 = ab + 1,$$

so

$$c_1 < b.$$

Therefore, $\{a, b, c_1\}$ is a Diophantine triple with $a + b + c_1 < a + b + c$, which contradicts the minimality of $a + b + c$. This completes the proof of Theorem 1. $\square$

Remark 1. Assuming Conjecture 1, we can show that there does not exist a Diophantine quadruple $\{a, b, c, d\}$ such that

$$a \equiv b \equiv c \equiv d \equiv k \pmod{n}, \tag{10}$$

unless $(n, k) = (2, 0)$. Indeed, the example (1) shows that there are infinitely many Diophantine quadruples with $a \equiv b \equiv c \equiv d \equiv 0 \pmod{2}$. Further we have seen that there are no quadruples with all odd elements. Conjecture 1 implies the Diophantine quadruple $\{a, b, c, d\}$ is regular, i.e. $d = a+b+c+2abc+2rst$ (assuming that $d = \max(a, b, c, d)$). But in the proof of Theorem 1 we have shown that a regular Diophantine quadruple cannot satisfy (10) with $n \geq 3$. Thus a Diophantine quadruple satisfying (10) is possible only when $(n, k) = (2, 0)$.

3 Diophantine triples in arithmetic progressions

We have seen in the proof of Theorem 1 that for pairs (n, k) with n prime and $k^2 + 1 \equiv 0 \pmod{n}$ there does not exist a Diophantine triple $\{a, b, c\}$ such that $a \equiv b \equiv c \equiv k \pmod{n}$, for example when $(n, k) = (5, 2), (5, 3), (13, 5), (13, 8), (17, 4), (17, 13)$. On the other hand, the example $\{1, 8, 15\}$ given in the introduction shows that for $(n, k) = (7, 1)$ such a triple exists. In this section, we prove a general result on existence of Diophantine triples in certain arithmetic progressions.

Theorem 2. *For any positive integer n there exist infinitely many Diophantine triples $\{a, b, c\}$ such that $a \equiv b \equiv c \equiv 0 \pmod{n}$.*

Proof. Take two positive integers a, b such that $a \equiv b \equiv 0 \pmod{n}$ and $ab+1$ is a perfect square. For example, we may take $a = \alpha n$, $b = (\alpha n^2+2)n$ for a positive integer α. We show that each such pair $\{a, b\}$ can be extended to a Diophantine triple $\{a, b, c\}$ with the property that $c \equiv 0 \pmod{n}$. From the conditions $ac + 1 = x^2$, $bc + 1 = y^2$ we get the Pellian equation

$$bx^2 - ay^2 = b - a. \tag{11}$$

Consider the corresponding Pell equation

$$u^2 - abw^2 = 1. \tag{12}$$

Note that ab is not a perfect square. It is well known (see e.g. [7, Corollary, p.55]) that there exists a solution (u, w) (in fact, infinitely many solutions) of (12) with $w \equiv 0 \pmod{d}$ for any positive integer d, hence in particular for $d = n$. Now $x = u + aw$, $y = u + bw$ is a solution of (11) and

$$\begin{aligned} x^2 &= 1 + abw^2 + a^2w^2 + 2auw = 1 + ac, \\ y^2 &= 1 + abw^2 + b^2w^2 + 2buw = 1 + bc, \end{aligned}$$

where

$$c = aw^2 + bw^2 + 2uw,$$

which clearly satisfies $c \equiv 0 \pmod{n}$. Hence, there are infinitely many triples with the desired property. $\square$

Acknowledgement: We like to thank Divyum Sharma for some useful comments. A.D. was supported by the Croatian Science Foundation under the project no. 6422.

References

[1] M. N. Deshpande, *Problem* 10622, Amer. Math. Monthly 104 (1997), 870.

[2] A. Dujella, *An absolute bound for the size of Diophantine m-tuples*, J. Number Theory **89** (2001), 126–150.

[3] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[4] Z. Franco, *Solution of Problem* 10622, Amer. Math. Monthly 106 (1999), 868.

[5] Y. Fujita, *Any Diophantine quintuple contains a regular Diophantine quadruple*, J. Number Theory **129** (2009), 1678–1697.

[6] B. W. Jones, *A second variation on a problem of Diophantus and Davenport*, Fibonacci Quart. **16** (1978), 155–165.

[7] L. J. Mordell, *Diophantine Equations,* 1969, Academic Press, London.

Addresses of the authors:
Department of Mathematics,
University of Zagreb,
Bijenička cesta 30,
10000 Zagreb, CROATIA

School of Mathematics,
Tata Institute of Fundamental Research,
Homi Bhabha Road,
Mumbai-400 005, INDIA