Periodica Mathematica Hungarica (2020) 81:134–148
https://doi.org/10.1007/s10998-020-00333-2

Arithmetic properties of polynomials

Yong Zhang[1] · **Zhongyan Shen**[2]

Published online: 17 March 2020

Abstract

First, we prove that the Diophantine system

$$f(z)=f(x)+f(y)=f(u)-f(v)=f(p)f(q)$$

has infinitely many integer solutions for $f(X)=X(X+a)$ with nonzero integers $a\equiv 0,1,4 \pmod 5$. Second, we show that the above Diophantine system has an integer parametric solution for $f(X)=X(X+a)$ with nonzero integers a, if there are integers m,n,k such that

$$\begin{cases}(n^2-m^2)(4mnk(k+a+1)+a(m^2+2mn-n^2)) & \equiv 0 \pmod{(m^2+n^2)^2},\\ (m^2+2mn-n^2)((m^2-2mn-n^2)k(k+a+1)-2amn) & \equiv 0 \pmod{(m^2+n^2)^2},\end{cases}$$

where $k\equiv 0 \pmod 4$ when a is even, and $k\equiv 2 \pmod 4$ when a is odd. Third, we get that the Diophantine system

$$f(z)=f(x)+f(y)=f(u)-f(v)=f(p)f(q)=\frac{f(r)}{f(s)}$$

has a five-parameter rational solution for $f(X)=X(X+a)$ with nonzero rational number a and infinitely many nontrivial rational parametric solutions for $f(X)=X(X+a)(X+b)$ with nonzero integers a,b and $a\neq b$. Finally, we raise some related questions.

Keywords Diophantine system · Integer solution · Parametric solution · Pellian equation · Elliptic curve

Mathematics Subject Classification Primary 11D25 · 11D72; Secondary 11G05

This research was supported by the National Natural Science Foundation of China (Grant No. 11501052), Younger Teacher Development Program of Changsha University of Science and Technology (Grant No. 2019QJCZ051), Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering (Changsha University of Science and Technology), and the Natural Science Foundation of Zhejiang Province (Project No. LY18A010016).

✉ Yong Zhang
zhangyongzju@163.com

Extended author information available on the last page of the article

1 Introduction

The kth n-gonal number is given by

$$P_k^n = \frac{k((n-2)(k-1)+2)}{2}.$$

For $n=3$, $P_k^3 = k(k+1)/2$ are called triangular numbers. In 1968, Sierpiński [14] showed that there are infinitely many triangular numbers which at the same time can be written as the sum, difference, and product of other triangular numbers. For $n=4$, $P_k^4 = k^2$, it is easy to show that $(4m^2+1)^2$ is the sum, difference, and product of squares (see [1]), from the identify $(4m^2+1)^2 = (4m)^2 + (4m^2-1)^2 = (8m^4+4m^2+1)^2 - (8m^4+4m^2)^2$ and there are infinitely many composite numbers of the form $4m^2+1$ (for example, if $m = 5j+1$, $4m^2+1$ is divisible by 5). In 1986, Hirose [10] proved that for $n = 5, 6, 8$, there are infinitely many n-gonal numbers which at the same time can be written as the sum, difference, and product of other n-gonal numbers. The cases with $n=7$ and $n \geq 9$ are still open.

Some authors proved similar results for the sum and the difference only, such as Hansen [8] for $n=5$, O′Donnell [11,12] in cases of $n = 6, 8$, Hindin [9] for $n=7$, and Ando [1] in the general case. In 1982, Eggan et al. [7] showed that for every n there are infinitely many n-gonal numbers that can be written as the product of two other n-gonal numbers. In 2003, Beardon [2] studied the integer solutions (n, a, b, c, d) of the Diophantine system

$$P(n) = P(a) + P(b) = P(c) - P(d), \quad P(a)P(b)P(c)P(d) \neq 0,$$

where P is a quadratic polynomial with integer coefficients. Some related information on n-gonal numbers could be found in [6, p.1–p.39].

The Diophantine equations about the product or sum of two other polynomials were studied by many authors, we can refer to [15–22] and the references in there.

A natural question is to consider the integer solutions of the Diophantine system

$$f(z) = f(x) + f(y) = f(u) - f(v) = f(p)f(q), \tag{1.1}$$

where $f(X)$ is a polynomial with rational coefficients and $\deg f \geq 2$.

By the theory of Pellian equation, we have the following result.

Theorem 1.1 *For $f(X) = X(X+a)$ with nonzero integers $a \equiv 0, 1, 4 \pmod 5$, Diophantine system (1.1) has infinitely many integer solutions (z, x, y, u, v, p, q).*

By the method of Theorem 1.1, we can get the same result for $a = 2, 3$ (see Remark 2.2), but we couldn't give a complete proof for the cases $a \equiv 2, 3 \pmod 5$. Motivated by the solutions of Theorem 1.1, we obtain the following result by the method of undetermined coefficients.

Theorem 1.2 *For $f(X) = X(X+a)$ with nonzero integers a, if there are integers m, n, k such that*

$$\begin{cases} (n^2-m^2)(4mnk(k+a+1) + a(m^2+2mn-n^2)) & \equiv 0 \pmod{(m^2+n^2)^2}, \\ (m^2+2mn-n^2)((m^2-2mn-n^2)k(k+a+1) - 2amn) & \equiv 0 \pmod{(m^2+n^2)^2}, \end{cases}$$

where $k \equiv 0 \pmod 4$ when a is even, and $k \equiv 2 \pmod 4$ when a is odd. Then Diophantine system (1.1) has an integer parametric solution.

By some computer-aided computation, for $1 \leq a \leq 100$ we can find integers m, n, k satisfying the above congruences. It seems that for any given nonzero integer a, there exists such integers m, n, k. However, we cannot prove it.

To study the integer solutions of Diophantine system (1.1) seems difficult for general polynomials $f(X)$ with $\deg f \geq 3$, so we turn to consider the rational parametric solutions of the Diophantine system

$$f(z) = f(x) + f(y) = f(u) - f(v) = f(p)f(q) = \frac{f(r)}{f(s)}. \tag{1.2}$$

For reducible quadratic polynomials we prove the following statement.

Theorem 1.3 *For $f(X) = X(X + a)$ with nonzero rational number a, Diophantine system (1.2) has a five-parameter rational solution.*

For reducible cubic polynomials, by the theory of elliptic curves, we have:

Theorem 1.4 *For $f(X) = X(X + a)(X + b)$ with nonzero integers a, b and $a \neq b$, Diophantine system (1.2) has infinitely many rational parametric solutions.*

2 The proofs of theorems

Proof of Theorem 1.1. (1) The cases $a \equiv 0, 1 \pmod 5$. Let us start with the equation $f(z) = f(p)f(q)$, where $f(X) = X(X + a)$. We can use the Runge's method [13] to study the integer solutions of it. Write $q = p + k$ for some integer k, then we obtain

$$(2z + a)^2 = 4p(p + a)(p + k)(p + k + a) + a^2.$$

The polynomial part of the Puiseux expansion of

$$\sqrt{4p(p + a)(p + k)(p + k + a) + a^2}$$

is given by $2p^2 + 2(a + k)p + ak$. If there exists a large integer solution, then

$$2z + a = 2p^2 + 2(a + k)p + ak.$$

We get in this case that $a^2(k + 1)(k - 1) = 0$, that is $k = \pm 1$. Hence, $q = p \pm 1$. If $k = 1$, then we obtain the solutions $z = p^2 + (a + 1)p$, or $-p^2 + (-a - 1)p - a$. If $k = -1$, then we get $z = p^2 + (a - 1)p - a$, or $-p^2 + (-a + 1)p$.

Let us deal with the equation $f(z) = f(x) + f(y)$, where $z = p^2 + (a + 1)p$ (we only consider this solution, the other should work in a similar way). We obtain

$$(2(p^2 + (a + 1)p) + a)^2 = (2x + a)^2 + (2y + a)^2 - a^2.$$

Take $y = x + b$ for some integer b. It follows that

$$(2(p^2 + (a + 1)p) + a)^2 - 2(2x + a + b)^2 = 2b^2 - a^2.$$

Let $X = 2(p^2 + (a + 1)p) + a$, $Y = 2x + a + b$, we get the Pellian equation

$$X^2 - 2Y^2 = 2b^2 - a^2. \tag{2.1}$$

It is easy to provide infinitely many integer solutions by the formula

$$X + Y\sqrt{2} = (1 + \sqrt{2})^{2m+1}(a + b\sqrt{2}),\ m \in \mathbb{Z}. \tag{2.2}$$

When $m = 0$, it yields the trivial solution with $x = 0$. When $m = 1$, we get

$$2x + a + b = 5a + 7b, \quad 2(p^2 + (a+1)p) + a = 7a + 10b,$$

then $x = 2a + 3b$ and

$$b = \frac{p^2 + (a+1)p - 3a}{5}.$$

Here b need to be an integer, which is in the cases when $a \equiv 0 \pmod 5$, $p \equiv 0, 4 \pmod 5$, or $a \equiv 1 \pmod 5$, $p \equiv 1, 2 \pmod 5$.

Up to now we constructed infinitely many integer solutions of the equations

$$f(z) = f(x) + f(y) = f(p)f(q),$$

so it remains to consider the case $f(z) = f(u) - f(v)$, where $z = p^2 + (a+1)p$. Let $v = u - c$ for some integer c. Then $f(z) = c(2u + a - c)$, a linear equation in u. Hence,

$$u = \frac{z^2 + az + c^2 - ac}{2c}.$$

As a solution, fix $p = 2c$ and we obtain

$$\begin{aligned} u &= (4c^2 + 2ac + a + 4c)(2c + a) + \frac{a + 5c}{2}, \\ v &= (4c^2 + 2ac + a + 4c)(2c + a) + \frac{a + 3c}{2}, \\ z &= 2c(2c + a + 1). \end{aligned}$$

According to the other variables we have

$$\begin{aligned} p &= 2c, \\ q &= 2c + 1, \\ x &= 2a + \frac{3(4c^2 + 2ac - 3a + 2c)}{5}, \\ y &= 2a + \frac{4(4c^2 + 2ac - 3a + 2c)}{5}. \end{aligned}$$

To get integral values of x, y, u, v, we need the following conditions:

$$a \equiv c \pmod 2$$

and

$$4c^2 + 2ac - 3a + 2c \equiv 0 \pmod 5.$$

(i) Case $a \equiv 0 \pmod 5$, $p \equiv 0, 4 \pmod 5$. From the second condition we have

$$c \equiv 0, 2 \pmod 5.$$

From the first condition we get

$$a \equiv 0 \pmod{10}, \quad c \equiv 0, 2 \pmod{10},$$

and

$$a \equiv 5 \pmod{10}, \quad c \equiv 5, 7 \pmod{10}.$$

For $a \equiv 0 \pmod{10}$, take $c = 10t$, or $10t + 2$, where t is an integer parameter, we have

$$b = 80t^2 + 4t + 4at - \frac{3a}{5} \quad \text{or} \quad 80t^2 + 36t + 4 + 4at + \frac{a}{5} \in \mathbb{Z}.$$

For $a \equiv 5 \pmod{10}$, put $c = 10t + 5$, or $10t + 7$, we get

$$b = 80t^2 + 84t + 22 + 4at + \frac{7a}{5} \quad \text{or} \quad 80t^2 + 116t + 42 + 4at + \frac{11a}{5} \in \mathbb{Z}.$$

(ii) Case $a \equiv 1 \pmod 5$, $p \equiv 1, 2 \pmod 5$. From the second condition we have

$$c \equiv 1, 3 \pmod 5.$$

As above, for $a \equiv 1 \pmod{10}$, take $c = 10t+1$, or $10t+3$, where t is an integer parameter, we have

$$b = 80t^2 + 20t + 1 + 4at + \frac{1-a}{5}, \quad \text{or} \quad 80t^2 + 52t + 8 + 4at + \frac{2+3a}{5} \in \mathbb{Z}.$$

For $a \equiv 6 \pmod{10}$, put $c = 10t + 6$, or $10t + 8$, we get

$$b = 80t^2 + 100t + 31 + 4at + \frac{1+9a}{5}, \quad \text{or} \quad 80t^2 + 132t + 54 + 4at + \frac{2+13a}{5} \in \mathbb{Z}.$$

(2) Case $a \equiv 4 \pmod 5$. Let us note that Pellian equation (2.1) has another family of integer solutions

$$X + Y\sqrt{2} = (1+\sqrt{2})^{2m+1}(-a + b\sqrt{2}), \; m \in \mathbb{Z}. \tag{2.3}$$

When $m = 1$, we get

$$2x + a + b = -5a + 7b, \quad 2(p^2 + (a+1)p) + a = -7a + 10b,$$

then $x = -3a + 3b$ and

$$b = \frac{p^2 + (a+1)p + 4a}{5}.$$

Here b need to be an integer, which is in the cases when $a \equiv 0 \pmod 5$, $p \equiv 0, 4 \pmod 5$, or $a \equiv 4 \pmod 5$, $p \equiv 2, 3 \pmod 5$. We only consider the case $a \equiv 4 \pmod 5$ in the following.

As in part (1), taking $p = 2c - 1$ in $z = p^2 + (a+1)p$ gives

$$\begin{aligned}
z &= (2c-1)(2c+a),\\
x &= -3a + \frac{3(4c^2 + 2ac + 3a - 2c)}{5},\\
y &= -3a + \frac{4(4c^2 + 2ac + 3a - 2c)}{5},\\
u &= (4c^2 + 2ac - a - 4c)(2c+a) + \frac{a+5c}{2},\\
v &= (4c^2 + 2ac - a - 4c)(2c+a) + \frac{a+3c}{2},\\
p &= 2c - 1,\\
q &= 2c.
\end{aligned}$$

To get integral values of x, y, u, v, we need the conditions

$$a \equiv c \pmod 2$$

and

$$4c^2 + 2ac + 3a - 2c \equiv 0 \pmod 5.$$

If $a \equiv 4 \pmod 5$, $p \equiv 2, 3 \pmod 5$, from the second condition we have

$$c \equiv 2, 4 \pmod 5.$$

As above, we can take $c = 10t+2$, or $10t+4$ for $a \equiv 4 \pmod{10}$, and $c = 10t+7$, or $10t+9$ for $a \equiv 9 \pmod{10}$, where t is an integer parameter.

Combining (1) and (2) completes the proof of Theorem 1.1. $\square$

Example 2.1 When $a = 1$, $c = 10t + 1$, then for $f(X) = X(X + 1)$ Diophantine system (1.1) has an integer parameter solution:

$$\begin{aligned}
&z = 400t^2 + 120t + 8,\\
&x = 240t^2 + 72t + 5, \quad y = 320t^2 + 96t + 6,\\
&u = 8000t^3 + 4000t^2 + 665t + 36, \quad v = 8000t^3 + 4000t^2 + 655t + 35,\\
&p = 20t + 2, \quad q = 20t + 3,
\end{aligned}$$

where t is an integer parameter. There are solutions not covered by the above solutions, such as

$$\begin{aligned}
(z, x, y, u, v, p, q) =&(3, 2, 2, 6, 5, 1, 2), (8, 5, 6, 13, 10, 2, 3),\\
&(15, 5, 14, 26, 21, 3, 4), (15, 5, 14, 41, 38, 3, 4),\\
&(48, 29, 38, 66, 45, 6, 7), (48, 29, 38, 81, 65, 6, 7),\\
&(80, 30, 74, 91, 43, 8, 9), (80, 30, 74, 94, 49, 8, 9).
\end{aligned}$$

It seems to be difficult to determine the complete integer solutions of Diophantine system (1.1) for $f(X) = X(X + a)$ with fixed a.

Remark 2.2 It's worth to note that we have other possibilities to obtain integer solutions if $a \not\equiv 0, 1, 4 \pmod 5$. When we apply the same idea using the other family of solutions with $z = -p^2 + (-a - 1)p - a$, $p^2 + (a - 1)p - a$, or $-p^2 + (-a + 1)p$ for $m = 1$, we do not obtain new cases of solutions.

To cover more classes one has to go in these directions. When $m = 2$, from formula (2.2), we have

$$2x + a + b = 29a + 41b, \quad 2(p^2 + (a + 1)p) + a = 41a + 58b,$$

then $x = 14a + 20b$ and

$$b = \frac{p^2 + (a + 1)p - 20a}{29}.$$

To make b be an integer, we get

$$a \equiv 0, 2, 3, 5, 6, 8, 10, 11, 15, 19, 23, 24, 26, 28 \pmod{29}.$$

As in Theorem 1.1, fix $p = 2c$ in $z = p^2 + (a+1)p$ and we obtain

$$\begin{aligned}
z &= 2c(2c+a+1),\\
x &= 14a + 20\frac{4c^2+2ac-20a+2c}{29},\\
y &= 14a + 21\frac{4c^2+2ac-20a+2c}{29},\\
u &= (4c^2+2ac+a+4c)(2c+a) + \frac{a+5c}{2},\\
v &= (4c^2+2ac+a+4c)(2c+a) + \frac{a+3c}{2},\\
p &= 2c,\\
q &= 2c+1.
\end{aligned}$$

To get integral values of x, y, u, v, we need the following conditions:

$$a \equiv c \pmod 2$$

and

$$4c^2+2ac-20a+2c \equiv 0 \pmod{29}.$$

For $a = 2$, take $c = 58t + 46$, or $58t + 54$, then

$$b = 4(29t+25)(4t+3), \text{ or } 4(t+1)(116t+103) \in \mathbb{Z}.$$

For $a = 3$, take $c = 58t + 3$, or $58t + 53$, then

$$b = 16t(29t+4), \text{ or } 16(t+1)(29t+25) \in \mathbb{Z}.$$

Similar congruences can be obtained for other values of m, and combining these systems via the Chinese remainder theorem would cover almost all classes. However, it seems difficult to cover all integers $a \equiv 2, 3 \pmod 5$.

Note that Pellian equation (2.1) has integer solutions given by

$$X + Y\sqrt{2} = (1+\sqrt{2})^{2m+1}(\pm a \pm b\sqrt{2}),\ m \in \mathbb{Z},$$

which including formulas (2.2) and (2.3). When $m = 1, 2, 3, 4, 5$, by applying the method of proof of Theorem 1.1 we are not able to handle the case $a = 83$ in the range $1 \le a \le 100$. However, we can show that the approach of Theorem 1.2 solves this case in Example 2.3.

We try to generalize the formulas obtained in Example 2.1 and give the proof of Theorem 1.2.

Proof of Theorem 1.2. First, we study the equation $f(z) = f(p)f(q)$ for $f(X) = X(X+a)$. Take

$$p = At + k, \quad q = At + k + 1,$$

then we have

$$z = (At+k)(At+k+a+1).$$

Second, we consider the equation $f(z) = f(u) - f(v)$. Let

$$u = Bt^3 + Ct^2 + Dt + E, \quad v = Bt^3 + Ct^2 + Ft + G,$$

then

$$\begin{aligned}&(At+k)(At+k+a)(At+k+1+a)(At+k+1)\\&\quad=(Dt-Ft+E-G)(2Bt^3+2Ct^2+Dt+Ft+E+G+a).\end{aligned}$$

To determinate the coefficients of u, v, by the method of undetermined coefficients, we obtain

$$\begin{aligned}A^4&=2B(D-F),\\2A^3(a+2k+1)&=2BE-2BG+2CD-2CF,\\A^2(a^2+6ak+6k^2+3a+6k+1)&=2CE-2CG+D^2-F^2,\\A(a+2k+1)(2ak+2k^2+a+2k)&=2DE+Da-2FG-Fa,\\k(k+1)(a+k+1)(a+k)&=(E-G)(E+a+G).\end{aligned}\tag{2.4}$$

In order to find a solution of (2.4), let $B=A^3$, $E-G=\frac{k}{2}$, then

$$F=D-\frac{A}{2},\quad G=E-\frac{k}{2}.$$

Put B, F, G into (2.4), and solve it for C, D, E, we get

$$\begin{aligned}C&=A^2(2a+3k+2),\\D&=A(a^2+4ak+3k^2+3a+4k)+\frac{5A}{4},\\E&=(ak+k^2+a+2k)(a+k)+\frac{2a+5k}{4}.\end{aligned}$$

Hence,

$$\begin{aligned}u=&A^3t^3+A^2(2a+3k+2)t^2+\left(A(a^2+4ak+3k^2+3a+4k)+\frac{5A}{4}\right)t\\&+(ak+k^2+a+2k)(a+k)+\frac{2a+5k}{4},\\v=&A^3t^3+A^2(2a+3k+2)t^2+\left(A(a^2+4ak+3k^2+3a+4k)+\frac{3A}{4}\right)t\\&+(ak+k^2+a+2k)(a+k)+\frac{2a+3k}{4}.\end{aligned}$$

At last, we study the equation $f(z)=f(x)+f(y)$. Put

$$x=Ht^2+It+J,\quad y=Kt^2+Lt+M,$$

then

$$\begin{aligned}&(At+k)(At+k+a)(At+k+1+a)(At+k+1)\\&\quad=(H^2+K^2)t^4+(2IH+2KL)t^3+(2HJ+Ha+2KM+Ka+L^2-I^2)t^2\\&\qquad+(2IJ+2LM+La+Ia)t+J^2+Ja+M^2+Ma.\end{aligned}$$

To determine the coefficients of x, y, by the method of undetermined coefficients, we obtain

$$
\begin{aligned}
A^4 &= H^2 + K^2,\\
2A^3(a+2k+1) &= 2IH + 2KL,\\
A^2(a^2+6ak+6k^2+3a+6k+1) &= 2HJ + Ha + 2KM + Ka + L^2 - I^2,\\
A(a+2k+1)(2ak+2k^2+a+2k) &= 2IJ + 2LM + La + Ia,\\
k(k+1)(a+k+1)(a+k) &= J^2 + Ja + M^2 + Ma.
\end{aligned}
\tag{2.5}
$$

Solve the first equation of (2.5), we get an integer parametric solution

$$A = n^2 + m^2, \quad H = 4nm(n^2 - m^2), \quad K = m^4 - 6m^2n^2 + n^4,$$

where $n > m$ are integer parameters. Take A, H, K into the second, third and fourth equations of (2.5), and solve them for I, L, M, then

$$
\begin{aligned}
I &= \frac{4nm(n^2-m^2)(a+2k+1)}{n^2+m^2},\\
L &= \frac{(m^4-6m^2n^2+n^4)(a+2k+1)}{n^2+m^2},\\
M &= \frac{4nm(n^2-m^2)J + (m^2+n^2)^2k^2 + (m^2+n^2)^2(a+1)k + 2amn(m^2+2mn-n^2)}{m^4-6m^2n^2+n^4}.
\end{aligned}
$$

Put M into the firth equation of (2.5), we have

$$J = \frac{(n^2-m^2)(4mnk(k+a+1) + a(m^2+2mn-n^2))}{(n^2+m^2)^2}.$$

Hence,

$$M = \frac{(m^2+2mn-n^2)((m^2-2mn-n^2)k(k+a+1) - 2amn)}{(n^2+m^2)^2}.$$

So

$$
\begin{aligned}
x &= 4nm(n^2-m^2)t^2 + \frac{4nm(n^2-m^2)(a+2k+1)}{n^2+m^2}t\\
&\quad + \frac{(n^2-m^2)(4mnk(k+a+1) + a(m^2+2mn-n^2))}{(n^2+m^2)^2},\\
y &= (m^4-6m^2n^2+n^4)t^2 + \frac{(m^4-6m^2n^2+n^4)(a+2k+1)}{n^2+m^2}t\\
&\quad + \frac{(m^2+2mn-n^2)((m^2-2mn-n^2)k(k+a+1) - 2amn)}{(n^2+m^2)^2}.
\end{aligned}
$$

According to the other variables, we have

$$
\begin{aligned}
p &= (n^2+m^2)t + k,\\
q &= (n^2+m^2)t + k + 1,\\
u &= (n^2+m^2)^3t^3 + (n^2+m^2)^2(2a+3k+2)t^2 + \Big((n^2+m^2)(a^2+4ak\\
&\quad +3k^2+3a+4k) + \frac{5(n^2+m^2)}{4}\Big)t + (ak+k^2+a+2k)(a+k) + \frac{2a+5k}{4},
\end{aligned}
$$

$$v=(n^2+m^2)^3t^3+(n^2+m^2)^2(2a+3k+2)t^2+\Big((n^2+m^2)(a^2+4ak+3k^2+3a+4k)+\frac{3(n^2+m^2)}{4}\Big)t+(ak+k^2+a+2k)(a+k)+\frac{2a+3k}{4}.$$

To get integral values of x, y, u, v, we can take $t=4(n^2+m^2)T$, where T is an integer parameter, $k\equiv 0 \pmod 4$ when a is even, and $k\equiv 2 \pmod 4$ when a is odd and get the following congruence conditions:

$$\begin{cases}(n^2-m^2)(4mnk(k+a+1)+a(m^2+2mn-n^2)) & \equiv 0 \pmod{(m^2+n^2)^2},\\ (m^2+2mn-n^2)((m^2-2mn-n^2)k(k+a+1)-2amn) & \equiv 0 \pmod{(m^2+n^2)^2}.\end{cases}$$

This completes the proof of Theorem 1.2. ◻

Example 2.3 When $a=83$, $f(X)=X(X+83)$, take $(m,n)=(1,9)$, $t=328T, k=4k_1+2$, then we have the conditions:

$$\begin{cases}46080k_1^2+1013760k_1+83680 & \equiv 0 \pmod{6724},\\ 97216k_1^2+2138752k_1+1137700 & \equiv 0 \pmod{6724}.\end{cases}$$

Solve these two congruences, we obtain

$$k_1\equiv 119, 1800, 1540, 3221, 3481, 4902, 5162, 6583 \pmod{6724}.$$

Then

$$k\equiv 478, 6162 \pmod{6724}.$$

If we set $k=6724S+478$, where S is an integer parameter, then for $f(X)=X(X+83)$ Diophantine system (1.1) has an integer parametric solution:

$$\begin{aligned}
z&=4(13448T+3362S+239)(13448T+281+3362S),\\
x&=309841920T^2+(154920960S+11980800)T+19365120S^2+2995200S\\
&\quad+115000,\\
y&=653680384T^2+(326840192S+25276160)T+40855024S^2+6319040S\\
&\quad+242761,\\
u&=19456426971136T^3+(14592320228352S+1158878495232)T^2\\
&\quad+(3648080057088S^2+579439247616S+22947647028)T+304006671424S^3\\
&\quad+72429905952S^2+5736911757S+151020156,\\
v&=(53792T+1123+13448S)(22606088S^2+180848704ST+361697408T^2\\
&\quad+3498161S+13992644T+134479),\\
p&=26896T+6724S+478,\\
q&=26896T+6724S+479.
\end{aligned}$$

By the parametrization of quadratic equation, we give the proof of Theorem 1.3 in the following.

Proof of Theorem 1.3. For $f(X)=X(X+a)$, let $z=T$, the first equation of Diophantine system (1.2) reduces to

$$T(T+a)=x(x+a)+y(y+a).$$

This can be parameterized by

$$x=-\frac{2Tk+ak+a}{k^2+1},\quad y=-\frac{(k+1)(Tk+ak-T)}{k^2+1},$$

where k is a rational parameter.

From $T(T+a)=u(u+a)-v(v+a)$, we get

$$u=-\frac{Tt^2+at^2-at+T}{t^2-1},\quad v=-\frac{2Tt+at-a}{t^2-1},$$

where t is a rational parameter.

For $T(T+a)=p(p+a)q(q+a)$, put $p=wT$, then

$$T=-\frac{a(aqw+q^2w-1)}{aqw^2+q^2w^2-1},\quad p=-\frac{aw(aqw+q^2w-1)}{aqw^2+q^2w^2-1},$$

where w is a rational parameter.

Take $s=mr$, from

$$T(T+a)=\frac{r(r+a)}{s(s+a)},$$

we obtain

$$r=-\frac{a(T^2m+Tam-1)}{T^2m^2+Tam^2-1},\quad s=-\frac{am(T^2m+Tam-1)}{T^2m^2+Tam^2-1},$$

where m is a rational parameter.

Put

$$T=-\frac{a(aqw+q^2w-1)}{aqw^2+q^2w^2-1}$$

into x, y, u, v, r, s, then Diophantine system (1.2) has a five-parameter rational solution. □

By the theory of elliptic curves, we provide the proof of Theorem 1.4.

Proof of Theorem 1.4. To prove this theorem, we need to consider four Diophantine equations. The first one is

$$z(z+a)(z+b)=x(x+a)(x+b)+y(y+a)(y+b). \tag{2.6}$$

Let $z=T$, and consider (2.6) as a cubic curve with variables x, y:

$$C_1: \ x(x+a)(x+b)+y(y+a)(y+b)-T(T+a)(T+b)=0.$$

By the method described in [4, p. 477], using Magma [3], C_1 is birationally equivalent to the elliptic curve

$$\begin{aligned}E_1: \ Y^2=&X^3-432(a^2-ab+b^2)^2X-314928T^6-629856(a+b)T^5\\&-314928(a^2+4ab+b^2)T^4+23328(a+b)(4a^2-37ab+4b^2)T^3\\&+1164(8a^4-4a^3b-51a^2b^2-4ab^3+8b^4)T^2+46656ab(2a-b)(a-2b)\\&\times(a+b)T-1728(a^2-4ab+b^2)(a^2+2ab-2b^2)(2a^2-2ab-b^2).\end{aligned}$$

The map $\varphi_1 : C_1 \to E_1$ is

$$X = \frac{12(3(a^2-ab+b^2)(x+y)+27T(T+a)(T+b)-2(a+b)(a^2-4ab+b^2))}{2a+2b+3x+3y},$$
$$Y = \frac{108(3T+2a-b)(3T+2a+2b)(3T-a+2b)(x-y)}{2a+2b+3x+3y},$$

and its inverse map $\varphi_1^{-1} : E_1 \to C_1$ is

$$x = \frac{-6(a+b)X+972T(T+a)(T+b)-72(a+b)(a^2-4ab+b^2)+Y}{18(X-12a^2+12ab-12b^2)},$$
$$y = \frac{-6(a+b)X+972T(T+a)(T+b)-72(a+b)(a^2-4ab+b^2)-Y}{18(X-12a^2+12ab-12b^2)}.$$

The discriminant of E_1 is nonzero as an element of $\mathbb{Q}(T)$, then E_1 is smooth.

Note that the point $(x, y) = (0, T)$ lies on C_1, by the map φ_1, the corresponding point on E_1 is

$$W = (108T^2+36(a+b)T-12a^2+48ab-12b^2, \quad -108(3T-b+2a)(3T+2b-a)T).$$

By the group law, we have

$$\begin{aligned}[2]W = \Big(& 12(9T^4+12(a+b)T^3+(5a^2+16ab+5b^2)T^2+6ab(a+b)T+3a^2b^2)/T^2,\\ & 108(9T^6+21(a+b)T^5+(16a^2+41ab+16b^2)T^4\\ & +2(a+b)(2a^2+13ab+2b^2)T^3+2ab(4a^2+11ab+4b^2)T^2\\ & +6a^2b^2(a+b)T+2a^3b^3)/T^3\Big).\end{aligned}$$

An easy computation reveals that the remainder of the division of the numerator by the denominator of the X-th coordinate of $[2]W$ with respect to T is equal to

$$(72a^2b+72ab^2)T+36a^2b^2$$

and thus is nonzero as an element of $\mathbb{Q}(T)$ provided $ab \neq 0$. By a generalization of Nagell–Lutz theorem (see [5, p.268]), $[2]W$ is of infinite order on E_1, then there are infinitely many $\mathbb{Q}(T)$-rational points on E_1.

For $m = 2, 3, \ldots,$ compute the points $[m]W$ on E_1, next calculate the corresponding point $\varphi_1^{-1}([m]W) = (x_m, y_m)$ on C_1. Then we get infinitely many $\mathbb{Q}(T)$-rational solutions (x, y) of (2.6).

The second one is

$$z(z+a)(z+b) = u(u+a)(u+b) - v(v+a)(v+b). \tag{2.7}$$

Take $z = T$, and consider (2.7) as a cubic curve with variables u, v:

$$C_2 : \ u(u+a)(u+b) - v(v+a)(v+b) - T(T+a)(T+b) = 0.$$

As (2.6), C_2 is birationally equivalent with the elliptic curve

$$E_2:\ V^2 = U^3 - 432(a^2 - ab + b^2)^2 U - 314928T^6 - 629856(a+b)T^5 - 314928(a^2 + 4ab + b^2)T^4 - 629856ab(a+b)T^3 - 314928a^2b^2T^2 + 3456(a^2 - ab + b^2)^3.$$

The map $\varphi_2 : C_2 \to E_2$ is

$$U = \frac{12((a^2 - ab + b^2)(u - v) + 9T(T+a)(T+b))}{u - v},$$
$$V = \frac{324T(T+a)(T+b)(2a + 2b + 3u + 3v)}{u - v},$$

and its inverse map $\varphi_2^{-1} : E_2 \to C_2$ is

$$u = \frac{-6(a+b)U + V + 72(a^3 + b^3) + 972T(T+a)(T+b)}{18(U - 12a^2 + 12ab - 12b^2)},$$
$$v = \frac{-6(a+b)U + V + 72(a^3 + b^3) - 972T(T+a)(T+b)}{18(U - 12a^2 + 12ab - 12b^2)}.$$

The discriminant of E_2 is nonzero as an element of $\mathbb{Q}(T)$, then E_2 is smooth.

It is easy to see that the point $(u, v) = (T, 0)$ lies on C_2, by the map φ_2, the corresponding point on E_2 is

$$W' = (108T^2 + 108(a+b)T + 12a^2 + 96ab + 12b^2, 324(T+a)(T+b)(3T + 2a + 2b)).$$

By the group law, we get

$$[2]W' = \Big(12(81T^4 + 108(a+b)T^3 + (45a^2 + 144ab + 45b^2)T^2 + (12a^3 + 54a^2b + 54ab^2 + 12b^3)T + 4a^4 + 4a^3b + 27a^2b^2 + 4ab^3 + 4b^4)/(3T + 2a + 2b)^2, - 324(81T^6 + 135(a+b)T^5 + (54a^2 + 189ab + 54b^2)T^4 - (12a^3 - 18a^2b - 18ab^2 + 12b^3)T^3 - (8a^4 + 68a^3b + 66a^2b^2 + 68ab^3 + 8b^4)T^2 - 6ab \times (a+b)(4a^2 + 5ab + 4b^2)T - 6a^2b^2(2a^2 + ab + 2b^2))/(3T + 2a + 2b)^3\Big).$$

Using the same method as above, there are infinitely many $\mathbb{Q}(T)$-rational solutions (u, v) of (2.7).

The third one is

$$z(z+a)(z+b) = p(p+a)(p+b)q(q+a)(q+b). \tag{2.8}$$

Put $z = T$, $q(q+a)(q+b) = Q$ and consider (2.8) as a cubic curve with variables T, p:

$$C_3:\ T(T+a)(T+b) - Qp(p+a)(p+b) = 0.$$

As (2.6), C_3 is birationally equivalent to the elliptic curve

$$E_3:\ Y^2 = X^3 - 432(a^2 - ab + b^2)^2Q^2X + 432Q^2(27a^2b^2(a-b)^2Q^2 + 2(2a-b)^2(a-2b)^2(a+b)^2Q + 27a^2b^2(a-b)^2).$$

Because the map $\varphi_3 : C_3 \to E_3$ is complicated, we omit it. The discriminant of E_3 is nonzero as an element of $\mathbb{Q}(Q)$, then E_3 is smooth.

Note that the point $(T, p) = (-a, -a)$ lies on C_3, by the map φ_3, the corresponding point on E_3 is

$$W'' = (12(a^2 + 2ab - 2b^2)Q, \quad -108ab(a - b)Q(Q + 1)).$$

By the group law, we get

$$\begin{aligned}[2]W'' = \Big(& -12Q(2a^2(a^2 + 2ab - 2b^2)Q^2 - (8a^4 + 4a^3b - a^2b^2 - 6ab^3 + 3b^4)Q \\ & + 2a^2(a^2 + 2ab - 2b^2))/((Q + 1)^2a^2), \\ & 108Q(a^4b(a - b)Q^4 - 2a^2(2a^4 + 3a^3b - a^2b^2 - 4ab^3 + 2b^4)Q^3 \\ & + 2(a^2 + ab - b^2)(4a^4 + a^3b - 2ab^3 + b^4)Q^2 - 2a^2(2a^4 + 3a^3b - a^2b^2 \\ & - 4ab^3 + 2b^4)Q + a^4b(a - b))/((Q + 1)^3a^3)\Big).\end{aligned}$$

Using the same method as above, we have infinitely many $\mathbb{Q}(Q)$-rational solutions (T, p) of (2.8).

The last one is

$$z(z + a)(z + b) = \frac{r(r + a)(r + b)}{s(s + a)(s + b)}. \tag{2.9}$$

Let $z = T$, and put $t = T(T + a)(T + b)$. By (2.8), there are infinitely many $\mathbb{Q}(t)$-rational solutions (r, s) of (2.9). This completes the proof of Theorem 1.4. □

3 Some related questions

In 1986, Hirose [10] conjectured that for $n \neq 4$ if $(n - 2)P_k^n - (n - 4) = 2P_l^n$, then $P_{P_k^n}^n = P_k^n P_l^n$ can be expressed as the sum and difference of two other n-gonal numbers. It is difficult to prove it. Following this idea, for $n = 12$, we find an example:

$$\begin{aligned}P^{12}_{215666848} &= P^{12}_{33841736} + P^{12}_{212995132} \\ &= P^{12}_{2907011822107606} - P^{12}_{2907011822107598} \\ &= P^{12}_{6568} P^{12}_{14686}.\end{aligned}$$

For general n-gonal numbers, the following question is still open.

Question 3.1 *Are there infinitely many n-gonal numbers, except $n = 3, 4, 5, 6, 8$, which at the same time can be written as the sum, difference, and product of other n-gonal numbers?*

In Theorem 1.1, we give infinitely many quadratic polynomials $f(X) \in \mathbb{Q}[X]$ such that Diophantine system (1.1) has infinitely many integer solutions, but it seems difficult to solve the following question.

Question 3.2 *Does there exist a polynomial $f(X) \in \mathbb{Q}[X]$ with $\deg f \geq 3$ such that Diophantine system (1.1) or (1.2) has infinitely many integer solutions?*

For polynomials $f(X) \in \mathbb{Q}[X]$ with $\deg f \geq 4$, we have

Question 3.3 *Does there exist a polynomial $f(X) \in \mathbb{Q}[X]$ with $\deg f \geq 4$ such that Diophantine system (1.1) or (1.2) has a nontrivial rational solution?*

References

1. S. Ando, A note on polygonal numbers. Fibonacci Q. **19**, 180–183 (1981)
2. A. Beardon, Sums and differences of values of a quadratic polynomial. Fibonacci Q. **41**, 372–373 (2003)
3. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symb. Comput. **24**, 235–265 (1997)
4. H. Cohen, *Number Theory, Vol. I: Tools and Diophantine Equations*, Graduate Texts in Mathematics (Springer, New York, 2007)
5. I. Connell, *Elliptic curve handbook* (1998). https://pendientedemigracion.ucm.es/BUCM/mat/doc8354.pdf
6. L.E. Dickson, *History of the Theory of Numbers, Vol II: Diophantine Analysis* (Dover Publications, New York, 2005)
7. L.C. Eggan, P.C. Eggan, J.L. Selfridge, Polygonal products of polygonal numbers and the Pell equation. Fibonacci Q. **20**, 24–28 (1982)
8. R.T. Hansen, Arithmetic of pentagonal numbers. Fibonacci Q. **8**, 83–87 (1970)
9. H.J. Hindin, A theorem concerning heptagonal numbers. Fibonacci Q. **18**, 258–259 (1980)
10. S. Hirose, On some polygonal numbers which are, at the same time, the sums, differences, and products of two other polygonal numbers. Fibonacci Q. **24**, 99–106 (1986)
11. W.J. O'Donnell, Two theorems concerning hexagonal numbers. Fibonacci Q. **17**, 77–79 (1979)
12. W.J. O'Donnell, A theorem concerning octagonal numbers. J. Recreat. Math. **12**, 271–272 (1979/80)
13. C. Runge, Üeber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen (German). J. Reine Angew. Math. **100**, 425–435 (1887)
14. W. Sierpiński, Un théorème sur les nombres triangulaires. Elem. Math. **23**, 31–32 (1968). (**French**)
15. S. Tengely, M. Ulas, On products of disjoint blocks of arithmetic progressions and related equations. J. Number Theory **165**, 67–83 (2016)
16. S. Tengely, M. Ulas, Power values of sums of certain products of consecutive integers and related results. J. Number Theory **197**, 341–360 (2019)
17. Y. Zhang, On the Diophantine equation $f(x)f(y) = f(z)^n$ involving Laurent polynomials. Colloq. Math. **151**, 111–122 (2018)
18. Y. Zhang, T. Cai, On the Diophantine equation $f(x)f(y) = f(z^2)$. Publ. Math. Debrecen **82**, 31–41 (2013)
19. Y. Zhang, T. Cai, A note on the Diophantine equation $f(x)f(y) = f(z^2)$. Period. Math. Hung. **70**, 209–215 (2015)
20. Y. Zhang, T. Cai, On products of consecutive arithmetic progressions. J. Number Theory **147**, 287–299 (2015)
21. Y. Zhang, Z.Y. Shen, On the Diophantine system $f(z) = f(x)f(y) = f(u)f(v)$. Period. Math. Hung. **75**, 295–301 (2017)
22. Y. Zhang, A.S. Zargar, On the Diophantine equation $f(x)f(y) = f(z)^n$ involving Laurent polynomials, II. Colloq. Math. **158**, 119–126 (2019)

Affiliations

Yong Zhang[1] · Zhongyan Shen[2]

Zhongyan Shen
huanchenszyan@yahoo.com.cn

[1] School of Mathematics and Statistics, Changsha University of Science and Technology, Hunan Provincial Key Laboratory of Mathematical Modeling and Analysis in Engineering, Changsha 410114, People's Republic of China

[2] Department of Mathematics, Zhejiang International Studies University, Hangzhou 310012, People's Republic of China