COLLOQUIUM MATHEMATICUM

VOL. 142 2016 NO. 2

SOME OBSERVATIONS ON THE DIOPHANTINE EQUATION $f(x)f(y) = f(z)^2$

BY

YONG ZHANG (Changsha and Hangzhou)

Abstract. Let $f \in \mathbb{Q}[X]$ be a polynomial without multiple roots and with $\deg(f) \geq 2$. We give conditions for $f(X) = AX^2 + BX + C$ such that the Diophantine equation $f(x)f(y) = f(z)^2$ has infinitely many nontrivial integer solutions and prove that this equation has a rational parametric solution for infinitely many irreducible cubic polynomials. Moreover, we consider $f(x)f(y) = f(z)^2$ for quartic polynomials.

1. Introduction. Let $f \in \mathbb{Q}[X]$ be a polynomial without multiple roots and with $\deg(f) \geq 2$. Several authors investigated the Diophantine equation

$$f(x)f(y) = f(z)^2. \tag{1.1}$$

We say a rational or integer solution (x, y, z) is *nontrivial* if $f(x) \neq f(y)$. In 1963, A. Schinzel and W. Sierpiński [SS] studied (1.1) for $f(X) = X^2 - 1$ and showed that it has infinitely many nontrivial integer solutions. But it is a difficult problem to determine all the integer solutions of (1.1) for $f(X) = X^2 - 1$. In 1967, K. Szymiczek [S] obtained the same result for $f(X) = X^2 - k^2$, where $k \in \mathbb{Z}$. In 2007, M. A. Bennett [B] showed that (1.1) has no nontrivial integer solution for $f(X) = X^k - 1$, $k \geq 4$.

In 2006, K. Katayama [K] investigated (1.1) for $f(X) = X^2 + 1$ and proved that it has infinitely many nontrivial integer solutions. In 2008, M. Ulas [U2] obtained the same result for $f(X) = X^2 + k$, $k = \pm(a^2 - 2b^2)$, where $a, b \in \mathbb{Z}$. Some related information on equation (1.1) can be found in [G, *D23 Some quartic equations*].

In 2007, M. Ulas [U1] studied the rational solutions of (1.1). He proved that if $f(X) = X^2 + k$, where $k \in \mathbb{Z}$, then (1.1) has infinitely many rational parametric solutions; and if $f(X) = X(X^2 + X + t)$, where $t \in \mathbb{Q}$, then (1.1) has infinitely many rational solutions for all but finitely many t.

In this paper we consider the integer solutions of (1.1) for quadratic polynomials, and rational solutions for cubic and quartic polynomials. By the theory of Pell's equation, we have

2010 *Mathematics Subject Classification*: Primary 11D72, 11D25; Secondary 11D41.
Key words and phrases: Diophantine equation, Pell's equation, integer solutions, rational solutions.

DOI: 10.4064/cm142-2-8

THEOREM 1.1. *Let $f(X) = AX^2 + BX + C$ be a quadratic polynomial without multiple roots, where $A, B, C \in \mathbb{Z}$ and $A \mid B$. Suppose that (x_0, y_0, z_0) is an integer solution of* (1.1) *and $y_0 = x_0 + 2z_0 + B/A$. Then* (1.1) *has infinitely many nontrivial integer solutions.*

M. Ulas raised the following question (see [U1, Question 4.1]): "Does there exist an irreducible polynomial $f \in \mathbb{Q}[X]$ of degree three such that (1.1) has infinitely many rational solutions?" Here we give a positive answer to this question: in fact, there are infinitely many such irreducible cubic polynomials.

THEOREM 1.2. *Let $f(X) = AX^3+BX^2+CX+D$ be a cubic polynomial without multiple roots, where $C = -(p^2+pq+q^2)A-(p+q)B$, $A, B, D, p, q \in \mathbb{Q}$. Then* (1.1) *has a rational parametric solution.*

In particular, we get

COROLLARY 1.3. *Let $f(X) = X^3+BX^2+CX+D$ be a cubic polynomial without multiple roots, where $C = -(p^2+pq+q^2)-(p+q)B$, $B, D, p, q \in \mathbb{Z}$ and $(B+C)D$ is odd. Then $f(X)$ is an irreducible polynomial and* (1.1) *has a rational parametric solution.*

For quartic polynomials it is difficult to give a positive answer to [U1, Question 4.3]. By the same idea of Theorem 1.2, we obtain the following two results.

THEOREM 1.4. *Let $f(X) = AX^4 + BX^3 + CX^2 + DX + E$ be a quartic polynomial without multiple roots, where $A, B, C, D, E \in \mathbb{Q}$. Suppose that there are infinitely many z such that the cubic equation*

$$(1.2)\quad Aw^3 + (Az + B)w^2 + (Az^2 + Bz + C)w + Az^3 + Bz^2 + Cz + D = 0$$

has two distinct rational solutions w. Then (1.1) *has infinitely many rational solutions (x, y, z).*

THEOREM 1.5. *There are infinitely many quartic polynomials without multiple roots such that* (1.1) *has a common rational solution.*

2. Proofs of the theorems. To prove Theorem 1.1, we need the following lemma about the solutions of Pell's equation.

LEMMA 2.1 (see [EES, Theorem 2]). *Let M be an integer and m, D be positive integers, where D is not a perfect square. If the Pell equation*

$$u^2 - Dv^2 = M$$

has an integer solution (u_0, v_0) satisfying

$$(u_0, v_0) \equiv (a, b) \pmod{m},$$

then there are infinitely many integer solutions (u, v) *satisfying*

$$(u, v) \equiv (a, b) \pmod{m}.$$

Proof of Theorem 1.1. Set $B = tA$, where $t \in \mathbb{Z}$. Let

$$y = x + 2z + t. \tag{2.1}$$

Then

$$f(x)f(y) - f(z)^2 = A(x + z + t)^2(Ax^2 + 2Axz + 2tAx + 2C - Az^2) = 0.$$

Considering $Ax^2 + 2Axz + 2tAx + 2C - Az^2 = 0$, we have

$$(Ax + Az + At)^2 - 2(Az + At)^2 = -A^2t^2 - 2AC.$$

Setting $U = Ax + Az + At, V = Az + At$, we get

$$U^2 - 2V^2 = -A^2t^2 - 2AC.$$

Note that the Pell equation

$$U^2 - 2V^2 = 1$$

has infinitely many integer solutions. Furthermore, (x_0, y_0, z_0) is an integer solution of (1.1) satisfying

$$y_0 = x_0 + 2z_0 + \frac{B}{A}.$$

Then the Pell equation

$$U^2 - 2V^2 = -A^2t^2 - 2AC$$

has a solution

$$(U_0, V_0) = (Ax_0 + Az_0 + At, Az_0 + At),$$

which satisfies the condition

$$(U_0, V_0) \equiv (0, 0) \pmod{A}.$$

By Lemma 2.1, there exist infinitely many integer solutions (U, V) satisfying this condition. Then there are infinitely many

$$z = \frac{V}{A} - t \in \mathbb{Z}, \qquad x = \frac{U}{A} - z - t \in \mathbb{Z},$$

and infinitely many integers $y = x + 2z + t$. ∎

When $A = 1$ and $t = 0$, we have $f(X) = X^2 + C$ and (2.1) becomes

$$y = x + 2z \ \Leftrightarrow \ z = \frac{y - x}{2}.$$

If $C = \pm(a^2 - 2b^2)$, our Theorem 1.1 becomes Theorem 2.1 of [U2].

When $A = 2$, $t = 0$, then $f(X) = 2X^2 + C$. If $C \neq \pm 2(a^2 - 2b^2)$, we give some examples in Table 1 with $0 < x, y, z < 1000$. In general, (1.1) has infinitely many integer solutions for $f(X) = 2X^2 + C$ with $C = 2b^2 - a^2$, where $a, b \in \mathbb{Z}$.

Table 1. Some solutions of (1.1) for $f(X) = 2X^2 + C$

C	(x, y, z)
1	$(2, 12, 5), (12, 70, 29), (70, 408, 169), (408, 2378, 985)$
7	$(1, 9, 4), (3, 19, 8), (9, 53, 22), (19, 111, 46), (53, 309, 128), (111, 647, 268)$
23	$(1, 13, 6), (7, 43, 18), (13, 77, 32), (43, 251, 104), (77, 449, 186)$
31	$(3, 23, 10), (5, 33, 14), (23, 135, 56), (33, 193, 80), (135, 787, 326)$
41	$(2, 20, 9), (8, 50, 21), (20, 118, 49), (50, 292, 121), (118, 688, 285)$
47	$(1, 17, 8), (11, 67, 28), (17, 101, 42), (67, 391, 162), (101, 589, 244)$
71	$(5, 37, 16), (7, 47, 20), (37, 217, 90), (47, 275, 114)$
73	$(2, 24, 11), (12, 74, 31), (24, 142, 59), (74, 432, 179), (142, 828, 343)$
79	$(1, 21, 10), (15, 91, 38), (21, 125, 52), (91, 531, 220), (125, 729, 302)$
89	$(4, 34, 15), (10, 64, 27), (34, 200, 83), (64, 374, 155)$
97	$(6, 44, 19), (8, 54, 23), (44, 258, 107), (54, 316, 131)$

When $A = 1$ and $t = 1$, we have $f(X) = X^2 + X + C$ and (2.1) becomes

$$y = x + 2z + 1 \;\Leftrightarrow\; z = \frac{y - x - 1}{2}.$$

For $0 < C \leq 50$, we give some examples in Table 2 with $0 < x, y, z < 1000$. In general, (1.1) has infinitely many integer solutions for $f(X) = X^2+X+C$ with $C = a(a + 1) + 2b(b + 1)$, where $a, b \in \mathbb{Z}$.

Table 2. Some solutions of (1.1) for $f(X) = X^2 + X + C$

C	(x, y, z)
2	$(2, 15, 6), (5, 32, 13), (15, 90, 37), (32, 189, 78), (90, 527, 218)$
6	$(1, 12, 5), (3, 22, 9), (12, 73, 30), (22, 131, 54), (73, 428, 177), (131, 766, 317)$
8	$(6, 39, 16), (9, 56, 23), (39, 230, 95), (56, 329, 136)$
12	$(2, 19, 8), (4, 29, 12), (19, 114, 47), (29, 172, 71), (114, 667, 276)$
16	$(1, 16, 7), (7, 46, 19), (16, 97, 40), (46, 271, 112), (97, 568, 235)$
18	$(10, 63, 26), (13, 80, 33), (63, 370, 153), (80, 469, 194)$
20	$(3, 26, 11), (5, 36, 15), (26, 155, 64), (36, 213, 88), (155, 906, 375)$
26	$(2, 23, 10), (8, 53, 22), (23, 138, 57), (53, 312, 129), (138, 807, 334)$
30	$(1, 20, 9), (4, 33, 14), (6, 43, 18), (11, 70, 29), (20, 121, 50),$
	$(33, 196, 81), (43, 254, 105), (70, 411, 170), (121, 708, 293)$
32	$(14, 87, 36), (17, 104, 43), (87, 510, 211), (104, 609, 252)$
38	$(3, 30, 13), (9, 60, 25), (30, 179, 74), (60, 353, 146)$
42	$(5, 40, 17), (7, 50, 21), (40, 237, 98), (50, 295, 122)$
44	$(2, 27, 12), (12, 77, 32), (27, 162, 67), (77, 452, 187), (162, 947, 392)$
48	$(1, 24, 11), (15, 94, 39), (24, 145, 60), (94, 551, 228), (145, 848, 351)$
50	$(18, 111, 46), (21, 128, 53), (111, 650, 269), (128, 749, 310)$

REMARK 2.2. In fact, for every $t \in \mathbb{Z}$ we can construct infinitely many polynomials $f(X) = AX^2 + tAX + C$ such that (1.1) has infinitely many nontrivial integer solutions. But it is difficult to find an integer solution of (1.1) for $f(X) = AX^2 + tAX + C$ where A, C, t are arbitrary integers.

In the following, we will give the proof of Theorem 1.2, which is simple but nontrivial.

Proof of Theorem 1.2. When $f(X) = AX^3 + BX^2 + CX + D$, where $C = -(p^2 + pq + q^2)A - (p + q)B$, then (1.1) is equivalent to

$$f(x)f(y) - f(z)^2 = A_1 D + A_0,$$

where

$$\begin{aligned} A_1 &= A(x^3 + y^3 - 2z^3) + B(x^2 + y^2 - 2z^2) + C(x + y - 2z), \\ A_0 &= (A^2y^3 + ABy^2 + ACy)x^3 + (ABy^3 + B^2y^2 + BCy)x^2 \\ &\quad + (ACy^3 + BCy^2 + C^2y)x - z^2(Az^2 + Bz + C)^2. \end{aligned}$$

Solving the Diophantine system $A_1 = 0, A_0 = 0$ for x, y, we note that if x and y are the rational roots of the equation

$$Aw^2 + (Az + B)w + Az^2 + Bz + C = 0, \tag{2.2}$$

then the system is satisfied. By the condition $C = -(p^2+pq+q^2)A-(p+q)B$, (2.2) has a solution $(w, z) = (p, q)$. It can be parameterized by

$$\begin{aligned} w &= \frac{pAu^2 + (-2Aq - B)u - pA - Aq - B}{A(u^2 + u + 1)}, \\ z &= -\frac{(Aq + pA + B)u^2 + (2pA + B)u - Aq}{A(u^2 + u + 1)}, \end{aligned}$$

so

$$\begin{aligned} x = w &= \frac{pAu^2 + (-2Aq - B)u - pA - Aq - B}{A(u^2 + u + 1)}, \\ y = -\frac{Az + B}{A} - x &= \frac{qAu^2 + (2pA + 2Aq + B)u + pA}{A(u^2 + u + 1)}. \end{aligned}$$

Therefore, (1.1) has a rational parametric solution (x, y, z). ■

When $(A, B, D) = (1, 1, 0)$, $f(X) = X(X^2 + X - (p^2 + pq + q^2 + p + q))$. Then (1.1) has a rational parametric solution

$$\begin{aligned} (x, y, z) = \bigg(&\frac{pu^2 + (-2q - 1)u - p - q - 1}{u^2 + u + 1}, \frac{qu^2 + (2p + 2q + 1)u + p}{u^2 + u + 1}, \\ &- \frac{(p + q + 1)u^2 + (2p + 1)u - q}{u^2 + u + 1} \bigg). \end{aligned}$$

REMARK 2.3. However, for quadratic polynomials there is no result similar to Theorem 1.2.

Proof of Corollary 1.3. In fact, we only need to prove that $f(X)$ is an irreducible polynomial. This is an easy exercise in algebra. We give the proof for completeness. If $f(X) = X^3 + BX^2 + CX + D$ is reducible, then there exist α, β, γ such that

$$f(X) = (X + \alpha)(X^2 + \beta X + \gamma).$$

So we have $f(0) = \alpha\gamma = D$. Noting that $(B + C)D$ is odd, we see that D is odd and α, γ are also odd. In the formula

$$f(1) = (1 + \alpha)(1 + \beta + \gamma) = 1 + B + C + D,$$

the right hand side is an odd number and the left hand side is an even number, a contradiction. Hence, $f(X)$ is irreducible. The remainder of the proof is a special case of the proof of Theorem 1.2. ∎

When $(B, p, q) = (1, 0, 0)$, we have $f(X) = X^3 + X^2 + D$ and D is an odd number; then $f(X)$ is an irreducible polynomial and (1.1) has a rational parametric solution

$$(x, y, z) = \left(-\frac{u+1}{u^2+u+1}, \frac{u}{u^2+u+1}, -\frac{(u+1)u}{u^2+u+1}\right).$$

This gives an answer to [U1, Question 4.1].

Proof of Theorem 1.4. When $f(X) = AX^4 + BX^3 + CX^2 + DX + E$, (1.1) becomes

$$f(x)f(y) - f(z)^2 = B_1 E + B_0,$$

where

$$\begin{aligned} B_1 &= A(x^4 + y^4 - 2z^4) + B(x^3 + y^3 - 2z^3) \\ &\quad + C(x^2 + y^2 - 2z^2) + D(x + y - 2z), \\ B_0 &= (A^2y^4 + ABy^3 + ACy^2 + ADy)x^4 + (ABy^4 + B^2y^3 + BCy^2 + BDy)x^3 \\ &\quad + (ACy^4 + BCy^3 + C^2y^2 + CDy)x^2 \\ &\quad + (ADy^4 + BDy^3 + CDy^2 + D^2y)x - z^2(Az^3 + Bz^2 + Cz + D)^2. \end{aligned}$$

Solving the Diophantine system $B_1 = 0$, $B_0 = 0$ for x, y, we note that if x and y are the rational roots of equation (1.2), i.e.,

$$Aw^3 + (Az + B)w^2 + (Az^2 + Bz + C)w + Az^3 + Bz^2 + Cz + D = 0,$$

then the system is satisfied. ∎

Proof of Theorem 1.5. Suppose that $f(X) = AX^4 + BX^3 + DX + E$, and let $x = T$, $y = u^2T$, $z = uT$. Then (1.1) is equivalent to

$$f(x)f(y) - f(z)^2 = T(u - 1)^2(C_1 A + C_0),$$

where

$$C_1 = T^3(Bu^6T^3 + Du^2(u^2+u+1)^2T + E(u+1)^2(u^2+1)^2),$$
$$C_0 = BDu^2(u+1)^2T^3 + BE(u^2+u+1)^2T^2 + DE.$$

Solving the Diophantine system $C_1 = 0$, $C_0 = 0$ for T, u, we note that if u is a rational root of the quartic equation

$$BE^2w^4 + (2BE^2 + D^3)w^2 + BE^2 = 0 \tag{2.3}$$

in w and T is a function of the rational root w, then the system is satisfied. From (2.3) we obtain

$$w = \pm\frac{\sqrt{-2B(2BE^2 + D^3 \pm \sqrt{4BD^3E^2 + D^6})}}{2BE}.$$

To see that w is a rational number, let

$$4BD^3E^2 + D^6 = s^2, \quad -2B(2BE^2 + D^3 - s) = t^2,$$

where s and t are rational numbers. So

$$B = \frac{s^2 - D^6}{4D^3E^2}, \quad \frac{(D^3-s)^3(D^3+s)}{4D^6E^2} = t^2.$$

Let $D^6 - s^2 = r^2$, where r is a rational number. Then

$$s = \frac{(k^2-1)D^3}{k^2+1}, \quad r = -\frac{2kD^3}{k^2+1},$$

where k is a rational number. So

$$t = \frac{2D^3k}{(k^2+1)^2E}, \quad B = -\frac{D^3k^2}{(k^2+1)^2E^2}.$$

Hence,

$$w = \pm k, \pm\frac{1}{k}.$$

We can get

$$u = k, \quad T = -\frac{E(k^2+1)}{Dk^2}.$$

Let $D = -E = 1$ and A be a positive integer. We have

$$f(X) = AX^4 + \frac{k^2}{(k^2+1)^2}X^3 + X - 1.$$

Then (1.1) has a rational solution

$$(x, y, z) = \left(\frac{k^2+1}{k^2}, k^2+1, \frac{k^2+1}{k}\right).$$

For rational numbers $k \neq 0$ and positive integers A, the discriminant of $f(X)$ is

$$-((256A^3+27A^2)k^{16}+(2048A^3+408A^2)k^{14}+(7168A^3+1908A^2-6A)k^{12} + (14336A^3+4392A^2-24A+4)k^{10}+(17920A^3+5730A^2-36A+35)k^8 + (14336A^3+4392A^2-24A+4)k^6+(7168A^3+1908A^2-6A)k^4 + (2048A^3+408A^2)k^2+256A^3+27A^2)/(k^2+1)^8<0,$$

so $f(X)=AX^4+\frac{k^2}{(k^2+1)^2}X^3+X-1$ has no multiple roots.

Therefore, there are infinitely many quartic polynomials without multiple roots such that (1.1) has a common rational solution. ∎

3. Some remarks for quartic polynomials. In Theorem 1.4 we suppose that there are infinitely many z such that the cubic equation (1.2) has two distinct rational solutions w. However, this assumption seems too strong. At present, we are not able to give a quartic polynomial without multiple roots such that (1.1) has infinitely many rational solutions.

In Theorem 1.5 we obtain the polynomial

$$f(X)=AX^4+\frac{k^2}{(k^2+1)^2}X^3+X-1$$

without multiple roots such that (1.1) has a common rational solution. For $k=1$ and positive integers $1\le A\le 1000$, the polynomial $f(X)=AX^4+\frac{1}{4}X^3+X-1$ is irreducible over $\mathbb{Q}$. It seems that the polynomial $f(X)=AX^4+\frac{1}{4}X^3+X-1$ is irreducible for every positive integer A.

In a similar way, we can get another quartic polynomial

$$f(X)=AX^4+\frac{4uv(3u+v)(u-v)}{D}X^3+(3u^2+v^2)X^2+DX$$

such that (1.1) has a rational solution

$$(x,y,z)=\left(-\frac{D(3u^2+v^2)}{(3u+v)^2(u-v)^2},-\frac{D(3u^2+v^2)}{16u^2v^2},-\frac{D(3u^2+v^2)}{4uv(3u+v)(u-v)}\right),$$

where u,v are rational numbers satisfying $uv(3u+v)(u-v)\neq 0$. If the discriminant of $f(X)$ is nonzero for suitable u,v,A,D, then this quartic polynomial has no multiple roots. For example, when $D=-1$, A is different from $\frac{4}{27}v^2(9u^2-12uv-v^2)(3u+v)^2$ and $-4u^2(u^2-4uv-v^2)(u-v)^2$, then $f(X)=AX^4-4uv(3u+v)(u-v)X^3+(3u^2+v^2)X^2-X$ has no multiple roots.

Acknowledgements. This research was supported by the National Natural Science Foundation of China (No. 11351002) and the Natural Science Foundation of Zhejiang Province (No. LQ13A010012).

REFERENCES

[B] M. A. Bennett, *The diophantine equation* $(x^k - 1)(y^k - 1) = (z^k - 1)^t$, Indag. Math. 18 (2007), 507–525.

[EES] L. C. Eggan, P. C. Eggan and J. L. Selfridge, *Polygonal products of polygonal numbers and the Pell equation*, Fibonacci Quart. 20 (1982), 24–28.

[G] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004.

[K] S. Katayama, *On the Diophantine equation* $(x^2+1)(y^2+1) = (z^2+1)^2$, J. Math. Univ. Tokushima 40 (2006), 9–14.

[SS] A. Schinzel et W. Sierpiński, *Sur l'équation diophantienne* $(x^2 - 1)(y^2 - 1) = [((y-x)/2)^2 - 1]^2$, Elem. Math. 18 (1963), 132–133.

[S] K. Szymiczek, *On a diophantine equation*, Elem. Math. 22 (1967), 37–38.

[U1] M. Ulas, *On the diophantine equation* $f(x)f(y) = f(z)^2$, Colloq. Math. 107 (2007), 1–6.

[U2] M. Ulas, *On the diophantine equation* $(x^2+k)(y^2+k) = (z^2+k)^2$, Rocky Mountain J. Math. 38 (2008), 2091–2097.

Yong Zhang
College of Mathematics and Computing Science
Changsha University of Science and Technology
410114 Changsha, People's Republic of China
and
Department of Mathematics
Zhejiang University
310027 Hangzhou, People's Republic of China
E-mail: zhangyongzju@163.com

Received 10 September 2014;
revised 1 April 2015 and 10 July 2015 (6364)