UNIVERSITAS COMENIANA
ACTA MATHEMATICA UNIVERSITATIS COMENIANAE
XXXVIII - 1981

DIOPHANTINE EQUATIONS
$x^2 + xy - y^2 = z^2$ AND $x^4 \pm x^2y^2 - y^4 = z^2$

IVAN KOREC, Bratislava

The solutions of the first equation will be presented in the form suggested in Theorem 4, Chapter 7 in [1]. Then they will be used to show that the other mentioned equations have only trivial solutions, i.e. solutions with $y = 0$ or $y = \pm x$.

Denote by $D(x_1, \ldots, x_n)$ the (nonnegative) greatest common divisor of the integers $x_1, \ldots, x_n$. Let a solution (x, y, z) of (1) be called primitive if $D(x, y, z) = 1$. Since the equation (1) is homogeneous every its solution is a multiple of a primitive solution. Hence it is sufficient to find formulas giving all primitive (and, maybe, some other) solutions of (1).

Theorem 1. Every primitive solution of the Diophantine equation

$$x^2 + xy - y^2 - z^2 = 0 \tag{1}$$

has one of the forms

$$(p^2 + r^2,\ p^2 + 2pr,\ - p^2 + pr + r^2) \tag{2}$$

$$(p^2 + r^2,\ p^2 + 2pr,\ p^2 - pr - r^2) \tag{3}$$

$$(- p^2 - r^2,\ - p^2 - 2pr,\ p^2 - pr - r^2) \tag{4}$$

$$(- p^2 - r^2,\ - p^2 - 2pr,\ - p^2 + pr + r^2) \tag{5}$$

where the integers p, r are relatively prime.

Conversely, for arbitrary integers p, r, (2), (3), (4) and (5) are solutions of (1).

<u>Proof</u>. Let (x, y, z) be a primitive solution of (1). If $D(x, y) \neq 1$ then there is a prime p such that $p \mid x$, $p \mid y$. Then obviously $p \mid z$, which is a contradiction. Hence $D(x, y) = 1$ and analogously $D(x, z) = D(y, z) = 1$.

Denote $d = D(x - z, y - z)$. Then there are integers p, q such that $D(p, q) = 1$ and

$$x = z + pd, \qquad y = z + qd \tag{6}$$

Substituting (6) into (1) we obtain

$$d.(\, z.(3p - q) + (p^2 + pq - q^2).d \,) = 0 \tag{7}$$

For $d = 0$ we obtain the primitive solutions $(1, 1, 1)$ and $(-1, -1, -1)$ which can be obtained from (3) and (5); assume further $d \neq 0$. If $3p - q = 0$ then (7) implies $-5p^2 = 0$, i. e. $p = 0$, $q = 0$, which contradicts $D(p, q) = 1$. Hence $3p - q \neq 0$ and

$$z = \frac{d.(p^2 + pq - q^2)}{q - 3p} \tag{8}$$

Since $D(d, z) = D(z + p.d, z) = D(x, z) = 1$ we have $d \mid (q - 3p)$. Further we have

$$D(q - 3p, p^2 + pq - q^2) = D(q - 3p, p^2 - 2pq) =$$
$$= D(q - 3p, p - 2q) = D(q - 3p, -5p) = D(q - 3p, 5) \mid 5$$

Hence there are four possible cases

$$q - 3p = \mp d, \qquad q - 3p = \mp 5d$$

In the first two cases we have $q = 3p \mp d$. If we denote $r = q - p$ we have

$$q = p + r, \qquad d = \mp (q - 3p) = \mp (r - 2p)$$

and then

$$z = \frac{d.(p^2 + pq - q^2)}{\mp d} = \pm (- p^2 + pr + r^2)$$

$$x = z + pd = \pm (p^2 + r^2)$$

$$y = z + qd = \pm (p^2 + 2pr)$$

These results coincide with (2) and (4).

In the third and the fourth cases we have $q = 3p \mp 5d$. To obtain the results in a nicer form denote $e = \pm d$ and $r = p - 2e$. Then

$$p = r + 2e, \qquad q = 3p \mp 5d = 3r + e$$

and

$$z = \frac{d.(p^2 + pq - q^2)}{\mp 5d} = \pm (r^2 - re - e^2)$$

$$x = z + pd = \pm (r^2 + e^2)$$

$$y = z + qd = \pm (r^2 + 2re)$$

These results coincide with (3) and (5) up to the notation.

By an easy computation we can check that every of (2)-(5) is a solution of (1); in fact it suffices to verify (2). Moreover, if one of (2)-(5) is a primitive solution of (1) then obviously $D(p, q) = 1$. This completes the proof.

Notice that no one of (2)-(5) can be omitted in Theorem 1. It cen be seen from the case $p = q = 1$.

Now we shall consider the equations $x^4 \pm x^2y^2 - y^4 = z^2$. It obviously suffices to study their nonnegative solutions, i. e. the solutions consisting of nonnegative integers.

T h e o r e m 2. All nonnegative solutions of the Diophantine equation

$$x^4 + x^2y^2 - y^4 - z^2 = 0 \tag{9}$$

are $(x, 0, x^2)$ and (x, x, x^2) where x is a nonnegative integer.

P r o o f . A nonnegative solution (x, y, z) of (9) is said to be primitive if it is not of the form (at, bt, ct^2) for some nonnegative integers a, b, c, t, $t \neq 1$. Every nonnegative solution of (9) can be obtained from a primitive solution (a, b, c) and a nonnegative integer t in this way. Hence we have to show that the only primitive solutions of (9) are $(1, 0, 1)$ and $(1, 1, 1)$.

Let (x, y, z) be a primitive solution of (9).

If $t = D(x, y)$ then $(x, y, z) = (at, bt, ct^2)$ for some nonnegative integers a, b, c and hence $t = D(x, y) = 1$. Analogously $D(x, z) = D(y, z) = 1$.

If x is even then y, z are odd and $4 \nmid (x^4 + x^2y^2 - y^4 - z^2)$, which contradicts (9). Hence x must be odd. If $3 \mid x$ then $3 \nmid y$, $3 \nmid z$ and hence $3 \nmid (x^4 + x^2y^2 - y^4 - z^2)$, which also contradicts (9). Hence $x = 1$ or $x \geqq 5$. For $x = 1$ we have

$$1 + y^2 - y^4 = z^2$$

which implies $y \leqq 1$. For $y = 0, 1$ we obtain the primitive solutions of (9) mentioned above. It remains to show that there are no other primitive solutions.

Let (x, y, z) be a primitive solution of (9) with $x \geqq 5$ and let there be no primitive solution (a, b, c) of (9) with $1 < a < x$. Since $D(x, y) = 1$ we have $y \neq 0$. Denote $X = x^2$, $Y = y^2$. Then

$$X^2 + XY - Y^2 - z^2 = 0$$

$X > 0$ and $D(X, Y, z) = 1$. Hence by Theorem 1 there are relatively prime integers p, r satisfying

$$x^2 = p^2 + r^2 \tag{10}$$

$$y^2 = p^2 + 2pr \tag{11}$$

Obviously $p \neq 0$, $r \neq 0$. Moreover, we may assume $p > 0$; if $p < 0$ we can change the signs of both p, r. By (10) and $D(p, r) = 1$ there are integers m, n such that

$$D(m, n) = 1 \ , \qquad 2 \mid mn \ , \qquad x = m^2 + n^2 \tag{12}$$

and one of the cases takes place:

$$p = 2mn \ , \qquad r = m^2 - n^2 \tag{13}$$

$$p = m^2 - n^2 \ , \qquad r = 2mn \tag{14}$$

It holds $m \neq 0$, $n \neq 0$, and we may assume $m > 0$ in both cases. Moreover, $m^2 + n^2 \geqq 5$, and hence

$$m + |n| \geqq 3 \tag{15}$$

If (13) holds then $p > 0$ implies $n > 0$. Further,

$$y^2 = p.(p + 2r) = 4mn.(m^2 + mn - n^2)$$

The numbers m, n, $m^2 + mn - n^2$ are pairwise relatively prime and positive, hence there are natural numbers u, v, w such that

$$m = u^2 \ , \qquad n = v^2 \ , \qquad m^2 + mn - n^2 = w^2 \tag{16}$$

Then (u, v, w) is a primitive solution of (9). If $u = 1$ then $m = 1$, $1 + n - n^2 \geqq 0$, hence $n = 1$ which contradicts (15); therefore $u > 1$. Then $u < m < x$, which contradicts the choice of (x, y, z).

If (14) holds we have $|n| < m$ and

$$y^2 = p.(p + 2r) = (m + n).(m - n).(m^2 + 4mn - n^2)$$

The factors of the right-hand side are pairwise relatively prime and positive, hence there are natural numbers u, v, w satisfying

$$m + n = u^2 , \quad m - n = v^2 , \quad m^2 - n^2 + 4mn = w^2 \tag{17}$$

The numbers u, v are different and $D(u, v) = 1$. Further, $m^2 - n^2 = u^2 v^2$ and

$$4mn = 2m.2n = (u^2 + v^2).(u^2 - v^2) = u^4 - v^4 \tag{18}$$

hence

$$u^4 + u^2v^2 - v^4 = w^2 \tag{19}$$

Therefore (u, v, w) is a primitive solution of (9). If $u = 1$ then (19) implies $v = 1$, which contradicts $u \neq v$; hence $u > 1$. Further, $u < u^2 = m + n < x$ which contradicts the choice of (x, y, z). This contradiction completes the proof of Theorem 2.

T h e o r e m 3. All nonnegative solutions of the Diophantine equation

$$x^4 - x^2y^2 - y^4 = z^2 \tag{20}$$

are of the form $(x, 0, x^2)$ where x is a nonnegative integer.

P r o o f . Since the proof is very similar to the proof of Theorem 2 we shall do some details more briefly.

Define the primitive solutions of (20) analogously as those of (9). We have to show that (1, 0, 1) is the unique primitive solution of (20). It can be easily verified that (1, 0, 1) is the unique primitive solution with $x \leq 4$.

Now let (x, y, z) be a primitive solution of (20) such that $x \geq 5$ and let there be no primitive solution (a, b, c) of (20) with $1 < a < x$. Then $D(x, y) = 1$ and $y \neq 0$. For $X = x^2$, $Y = -y^2$ we have $D(X, Y) = 1$ and

$$X^2 + XY - Y^2 - z^2 = 0$$

Hence there are integers p, q satisfying (10) and

$$y^2 = -(p^2 + 2pq) \tag{21}$$

It holds $D(p, q) = 1$, $p \neq 0$ and $q \neq 0$; we may assume $p > 0$ and then $q < 0$. There are integers $m > 0$, n which safisfy (12), (15) and one of (13), (14).

If (13) holds then $n > 0$ and

$$y^2 = -p.(p + 2q) = 4mn.(n^2 - nm - m^2)$$

The integers m, n, $n^2 - nm - m^2$ are positive and pairwise relatively prime. Hence there are positive integers u, v, w satisfying

$$m = u^2, \qquad n = v^2, \qquad n^2 - nm - m^2 = w^2$$

Then we have $D(u, v) = 1$ and

$$v^4 - u^2v^2 - u^4 - w^2 = 0 \tag{22}$$

i. e. (v, u, w) is a primitive solution of (20). However, $v \leqq |n| < |r| < x$, hence $v = 1$ by the choice of (x, y, z). Then $n = 1$, $m^2 + m = 1 - w^2$, $m.(m + 1) \leqq 1$, which is a contradiction.

If (14) holds we have $|n| < m$ and

$$y^2 = -p.(p + 2q) = (m + n).(m - n).(n^2 - m^2 + 4mn)$$

The numbers $m + n$, $n^2 - m^2 + 4mn$, $m - n$ are positive and pairwise relatively prime, hence there are positive integers u, v, w such that

$$m + n = u^2 , \quad m - n = v^2 , \quad n^2 - m^2 + 4mn = w^2$$

and hence

$$u^4 - u^2v^2 - v^4 - w^2 = 0 \qquad (23)$$

Since obviously $D(u, v) = 1$, (u, v, w) is a primitive solution of (20). Moreover, (23) and $v \neq 0$ imply $u \neq 1$ and then $1 < u < u^2 = m + n \leqq p < x$. This inequality contradicts the choice of (x, y, z), and the proof is completed.

References

[1] M o r d e l l, L. J.: Diophantine equations. Academic Press, London and New York, 1969.

Author's address: Ivan Korec, Katedra algebry a teórie čísel PFUK
Matematický pavilón - Mlynská dolina
816 31 Bratislava

Received: 24. 10. 1978

S ú h r n

DIOFANTICKÉ ROVNICE $x^2 + xy - y^2 = z^2$ a $x^4 \pm x^2y^2 - y^4 = z^2$

Ivan Korec, Bratislava

Hľadajú sa explicitné vzorce pre primitívne riešenia prvej z uvedených rovníc. Nájdené vzorce sa potom používajú na dôkaz, že ďalšie dve uvedené rovnice majú iba triviálne riešenia, t.j. riešenia s vlastnosťou $y = 0$ alebo $y = \pm x$.

Резюме

ДИОФАНТОВЫ УРАВНЕНИЯ $x^2 + xy - y^2 = {}^2$ И $x^4 \pm x^2y^2 - y^4 = {}^2$

Иван Корец, Братислава

В статье найдены явные форрмулы для всех примитивных решений первого уравнения. Эти формулы потом используются для доказательства теорем утверждающих, что следующих два уравнения обладают только тривиальными решениями, т. е. такими решениями, что $y = 0$ или $y = \pm x$.