*Вестник Сыктывкарского университета.
Сер.1. Вып.13.2011*

УДК 511.92

ON THE DIOPHANTINE EQUATION $x^2 - dy^2 = z^n$

A. Grytczuk

In this Note we remark that there is some duality connected with the problem of solvability of the Diophantine equation

(*) $x^2 - dy^2 = z^n$.

Namely, we prove that the equation (*) has no solution in positive integers x, y for every pime $z = q^*$ generated by an arithmetic progression and for every odd positive integer n if d is squarefree positive integer such that $p \mid d$, where p is an odd prime.

Keywords: solvability of the Diophantine equation.

1. Introduction. In 1770 Euler obtained integral solutions of the Diophantine equation

(1) $ax^2 - dy^2 = z^3$.

Denoting by A, D the square roots of a and d ,respectively and assuming that

(2) $Ax + Dy = (Au + Dv)^3$

and replacing D by $-D$ for the like equation we obtain the following formulas for the integer solutions of the equation (1):

(3) $x = u\left(au^2 + 3dv^2\right), \; y = v\left(3au^2 + dv^2\right), \; z = au^2 - dv^2$.

Euler remarked also that this method is fals to give integer solution with $y = 1$, when $a = 2$ and $d = 5$.Indeed, in this case the equation (1) reduces to the form:

(4) $2x^2 - 5 = z^3$,

but the formulas (3) we can't obtained the solution $x = 4, z = 3$ of the equation (4).

In 1769 Lagrange extended Euler's method by the following way; let the equation

(5) $\xi^2 - d\eta^2 = (\xi + D\eta)(\xi - D\eta)$

for $d = D^2$ has the property that its product by $u^2 - dv^2$ is equal to $x^2 - dy^2$, where

(6) $x + Dy = (\xi + D\eta)(u + Dv)$,

whence

(7) $x = \xi u + d\eta v, \ \ y = \xi v + \eta u.$

Putting $\xi = u, \eta = v$ and concluding that $x^2 - dy^2 = z^2$ holds if $x = u^2 + dv^2, y = 2uv, z = u^2 - dv^2$ then the factors in the second member of (6) are equal.

Next, we observe that these values of x and y are news values of ξ and η;

(8) $\xi = u^2 + dv^2, \eta = 2uv, \xi + D\eta = (u + Dv)^2$,

and consequently we obtain that the Diophantine equation (1) has the solutions given by the formulas (3) for $a = 1$.

A repetition of this process leads to certain integer solutions of the Diophantine equation:

(*) $x^2 - dy^2 = z^n$,

but this method rarely gives all integer solutions of (*) (Cf.[3]).Some further investigations concerning solvability of the Diophantine equation (*) are given by Ward [4], Czech [1] and Czech and Wieczorkiewicz [2].

In this paper we note that there is some duality connected with the problem of solvability of the Diophantine equation (*).

Namely,we prove, in contrast to the fact that the equation (*) has infinitely many solutions in positive integers x, y, z; in general, that for some fixed squarefree positive integer d and prime p such that $p \mid d$

there are infinitely many primes q^*such that for every $z = q^*$ and every odd natural number $n \geq 1$, the Diophantine equation (*) has no solutions in integers x, y.The following theorem is true:

Theorem. *Let* p *be an odd prime such that* $p \mid d$ *,where* d *is a squarefree positive integer. Then for every prime* $q^* = z$ *from the arithmetic progression of the form;* $8pm+pj_0+r$, *with* $pj_0+r \equiv 5 \pmod 8$ *where* $\left(\frac{r}{p}\right) = -1$ *and every odd positive integer* n, *the Diophantine equation (*) has no solutions in integers* x, y.

2. Proof of the Theorem

Let $p \mid d$, where p is an odd prime and let r be quadratic non-residues for p, so $\left(\frac{r}{p}\right) = -1$. it is easy to see that the numbers of the form: $pj + r$ give distinct residues $\mod 8$. Hence, for some $j = j_0$, we have

(2.1) $pj_0 + r \equiv 5 \,(\mod 8)\,.$

Now, we can consider the positive integers a_m of the following form:

(2.2) $a_m = p\,(8m + j_0) + r = 8pm + pj_0 + r.$

We oserve that the greatest common divisor of the numbers $8p$ and $pj_0 + r$ is equal to one, so $(8p.pj_0 + r) = 1$.

Indeed, suppose that $(8p, pj_0 + r) = k > 1$.Then there is a prime q such that $q \mid k$. Hence, from the property of the greatest common divisor and divisibility relation ,we get

(2.3) $q \mid 8p, \;\; q \mid pj_0 + r.$

From (2.3) we obtain that $q = p$ and $q \mid r$, so $p \mid r$,so is impossible, because $\left(\frac{r}{p}\right) = -1$.

Since $(8p, pj_0 + r) = 1$, then by Dirichlet theorem on arithmetic progressions it follows that the arithmetic progression given by (2.2) contains infinitely many primes.

Let for some positive integer $m = m_0$ the number a_{m_o} generated by arithmetic progresson (2.2) is a prime number, so $a_{m_0} = q^*$.Then by (2.1) and (2.2) it follows that

(2.4) $q^* \equiv 5 \,(\mod 8)\,.$

By the assumption of the Theorem and well-known properties of Legendre's symbol it follows that

(2.5) $\left(\frac{q^*}{p}\right) = \left(\frac{8pm+pj_0+r}{p}\right) = \left(\frac{r}{p}\right) = -1.$

Suppose that the Diophantine equation (*) has a solution in integers x, y and $z = q^*$ for some odd positive integer n.Hence,we have

(2.6) $x^2 - dy^2 = (q^*)^n\,,$

where $p \mid d$ for some odd prime p.

From (2.6) we obtain that

(2.7) $x^2 \equiv (q^*)^n \,(\mod d)\,.$

Since $p \mid d$ then by (2.7) it follows that $(q^*)^n$ is a quadratic residues mod p,so we have

(2.8) $\left(\frac{(q^*)^n}{p}\right) = +1.$

From (2.5) and the assumption that $n = 2k+1$ and well-known properties of the Legendre symbol ,we obtain

(2.9) $\left(\frac{(q^*)^n}{p}\right) = \left(\frac{q^*}{p}\right)^n = \left(\frac{q^*}{p}\right)^{2k}\left(\frac{q^*}{p}\right) = (+1)(-1) = -1.$

We see that the equality (2.9) contrary to the equality (2.8) and the proof of the Theorem is complete.■

From the Theorem immediately follows of the following Corollary:

Corollary. *There are infinitely many primes* $q^* \equiv 5 \pmod 8$ *such that each of them can't be representable by the quadratic form* $x^2 - dy^2$ *with some squarefree positive integer* d.

References

1. **J.Czech**, On the equation $x^2 - Dy^2 = z^k$ with $D = 2, 3, 5, 7, 11, 13//$ *Funct. Approx. Comment. Math. 16(1988), 77–79.*
2. **J.Czech and J.Wieczorkiewicz**, An application of matrices to parametrization of the equation $3x^2 - 2y^2 = z^k//$ *Discuss. Math. 8(1986), 45–52.*
3. **L.E.Dickson**, Introduction to the Theory of Numbers. Dower Publ. Inc. New York, 1957.
4. **M.Ward**, The Diophantine equation $x^2 - dy^2 = z^M//$ *Trans. Amer. Math. Soc. 38 (1935), 447–457.*

Faculty of Mathematics,Computer Science and Econometrics University of Zielona Góra, ul.Prof.Szafrana 4a,65-516 Zielona Góra, Poland and
Western Higher School of Marketing and Internationale Finances pl.Słowiański 9, 65-069 Zielona Góra, Poland
e-mail: A.Grytczuk@wmie.uz.zgora.pl or
e-mail: algrytczuk@onet.pl

Поступила 07.02.2011