2010

# On a Diophantine equation of Stroeker

Luca, Florian; Stnic, Pantelimon; Togbe, A.

Bulletin of Belgian Math Society 17 (2010), 1-8.
https://hdl.handle.net/10945/38842

# On a Diophantine Equation of Stroeker

F. Luca, P. Stănică, and A. Togbé

October 27, 2008

**Abstract**

In this paper, we prove that there are infinitely many positive integers $N$ such that the Diophantine equation $(x^2+y)(x+y^2) = N(x-y)^3$ has no nontrivial integer solution $(x,y)$.

## 1 Introduction

Let $N$ be a nonzero integer. In [6], Stroeker investigated the Diophantine equation

$$(x^2+y)(x+y^2) = N(x-y)^3, \qquad (x,y) \in \mathbb{Z}^2. \tag{1}$$

It clearly suffices to consider the case when $N > 0$ since if $(x,y)$ is a solution of equation (1) above, then $(y,x)$ is a solution of (1) with $N$ replaced by $-N$. We shall only consider solutions $(x,y)$ such that $xy \neq 0$. Following Stroeker, we refer to such solutions as *proper*. Note that equation (1) always admits the solution $x = y = -1$. This will be referred to as the *trivial solution*. Stroeker proved that if $(x,y)$ is any proper solution to equation (1), then $\max\{|x|,|y|\} < N^3$ if $N > 4$. He also showed that if $N > 1$ is odd, then equation (1) has at least one non-trivial proper solution and if additionally $27N^2 - 2$ is a square, then equation (1) has at least 5 non-trivial proper solutions. In [4], Mąkowski pointed out a connection between (1)

**Mathematics Subject Classification:** 11D25, 11G05
**Key Words:** Diophantine equations; Elliptic Curves.

and Fibonacci numbers. In fact, he showed that if $N = F_{k-2}F_{k-1}$, then $(x, y) = (F_kF_{k+1}, -F_{k+1}^2)$ (for $k$ even) and $(x, y) = (F_{k+1}^2, -F_kF_{k+1})$ (for $k$ odd) are solutions of (1). Moreover, he asked the following question: "*Do there exist infinitely many positive (even) integers $N$ such that equation* (1) *has only the trivial solution*"? Computations in the range $1 \leq N \leq 51$ showed that if $N \in \{8, 10, 12, 14, 16, 20, 24, 26, 28, 30, 36, 44, 48\}$, then equation (1) has no proper non-trivial solution.

Our main result is an affirmative answer to this question.

**Theorem 1.** *There are infinitely many positive integers $N$ such that equation* (1) *has no non-trivial proper solution $(x, y)$.*

Throughout this paper, we use the Vinogradov symbols $\gg$ and $\ll$ as well as the Landau symbol $O$ with their usual meanings. The constants implied by them are absolute.

# 2 Proof of Theorem 1

We let $X$ be a large positive real number. We put $N = 2p$, where $p \in (X/2, X)$ is a prime. Stroeker showed that for any non-trivial solution $(x, y)$ of equation (1) there are integers $u \geq 2,\ v \geq 1$ and $\ell \neq 0$ such that

$$2x = v - u + \ell + 1, \qquad 2y = v - u - \ell + 1, \qquad uv = N\ell,$$

and

$$(u + v - \ell)^2 = 4(u - 1)(v + 1) + 1.$$

Stroeker showed that $\max\{u, v\} \leq 2N^3/3 < 6X^3$ if $p \geq 5$, and showed also that both formulae

$$u^2(v - N)^2 - 2uN(v^2 + vN + 2N) + N^2(v + 1)(v + 3) = 0 \tag{2}$$

and

$$v^2(u - N)^2 - 2vN(u^2 + uN - 2N) + N^2(u - 1)(u - 3) = 0 \tag{3}$$

hold. Furthermore, both $u(v - N)^2/N$ and $v(u - N)^2/N$ are integers. If $v = N$, then $4u = N + 3$, which is impossible since $N + 3$ is odd. Thus, $v \neq N$. The same argument shows that $u \neq N$. Since $N = 2p$, it follows easily from the fact that $u(v - N)^2/N$ is an integer that $p \mid uv$.

Let us assume that $p \mid v$ (*Case 1*). Write $v = p\lambda$, where $\lambda \neq 2$. Note that $\lambda \leq 2N^3/(3p) < 6X^2$. Replacing $v$ by $\lambda p$ in equation (2) and simplifying a factor of $p^2$, we get

$$u^2(\lambda-2)^2 - 4u(\lambda^2 p + 2\lambda p + 4) + 4(\lambda p+1)(\lambda p+3) = 0. \tag{4}$$

(If instead $p \mid u$, then $u = p\lambda$, and equation (3) simplified by a factor of $p^2$ becomes $v^2(\lambda-2)^2 - 4v(\lambda^2 p + 2\lambda p - 4) + 4(\lambda p-1)(\lambda p-3) = 0$. We shall refer to this as *Case 2*.)

The relation (4) of Case 1 can be rewritten as

$$U^2 - 2\lambda V^2 = 4 - 2\lambda, \tag{5}$$

where

$$U = 2\lambda p + 4 - u\lambda - 2u, \qquad V = 2u - 1.$$

(If $u = p\lambda$, then the corresponding Pell equation is also $U^2 - 2\lambda V^2 = 4 - 2\lambda$, with $U = 2\lambda p - 4 - v\lambda - 2v$ and $V = 2v + 1$.)

Let $T := T(X) < 6X^2$ be some parameter depending on $X$ and tending to infinity with $X$, to be made more precise later. Assume that $\lambda \leq T$ is given. If $2\lambda$ is a square, then $U - \sqrt{2\lambda}V$ and $U + \sqrt{2\lambda}V$ are two divisors of $4 - 2\lambda$ whose product is $4-2\lambda$. Hence, the pair $(U, V)$ can be determined in at most $2\tau(|2\lambda-4|)$ ways, where for a positive integer $m$ we write $\tau(m)$ for the number of its positive divisors. Note that the triple $(\lambda, U, V)$ determines $p$ uniquely. Thus, the number of possibilities for the prime $p$ when $2\lambda$ is a square is $\ll \tau(|2\lambda - 4|)$. Assume now that $2\lambda$ is not a square. It is then well-known from the theory of quadratic fields that there exist $t$ *fundamental* positive integer solutions $(U_1, V_1), \ldots, (U_t, V_t)$ of equation (5) in the following sense: if $(U, V)$ is any positive integer solution of equation (5), then $U + \sqrt{2\lambda}V = (U_i + \sqrt{2\lambda}V_i)\zeta^m$ holds for some $i = 1, \ldots, t$ and some nonnegative integer $m$, where we put $\zeta$ for the fundamental unit of the real quadratic field $\mathbb{Q}[\sqrt{2\lambda}]$. Since $\zeta \geq (1 + \sqrt{5})/2$ and $\max\{|U|, |V|\} \ll X^5$, it follows that $m \ll \log X$. It is known that the number $t$ of fundamental solutions to equation (5) is $\ll \tau(|2\lambda - 4|)$. Observe, as before, that the triple $(\lambda, U, V)$ determines $p$ uniquely. Hence, the total number of primes $p$ that can arise in this way when $1 \leq \lambda \leq T$ and $\lambda \neq 2$ is

$$\ll \sum_{\substack{1 \leq \lambda \leq T \\ \lambda \neq 2}} \tau(|2\lambda - 4|) \log X \ll T(\log T)(\log X) \ll T(\log X)^2. \tag{6}$$

We now assume that $\lambda \in (T, 6X^2)$. Stroeker showed, under the condition $v \neq N$, which is the case for the positive integers $N$ we are considering, that there exists a positive integer $z$ such that

$$(v^2 + vN + 2N)^2 - (v - N)^2(v^2 + 4v + 3) = z^2, \tag{7}$$

and

$$u = \frac{N(v^2 + vN + 2N \pm z)}{(v - N)^2}.$$

If one looks at (3) instead, one gets, under the assumption $u \neq N$ which is the case for us, that there exists an integer $w$ such that

$$(u^2 + uN - 2N)^2 - (u - N)^2(u^2 - 4u + 3) = w^2,$$

with

$$v = \frac{N(u^2 + uN - 2N \pm w)}{(u - N)^2}.$$

Returning to formula (7), let us observe that

$$(v^2 + vN + 2N)^2 = v^4 \left(1 + O\left(\frac{N}{v}\right)\right)^2 = v^4 \left(1 + O\left(\frac{1}{\lambda}\right)\right),$$

while

$$\begin{aligned} (v - N)^2(v^2 + 4v + 3) &= v^4 \left(1 + O\left(\frac{N}{v}\right)\right)^2 \left(1 + O\left(\frac{1}{v}\right)\right) \\ &= v^4 \left(1 + O\left(\frac{1}{\lambda}\right)\right). \end{aligned}$$

Hence,

$$z^2 = v^4 \left(1 + O\left(\frac{1}{\lambda}\right)\right) - v^4 \left(1 + O\left(\frac{1}{\lambda}\right)\right) = O\left(\frac{v^4}{\lambda}\right),$$

giving

$$z = O\left(\frac{v^2}{\sqrt{\lambda}}\right).$$

Thus,

$$u = \frac{N(1 + v/N + 2N/v^2 \pm z/v^2)}{(1 - N/v)^2} = N\left(1 + O\left(\frac{1}{\sqrt{\lambda}}\right)\right) = N + O\left(\frac{X}{\sqrt{T}}\right).$$

Let $c$ be the constant implied by the above Landau symbol and let $Y = cX/T^{1/2}$. Then $u = N + m$, where $0 < |m| \leq Y$. Replacing in relation (3) the variable $u$ by $2p + m$ and simplifying a factor of $p^2$, we get the relation

$$\lambda^2 m^2 - 4\lambda((2p+m)^2 + 2(2p+m)p - 4p) + 4(2p+m-1)(2p+m-3) = 0.$$

(In Case 2, we replace $v = N + m = 2p + m$ in (2) and, after simplifying a factor of $p^2$, we obtain $\lambda^2 m^2 - 4\lambda((2p+m)^2 + 2(2p+m)p + 4p) + 4(2p+m+1)(2p+m+3) = 0$.) Multiplying both sides of the above relation by $1 - 2\lambda$ and regrouping it we get

$$W^2 = 2\lambda^3 m^2 - \lambda^2(12m - 4) + 8\lambda + 4, \tag{8}$$

where $W = 4(1-2\lambda)p + 2(m-2) - \lambda(3m-2)$. (In a similar way, in Case 2, we obtain $W^2 = 2\lambda^3 m^2 + \lambda^2(12m+4) + 8\lambda + 4$, where $W = 4(1-2\lambda)p + 2(m+2) - \lambda(3m+2)$.) It is easy to check that the two variable polynomial

$$P(\Lambda, M) = 2\Lambda^3 M^2 - \Lambda^2(12M - 4) + 8\Lambda + 4$$

is irreducible as a polynomial in $\mathbb{C}[\Lambda, M]$. Indeed,

$$\Lambda P(\Lambda, M) = 2((\Lambda^2 M - 3\Lambda)^2 + 2\Lambda^3 - \Lambda^2 + 8\Lambda)$$

and $-2\Lambda^3 + \Lambda^2 - 8\Lambda$ is not the square of some polynomial in $\mathbb{C}[\Lambda]$. This shows that $P(\Lambda, M)$ is irreducible as a quadratic polynomial in $M$ over $\mathbb{C}[\Lambda]$, so in particular $P(\Lambda, M)$ is irreducible in $\mathbb{C}[\Lambda, M]$. (A similar argument shows that the polynomial $Q(\Lambda, M) = 2\Lambda^3 M^2 + \Lambda^2(12M+4) + 8\Lambda + 4$ of Case 2 is also irreducible.)

Assume that $m$ is an integer such that $P(\Lambda, m)$ is still irreducible as a polynomial of degree 3 in $\Lambda$ with integer coefficients. Let $\theta_m$ be any root of $P(\Lambda, m)$ and let $\Delta_m$ be the discriminant of the cubic field $\mathbb{Q}[\theta_m]$. Corollary 3.12 in [3] shows that the number of integer solutions $(W, \lambda)$ of equation (8) is

$$\ll |\Delta_m|^{0.201}. \tag{9}$$

Notice that $\Delta_m$ is a divisor of the discriminant of the polynomial $\Lambda^3 + 4\Lambda^2 - (12m-4)\Lambda + 4m^2$ (obtained by rewriting the equation $P(\Lambda, m) = 0$ as a monic polynomial equation in $2/\Lambda$) and this last discriminant is $-16(27m^4 - 216m^3 + 280m^2 - 48m)$. (In Case 2, $Q(\Lambda, m)$ produces the polynomial $\Lambda^3 + 4\Lambda^2 + (12m+4)\Lambda + 4m^2$, whose discriminant is $-16(27m^4 + 216m^3 + 280m^2 +$

$48m$).) In both cases, these expressions are never zero if $m$ is a non-zero integer, which is an observation that will be useful later. For the moment, we simply record that estimate (9) and the above calculation show that the number of integer solutions to equation (8) is $\ll |m|^{.804}$. Clearly, every integer solution $(W, \lambda)$ of equation (8) determines $p$ uniquely. This shows that the number of primes $p$ that can arise in this way when $P(\Lambda, m)$ is irreducible and $1 \leq |m| \leq Y$ is

$$\ll \sum_{1 \leq |m| \leq Y} m^{.804} \ll Y^{1.804} \ll \frac{X^{1.804}}{T^{.902}}.$$

Assume finally that $1 \leq |m| \leq Y$ is such that $P(\Lambda, m)$ is reducible as a polynomial in $\Lambda$ with integer coefficients. By Hilbert's Irreducibility Theorem, the number of such values for $m$ is $\ll Y^{1/2} \log Y \ll Y^{1/2} \log X$ (see, for example, [2], or Theorem 1, Section 13.1 in [7]). Multiplying both sides of equation (8) by $4m^4$, we get

$$U^2 = V^3 - (12m - 4)V^2 + 16m^2V + 16m^4,$$

where $U = 2m^2W$ and $V = 2\lambda m^2$ (in Case 2, we get the equation $U^2 = V^3 + (12m + 4)V^2 + 16m^2V + 16m^4$ with similarly defined $U, V$, as in Case 1). Write

$$\Lambda^3 - (12m - 4)\Lambda^2 + 16m^2\Lambda + 16m^4 = (\Lambda + a)(\Lambda^2 + b\Lambda + c),$$

where $a$, $b$ and $c$ are integers. Then there exist two squarefree integers $d_1$ and $d_2$ dividing the discriminant of the above polynomial (which is $16m^4\Delta_m$), such that

$$V + a = d_1U_1^2 \qquad \text{and} \qquad V^2 + bV + c = d_2U_2^2.$$

The second equation can be rewritten as

$$V_1^2 + \Delta = d_2U_3^2, \tag{10}$$

where $V_1 = 2V + b$, $U_3 = 2U_2$ and $\Delta = 4c - b^2$. Note that $\Delta \neq 0$, since if $\Delta = 0$, then $P(\Lambda, m)$ has a double root, and, as we have seen, this is not possible if $m \neq 0$ is an integer. Note that $ac = 16m^4$ and $ab + c = 16m^2$, therefore $|c| \leq 16m^4$ and $|b| \leq 16m^2 + 16m^4 \leq 32m^4$, which shows that $|\Delta| \ll m^8$. It is now easy to check that $\max\{|V_1|, |U_3|\} \ll X^8$. The arguments from the first part of our proof (the case when $\lambda < T$) show

that for fixed values of $\Delta$ and $d_2$, the number of integer solutions $(V_1, U_3)$ to equation (10) is $\ll \tau(|\Delta|)\log X \ll X^{o(1)}$ as $X \to \infty$. Since $d_2$ can be chosen in at most $\tau(|\Delta_m|) \leq X^{o(1)}$ ways for a fixed $m$, there are only $O(Y^{1/2}\log X)$ possibilities for $m$, and each quadruple $(m, d_2, V_1, U_3)$ arising in this way determines $p$ uniquely, we get that the number of possibilities for $p$ is at most $Y^{1/2}X^{o(1)} < X^{2/3}$ whenever $X$ is sufficiently large. (The same argument holds for Case 2.) Putting everything together, we get that the number of primes $p \in (X/2, X)$ such that the Diophantine equation (1) can have a non-trivial proper solution is

$$\ll T(\log X)^2 + \frac{X^{1.804}}{T^{.902}} + X^{2/3}.$$

Choosing $T = X^{1.804/1.902}$, we get that the number of such possibilities for $p$ is $< X^{0.95}$ for large values of $X$. Since there are $\geq (0.5 + o(1))X/\log X$ primes $p \in (X/2, X)$ as $X \to \infty$, we deduce that for most primes $p$ in the above interval, equation (1) has no non-trivial reduced solutions when $N = 2p$. This completes the proof of the theorem.

# 3 Related elliptic curves

In the construction of solutions, Stroeker obtained elliptic curves of the following equations (see formulas (14) and (14') in [6])

$$z^2 = 4(N-1)(v+1)^3 + (N-3v-2)^2, \tag{11}$$

and

$$w^2 = 4(N+1)(u-1)^3 + (N-3u+2)^2. \tag{12}$$

If $u = (N+3)/4$, then

$$(v, z) = ((N-3)/4, N(N+1)/4) \tag{13}$$

is a point on the elliptic curve defined by (11). In the same way,

$$(u, w) = ((N+3)/4, N(N-1)/4) \tag{14}$$

is a point on the elliptic curve defined by (12).

**Theorem 2.** *The above points $(v, z)$ and $(u, w)$ are not torsion points except if $N = 3, 9$. Moreover, if $N = 3$, both points are of order 9 and if $N = 9$, they are of order 6.*

*Proof.* Using Magma [1], for $2 \leq N \leq 100$, we checked that the points (13) and (14) are not torsion points on the curves (11) and (12), respectively, except for $N = 3, 9$. If $N = 3$, both are torsion points of order 9, while when $N = 9$, both are torsion points of order 6. To achieve this, multiply both members of equation (11) by $4(N-1)^2$ and put $X = 4(N-1)v$ and $Y = 4(N-1)z$ to obtain

$$Y^2 = X^3 + (12N-3)X^2 + 24N(N-1)X + (4N(N-1))^2.$$

Now we set $y = Y$ and $x = X + 4N - 1$ and arrive at

$$y^2 = x^3 + (-24N^2 - 3)x + 16N^4 + 40N^2 - 2. \tag{15}$$

If $u = (N+3)/4$, then $v = (N-3)/4$ and $z = N(N+1)/4$. One can deduce that $x = N(N-1)$ and $y = 5N - 4$. Therefore $P = (x, y) = (N^2 + 2, N(N^2-1))$ is the point on (15) corresponding to the initial point $(v, z) = ((N-3)/4, N(N-1)/4)$ on (11) via the above birational transformation. We follow a similar procedure for equation (12) and we obtain the same equation (15) with the same corresponding point $P = (x, y) = (N^2+2, N(N^2-1))$ to the point $(u, w)$ when $u = (N+3)/4$ on (12). So, we deal only with equation (15).

Let $kP = (x_k, y_k)$ be the sum of $P = (x, y) = (N^2 + 2, N(N^2 - 1))$ with itself $k$ times in the Mordell-Weil group of (15). By Mazur's Theorem (see [5]), if $P$ is a torsion point then $kP = O$ for some $k \in \{1, \ldots, 12\}$. So, we computed $(x_k, y_k)$ for all $1 \leq k \leq 12$. In fact, consider the associated projective points $(X_k : Y_k : Z_k)$ with $X_k, Y_k, Z_k \in \mathbb{Z}[N]$. We solved separately each one of the polynomial equations $Y_k(N) = 0, Z_k(N) = 0$ for $2 \leq k \leq 12$. Here are the results:

- If $Y_k(N)Z_k(N) = 0$ for some positive integer $N$ and $1 \leq k \leq 12$, then $k \in \{3, 6, 9, 12\}$.
- If $Y_3(N) = 0$, then $N = 9$;
- If $Z_6(N) = 0$, then $N = 9$. If $Y_6(N) = 0$, then $N = 9$;
- If $Z_9(N) = 0$, then $N = 3$;
- If $Z_{12}(N) = 0$, then $N = 9$.

□

**Acknowledgements.** We thank the referee for suggestions which improved the quality of the paper. Work on this paper started during a pleasant visit of F. L. and P. S. at the Mathematics Department of the Universidad Autónoma de Madrid in Spring of 2008. These authors thank the people of this department for their hospitality. Research of F. L. was also supported in part by grants SEP-CONACyT 79685 and PAPIIT 100508. The second author was supported by a RIP grant from NPS. The third author was supported by Purdue University North Central.

# References

[1] Wieb Bosma, John Cannon, and Catherine Playoust, 'The Magma algebra system. I. The user language', *J. Symbolic Comput.* **24** 3-4 (1997), 235-265.

[2] S. D. Cohen, 'The distribution of Galois groups and Hilbert's irreducibility theorem', *Proc. London Math. Soc.* **43** (1981), 227–250.

[3] H. Helfgott and A. Venkatesh, 'Integral points on elliptic curves and 3-torsion in class groups', *J. Amer. Math. Soc.* **19** (2006), 527–550.

[4] A. Mąkowski, 'Stroeker's equation and Fibonacci numbers', *Fibonacci Quart.* **26** (1988), 336–337.

[5] J.M. Milne, *Elliptic curves*, 2006, BookSurge Publishers.

[6] R. J. Stroeker, 'The diophantine equation $(x^2+y)(x+y^2) = N(x-y)^3$', *Simon Stevin* **54** (1980), 151–163.

[7] J. P. Serre, *Lectures on the Mordell-Weil theorem*, 3rd edition, Aspects in Mathematics E15, Vieweg, 1997.

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autónoma de México
C.P. 58089, Morelia, Michoacán, México
`fluca@matmor.unam.mx`

Pantelimon Stănică
Department of Applied Mathematics

Naval Postgraduate School
Monterey, CA 93943–5216, USA
pstanica@nps.edu

Alain Togbé
Department of Mathematics
Purdue University North Central
1401 S. U.S. 421
Westville, IN 46391 , USA
atogbe@pnc.edu