INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 5(3) (2005), #A15

SQUARES IN LUCAS SEQUENCES WITH RATIONAL ROOTS

P.G. Walsh [1]

Department of Mathematics, University of Ottawa, Ottawa, Ontario, Canada

gwalsh@mathstat.uottawa.ca

Received: 10/16/04, Revised: 4/21/05, Accepted: 8/12/05, Published: 9/8/05

Abstract

In 1997, Darmon and Merel proved the stunning result that the Diophantine equation $x^n + y^n = z^2$ has no nontrivial integer solutions for $n \geq 4$. This can be interpreted as saying that if $\{v_n\}$ represents a Lucas sequence of the second kind, defined by a quadratic polynomial with rational roots, then the equation $v_n = x^2$, with x an integer, implies that $n \leq 3$. The goal of the present paper is to prove a similar, but partial, result for the case that the sequence is a Lucas sequence of the *first* kind, whose defining polynomial has rational roots. In other words, our goal is to study the Diophantine equation $z^2 = (x^n - y^n)/(x - y)$. Employing a combination of recently proved Diophantine results of Bennett and Skinner, Poonen, Darmon and Merel, Wiles, and Ribet, from the modularity approach, together with recent advances by N. Bruin on the effective Chabauty method for determining all rational points on a given curve of genus greater than one, we deduce that the equation in question is not solvable for a substantial proportion of positive integer values n.

1. Introduction

There are many results on the location of squares in Lucas sequences. In the case that the Lucas sequence is defined by a polynomial with rational roots, Darmon and Merel [4] solved the problem for Lucas sequences of the *second kind.* In particular, they proved that the equation

$$x^n + y^n = z^2 \ \ (n \geq 4)$$

has no solutions in pairwise coprime integers x, y, z, with $xyz \neq 0$. The purpose of this paper is to prove a similar result for Lucas sequences of the *first kind* with rational roots.

[1] Research Supported by NSERC

In particular, we want to classify those positive integers n for which the equation

$$\frac{x^n - y^n}{x - y} = z^2 \tag{1.1}$$

has solutions in pairwise coprime integers x, y, z with $xyz \neq 0$, which will be referred to as nontrivial integer solutions.

Theorem 1
(i.) For each $0 \leq n \leq 5$*, equation* (1.1) *has infinitely many nontrivial integer solutions.*
(ii.) For each $n > 5$*, divisible by any of* 2, 3,7,*or* 25*, equation* (1.1) *has no nontrivial integer solutions.*
(iii.) For all other positive integers n*, equation* (1.1) *has finitely many nontrivial integer solutions, and if such a solution exists, then there is a prime* $p \geq 11$ *dividing* n *for which one of the equations*

$$z^2 = \frac{x^p - y^p}{x - y}, \quad pz^2 = \frac{x^p - y^p}{x - y}$$

has a nontrivial integer solution.

The proof of this result will make use of an array of existing results related to the modularity of elliptic curves, and also recent extensions of Chabauty's result. We remark that the *abc* conjecture implies that there are no solutions for n sufficiently large, and if one is willing to believe a certain effective version of the *abc* conjecture, then one could deduce from it that there are no solutions for $n > 8$. We therefore make the following

Conjecture 1 *For* $n > 5$*, equation* (1.1) *has no nontrivial integer solutions.*

2. Proof of Theorem 1

The proof of the first part of the theorem is trivial for $0 \leq n \leq 3$. For $n = 4$, we must show that the Diophantine equation $z^2 = x^3 + x^2y + xy^2 + y^3$ has infinitely many solutions. Indeed it is a curve of genus zero, with parametric solutions given by the polynomials

$$x(u, v) = 4uv(u^2 - 2uv + 2v^2), y(u, v) = u^4 - 4u^3v + 4u^2v^2 - 8uv^3 + 4v^4$$

$$z(u, v) = u^6 - 4u^5v + 10u^4v^2 - 20u^2v^4 + 16uv^5 - 8v^6,$$

and moreover, $x(u, v)$ and $y(u, v)$ are coprime integers for nonzero coprime integers u and v. Hence there are infinitely many nontrivial solutions when $n = 4$. We now consider the case $n = 5$. Nontrivial integer solutions to (1.1), with $n = 5$, are in correspondence with rational points on the curve

$$C_4 : \; y^2 = x^4 + x^3 + x^2 + x + 1.$$

This curve is birational to the elliptic curve

$$E: \ Y^2 = X^3 - 5X^2 - 45X + 25.$$

The point $(X, Y) = (-1, 8)$ does not have order less than or equal to 12, and so by Mazur's theorem on rational torsion, $E(\mathbf{Q})$ has positive rank, from which the stated result follows in the case $n = 5$.

Throughout the remainder of the proof we will assume that $x > y$ for any solution to (1.1). We now consider the case that $n > 5$ and even. The case $n = 6$ must be dealt with first, and then all other such values of n can be dealt with by a different argument. For $n = 6$, the left-hand side of (1.1) factors as

$$(x^2 + xy + y^2)(x^3 + y^3),$$

and since these two factors are coprime, there are integers u, v for which

$$x^3 + y^3 = u^2, x^2 + xy + y^2 = v^2.$$

All integer solutions to the first of these two equations are given parametrically by 5 homogeneous polynomials of degree 4; $x = F_i(X, Y), y = G_i(X, Y), i = 1, ..., 5$ (see [5], p.235), and upon substitution into the second equation leads to integer points on the 4 curves (because of duplication)

$$v^2 = X^8 - 4X^7Y + 16X^6Y^2 + 16X^5Y^3 - 28X^4Y^4 - 32X^3Y^5 + 64X^2Y^6 + 32XY^7 + 16Y^8,$$

$$v^2 = X^8 + 20X^7Y + 184X^6Y^2 + 960X^5Y^3 + 3012X^4Y^4 + 5760X^3Y^5 + 6624X^2Y^6$$
$$+4320XY^7 + 1296Y^8,$$
$$v^2 = X^8 + 102X^4Y^4 + 9Y^8,$$
$$v^2 = 7X^8 - 4X^7Y - 8X^6Y^2 - 28X^5Y^3 + 82X^4Y^4 - 28X^3Y^5 - 8X^2Y^6 - 4XY^7 + 7Y^8.$$

The first two polynomials factor over the integers into two quartics. By checking the appropriate resultant, one can deduce that there is a point on a corresponding curve of genus one defined by $v_1^2 = g(x)$, where g is a quartic factor of the dehomogenized polynomial of degree 8, and in both cases, one of the two elliptic curves so determined has rank zero over the rationals, and one easily deduces that there are no solutions to (1.1) arising from these two cases. The last of the four curves can be transformed to the third by a linear change of variables, hence we must only deal with the third curve. But this curve has the elliptic cover $v_1^2 = X^4 + 102X^2 + 9$, which is birational to the curve $y^2 = x^3 - 51x^2 + 648x$, which has rank zero over the rationals, and hence does not lead to any solutions of (1.1). The rank of the curve $y^2 = x^3 - 51x^2 + 648x$ was computed using Ian Connell's APECS program.

For $n > 6$ and even, $n = 2m$ say, then (1.1) can be written as

$$z^2 = (x^m - y^m)/(x - y) \cdot (x^m + y^m),$$

from which it follows that $x^m + y^m = u^2$ or $x^m + y^m = 2u^2$ for some integer u. By the aforementioned result of Darmon and Merel, the first equation has no nontrivial integer solutions. By a recent result of Bennett and Skinner [1], the equation $x^m + y^m = 2u^2$ has no solutions in nonzero pairwise coprime integers x, y, u, with $x > y$.

Our attention is now restricted to the case that n is odd. We now consider the case that 3 divides n. Let $n = 3t$ for $t > 2$ and odd, and assume first that 3 does not divide t. Then (1.1) gives

$$z^2 = (\frac{x^{3t} - y^{3t}}{x^t - y^t})(\frac{x^t - y^t}{x - y}),$$

and it follows that there are integers u, v for which either

$$\frac{x^{3t} - y^{3t}}{x^t - y^t} = u^2, \ \frac{x^t - y^t}{x - y} = v^2,$$

or

$$\frac{x^{3t} - y^{3t}}{x^t - y^t} = 3u^2, \ \frac{x^t - y^t}{x - y} = 3v^2.$$

By our assumption that 3 does not divide t, and the fact that t is odd, the latter case is not possible because $\frac{x^t - y^t}{x - y}$ is not divisible by 3. In the former case, we see that

$$u^2 = x^{2t} + x^t y^t + y^{2t}.$$

Since one of x or y is odd, we will assume without loss of generality that y is odd. Completing the square of the last equation yields

$$4u^2 = (2x^t + y^t)^2 + 3y^{2t}.$$

Writing $3y^{2t}$ as a difference of squares, we obtain

$$3y^{2t} = (2u - (2x^t + y^t))(2u + 2x^t + y^t).$$

If p is a prime which divides these two factors, then p divides $3y$ and p divides $2(2x^t + y^t)$, and so because $(x, y) = 1$, it follows that $p = 2$ or $p = 3$. We show that the case $p = 3$ is not possible. If 3 were a factor of both $2u - (2x^t + y^t)$ and $2u + 2x^t + y^t$, then 3^2 would necessarily divide $3y^{2t}$, hence 3 would divide y. Also, 3 would be a factor of $2(2x^t + y^t)$, hence it follows that 3 is a factor of x, contradicting $(x, y) = 1$. If $p = 2$ were a divisor of both $2u - (2x^t + y^t)$ and $2u + 2x^t + y^t$, then 2 would necessarily divide y, contradicting our earlier assumption that y is odd.

Therefore, there are coprime integers a, b, with $y = ab$, such that

$$2u - (2x^t + y^t) = 3^\mu a^{2t}, 2u + 2x^t + y^t = 3^\nu b^{2t},$$

where $(\mu, \nu) = (1, 0)$ or $(0, 1)$. We will assume that $(\mu, \nu) = (1, 0)$, as a similar argument deals with the other case. Upon taking the difference of the two equations in the last expression, we see that

$$b^{2t} - 3a^{2t} = 2(2x^t + y^t) = 2(2x^t + a^t b^t),$$

and so

$$b^{2t} - 2a^t b^t - 3a^{2t} = 4x^t.$$

The expression on the left factors, showing that

$$4x^t = (b^t - 3a^t)(a^t + b^t).$$

The corresponding factors on the right have no common divisor, except possibly a power of two, and so we find that

$$a^t + b^t = 2^\alpha c^t$$

for some integers c, and $\alpha \geq 0$. By the results of Wiles [9], and Taylor and Wiles [8], for $\alpha = 0$, Ribet [7] for $\alpha > 1$, and Darmon and Merel [4] for $\alpha = 1$, (1.1) has no nontrivial solutions in this case.

We now consider the case that $n = 9t$, where $t \geq 1$ and is not divisible by 2 or 3. In this case (1.1) gives

$$z^2 = (\frac{x^{9t} - y^{9t}}{x^t - y^t})(\frac{x^t - y^t}{x - y}).$$

As in the previous case, this implies that

$$\frac{x^{9t} - y^{9t}}{x^t - y^t} = u^2,$$

for some nonzero integer u. The result will follow by showing that equation (1.1) has no nontrivial solutions at $n = 9$. If it did, then from the factorization

$$\frac{x^9 - y^9}{x - y} = (\frac{x^3 - y^3}{x - y})(x^6 + x^3 y^3 + y^6),$$

there is an integer v for which

$$\epsilon v^2 = x^6 + x^3 y^3 + y^6,$$

with $\epsilon \in \{1,3\}$, and these equations were shown to have no solutions in section 2 of [6].

We deal finally with the case that 27 divides n. In this case (1.1) gives

$$z^2 = (\frac{x^{27t}-y^{27t}}{x^{3t}-y^{3t}})(\frac{x^{3t}-y^{3t}}{x-y}),$$

and it follows that there is a nonzero integer u for which

$$\epsilon u^2 = \frac{x^{27t}-y^{27t}}{x^{3t}-y^{3t}},$$

with $\epsilon \in \{1,3\}$. By the remarks of the previous paragraph, we must have $\epsilon = 3$. Since 3 divides $x^{27t}-y^{27t}$, 3 must divide $x^{3t}-y^{3t}$, as the mapping $x \to x^3$ is injective on the integers modulo 3. Let $a \geq 1$ be the highest power of 3 dividing $x^{3t}-y^{3t}$. The binomial theorem shows that $a+2$ is the highest power of 3 dividing $x^{27t}-y^{27t}$, and so 3 cannot divide $\frac{x^{27t}-y^{27t}}{x^{3t}-y^{3t}}$ to an odd power.

To complete the proof of the theorem, we require the following simple observation.

Lemma 1 *Let $l \geq 7$ denote a prime number, or $l = 25$. If the equations*

$$z^2 = \frac{x^l-y^l}{x-y}, \;\; lz^2 = \frac{x^l-y^l}{x-y} \;\; (l \neq 25)$$

$$z^2 = \frac{x^l-y^l}{x-y}, \;\; (l = 25)$$

have no nontrivial solutions, then the equations

$$z^2 = \frac{x^{kl}-y^{kl}}{x-y}$$

have no nontrivial solutions for all $k \geq 1$.

Proof We may assume that k is odd. If there is a nontrivial solution to $z^2 = \frac{x^{kl}-y^{kl}}{x-y}$, then

$$z^2 = (\frac{x^{kl}-y^{kl}}{x^k-y^k})(\frac{x^k-y^k}{x-y}),$$

and it follows from a resultant computation that the greatest common divisor of the two factors is either 1 or l (1 if $l = 25$). Therefore, $\frac{x^{kl}-y^{kl}}{x^k-y^k}$ is either a square, or l times a square (a square if $l = 25$), contradicting the hypotheses given.

To complete the proof of the theorem, it suffices to show that the two equations

$$z^2 = \frac{x^7 - y^7}{x - y}, \;\; 7z^2 = \frac{x^7 - y^7}{x - y},$$

and the equation

$$z^2 = \frac{x^{25} - y^{25}}{x - y},$$

have no nontrivial integer solutions. Equivalently, it must be shown that that the set of (finite) rational points on the curves

$$y^2 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \text{ and } y^2 = x^{24} + x^{23} + \cdots + x + 1$$

are $\{(-1, \pm 1), (0, \pm 1)\}$ and $\{(1, \pm 5), (-1, \pm 1), (0, \pm 1)\}$ respectively, and that the only finite rational point on the curve

$$7y^2 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

is $\{(1, 1)\}$.

This was achieved by N. Bruin using his implementation of the effective Chabauty method in MAGMA. The details of the computation can be found in [3]. For details on the effective Chabauty method for determining the set of rational points on a curve, we refer the reader to a recent paper by Bruin [2].

It is worth noting that one could improve upon the main result of this paper by determining the set of rational points on the curves

$$y^2 = x^{p-1} + x^{p-2} + \cdots + x + 1, \;\; py^2 = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

where $p > 7$ is prime. In particular, by doing so, the main result would be improved in such a way as to include all indices divisible by the prime p.

Acknowledgements The author gratefully acknowledges the help of Nils Bruin, who performed the MAGMA computations required to show that the main result holds for all indices divisible by either 7 or 25. The author's research is supported by the Natural Sciences and Engineering Research Council of Canada.

References

[1] M.A. Bennett and C.M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms,* To appear in Canad. J. Math.

[2] N. Bruin, *Chabauty methods using elliptic curves,* J. Reine Angew. Math. **562** (2003), 27-49.

[3] N. Bruin *Explicit MAGMA computations on certain cyclotomic curves,* (see http://members.rogers.com/superprof/bruin.html)

[4] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's Last Theorem,* J. Reine Angew. Math. **490** (1997), 81-100.

[5] L.J. Mordell, *Diophantine Equations,* Academic Press, New York, 1969.

[6] B. Poonen, *Some Diophantine equations of the form $x^n + y^n = z^m$*, Acta Arith. **86** (1998), 193-205.

[7] K. Ribet, *On the equation $a^p + 2^\alpha b^p + c^p = 0$*, Acta Arith. **79** (1997), 7-16.

[8] R.L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras,* Ann. of Math. **141** (1995), 553-572.

[9] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem,* Ann. of Math. **141** (1995), 443-551.

P.G. Walsh

Department of Mathematics

University of Ottawa

585 King Edward

Ottawa, Ontario, Canada

K1N-6N5

gwalsh@mathstat.uottawa.ca