ACTA ARITHMETICA
105.4 (2002)

Lucas' square pyramid problem revisited

by

Michael A. Bennett (Urbana, IL)

1. Introduction

Une pile de boulets à base carée ne contient un nombre de boulets égal au carré d'un nombre entier que lorsqu'elle en contient vingt-quatre sur le côté de la base (Édouard Lucas [24]).

This assertion of Lucas, made first in 1875, amounts to the statement that the only solutions in positive integers (s,t) to the Diophantine equation

$$1^2 + 2^2 + \ldots + s^2 = t^2 \tag{1.1}$$

are given by $(s,t) = (1,1)$ and $(24,70)$. Putative solutions by Moret-Blanc [30] and Lucas [25] contain fatal flaws (see e.g. [39] for details) and it was not until 1918 that Watson [39] was able to completely solve equation (1.1). His proof depends upon properties of elliptic functions of modulus $1/\sqrt{2}$ and arguably lacks the simplicity one might desire. A second, more algebraic proof was found in 1952 by Ljunggren [23], though it also is somewhat on the complicated side. Attempts to repair this perceived defect have, in recent years, resulted in a number of elementary proofs, by Ma [26] and [27], Cao and Yu [6], Cucurezeanu [10] and Anglin [2]. Various generalizations, distinct from that considered here, have been addressed in [12] and [33].

We rewrite equation (1.1) as

$$\frac{s(s+1)(2s+1)}{6} = t^2$$

and, multiplying by 24 and setting $x = 2s, y = 2t$, find that

$$x(x+1)(x+2) = 6y^2. \tag{1.2}$$

In this paper, we will consider the generalization of this equation obtained by replacing the constant 6 in (1.2) by an arbitrary squarefree integer n; viz.

$$x(x+1)(x+2) = ny^2. \tag{1.3}$$

2000 *Mathematics Subject Classification*: Primary 11D25, 11J86.

Supported in part by NSF Grant DMS-9700837.

This corresponds to finding integral "points" on quadratic twists of the elliptic curve $y^2 = u^3 - u$. We begin by proving a general upper bound on the number of integral solutions to (1.3) which implies Lucas' problem as a special case.

2. Solutions to equation (1.3). If b and d are positive integers, let us denote by $N(b,d)$ the number of solutions in positive integers (x, y) to the Diophantine equation

$$b^2x^4 - dy^2 = 1. \tag{2.1}$$

Our first result is the following:

THEOREM 2.1. *If n is a squarefree positive integer, then equation* (1.3) *has precisely*

$$\sum N(b,d) \leq 2^{\omega(n)} - 1$$

solutions in positive integers x and y. Here, the summation runs over positive integers b and d with $bd = n$ and $\omega(n)$ denotes the number of distinct prime factors of n.

Proof. From (1.3), we may write

$$x = 2^\delta au^2, \quad x+1 = bv^2, \quad x+2 = 2^\delta cw^2$$

where a, b, c, u, v and w are positive integers, $\delta \in \{0, 1\}$ and

$$(a,b) = (a,c) = (b,c) = 1.$$

If we set $d = ac$, it follows that

$$b^2v^4 - d(2^\delta uw)^2 = 1$$

where $bd = n$. Conversely, if X and Y are positive integers for which $b^2X^4 - dY^2 = 1$, where b and d are positive integers with $bd = n$, writing $x = bX^2 - 1$ and $y = XY$, we find that

$$x(x+1)(x+2) = bdy^2 = ny^2.$$

To prove the inequality in Theorem 2.1, we note, since we assume n to be squarefree, that there are precisely $2^{\omega(n)}$ pairs of positive integers (b, d) with $bd = n$. Since $N(b, 1) = 0$, the stated bound is essentially a consequence of theorems of Cohn [9] and the author and Gary Walsh [3]. To state this result, we require some notation. Let $d > 1$ be a squarefree integer and let $T + U\sqrt{d}$ be the fundamental solution to $X^2 - dY^2 = 1$; i.e. T and U are the smallest positive integers with $T^2 - dU^2 = 1$. Define T_k and U_k via the equation

$$T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$$

and let the *rank of apparition* $\alpha(b)$ be the smallest positive integer k such that b divides T_k (where we set $\alpha(b) = \infty$ if no such integer exists).

Theorem 2.2. *Let b and d be squarefree positive integers. Then $N(b,d) \leq 1$ unless $(b,d) = (1,1785)$ in which case there are two positive solutions to* (2.1), *given by $(x,y) = (13,4)$ and $(239,1352)$. If $N(b,d) = 1$, so that* (2.1) *has a solution in positive integers (x,y), then, if $b = 1$, we may conclude that $x^2 \in \{T_1, T_2\}$. If, on the other hand, $b > 1$, then $bx^2 = T_{\alpha(b)}$.*

For $n = 1785 = 3 \cdot 5 \cdot 7 \cdot 17$, it remains to show that (1.3) has at most 15 positive integral solutions (x,y). This is immediate from Theorem 2.2 upon noting that (2.1) is insoluble modulo 3 if $(b,d) = (255,7)$. ∎

Since (1.2) has the solutions

$$(x,y) = (1,1),\ (2,2),\ \text{and } (48,140),$$

we conclude from Theorem 2.1 that it has no others with x and y positive. These lead to precisely the solutions $(s,t) = (1,1)$ and $(24,70)$ in Lucas' original problem.

Theorem 2.1 implies that equation (1.3) has at most a single solution in positive integers, if n is prime. In fact, work of Ljunggren [23] on $N(1,p)$ immediately enables one to strengthen this:

Corollary 2.3. *If n is prime, then equation* (1.3) *has no solutions in positive integers x and y, unless $n \in \{5, 29\}$. In each of these cases, there is precisely one such solution, given by $(x,y) = (8,12)$ and $(9800, 180180)$, respectively.*

It is reasonable to suppose that the dependence in Theorem 2.1 on $\omega(n)$ is an artificial one. Indeed, a conjecture of Lang (see e.g. Abramovich [1] and Pacelli [32]) implies that the number of integral solutions to (1.3) should be absolutely bounded. We present some computations in support of this in our final section.

3. Congruent numbers. A positive integer n is called a *congruent number* if there exists a right triangle with sides of rational length and area n. It is a classical result (and elementary to prove; see e.g. Chahal [8, Theorems 1.34 and 7.24]) that n is congruent precisely when the elliptic curve

$$E_n: \quad Y^2 = X^3 - n^2 X$$

has positive Mordell rank; i.e. $E_n(\mathbb{Q})$ is infinite. This leads to

Proposition 3.1. *If n is a positive integer for which equation* (1.3) *has a solution in positive $x, y \in \mathbb{Q}$, then n is a congruent number or, equivalently, $E_n(\mathbb{Q})$ has positive rank.*

Proof. As is well known (see e.g. [8, Corollary 7.23]), the torsion subgroup of $E_n(\mathbb{Q})$ consists of the point at infinity, together with $(0,0), (n,0)$ and $(-n,0)$ (i.e. the obvious points of order 2). If we write $X = n(x+1)$

and $Y = n^2 y$, it follows that a positive rational solution (x, y) to (1.3) corresponds to a point with positive rational coordinates (X, Y) on E_n, which is necessarily of infinite order. By our above remarks, this implies that n is a congruent number. ■

In [7], Chahal applied an identity of Desboves to show that there are infinitely many congruent numbers in each residue class modulo 8 (and, in particular, infinitely many squarefree congruent numbers, congruent to $1, 2, 3, 5, 6$ and 7 modulo 8). We can generalize this as follows:

THEOREM 3.2. *If m is a positive integer and a is any integer, then there exist infinitely many (not necessarily squarefree) congruent numbers n with $n \equiv a \pmod{m}$. If, further,* $\gcd(a, m)$ *is squarefree, then there exist infinitely many (squarefree) congruent numbers n with $n \equiv a \pmod{m}$.*

Proof. Suppose that l is a positive integer and set

$$n = m^4 l^3 - l = (m^2 l - 1)(m^2 l + 1) l.$$

It follows that $(x, y) = (m^2 l - 1, m)$ is a positive solution to (1.3). Since $n \equiv -l \pmod{m}$, every $l \equiv -a \pmod{m}$ yields a value of n with $n \equiv a \pmod{m}$ and, by Proposition 3.1, n congruent. If, further, $\gcd(a, m)$ is squarefree, we may apply work of Mirsky [28] to conclude that n is squarefree for infinitely many $l \equiv -a \pmod{m}$. Indeed, if we write $l = mk - a$ for $k \in \mathbb{N}$, and denote by $N(X)$ the cardinality of the set of positive integers $k \le X$ for which n is squarefree, Theorems 1 and 2 of [28] show that

$$N(X) = AX + O(X^{2/3+\varepsilon}) \quad \text{as } X \to \infty,$$

for any $\varepsilon > 0$. Here $A = A(a, m) > 0$ is a computable constant. ■

It is worth remarking that a much more refined version of the above result should follow from the work of Gouvea and Mazur [11].

4. Quartic equations. There is a vast literature on equations of the form $Ax^4 - By^2 = \pm 1$ (the reader is directed to the survey paper of Walsh [38] for more details). In particular, there are many papers giving explicit characterizations of $N(b, d)$ when $\omega(bd)$ is suitably small (see e.g. [4], [5], [13]–[19]). The preceding observations (specifically Theorem 2.1 and Proposition 3.1) imply that $N(b, d) = 0$ whenever bd is noncongruent. Together with criteria for noncongruent numbers (see e.g. Table 3.8 of [34]), this enables one to recover many classical vanishing results for $N(b, d)$. It also leads to various new statements, the simplest of which is the following:

COROLLARY 4.1. *If b and d are positive integers with $bd = 2pq$, where p and q are distinct primes with $p \equiv q \equiv 5 \pmod{8}$, then equation* (2.1) *has no solution in positive integers x and y.*

For the state of the art on the problem of determining congruent numbers, the reader is directed to, for example, [29], [31] and [36]. A good overview of this subject can be found in [20].

5. Computations. Given $n \in \mathbb{N}$, as noted previously, the set of positive integer solutions to (1.3) corresponds to a subset of the integer "points" on E_n. We could thus apply standard computational techniques based either on the solution of Thue equations (see e.g. [37]) or on lower bounds for linear forms in elliptic logarithms (see e.g. [35]) to find all integer solutions (X, Y) to $Y^2 = X^3 - n^2 X$ and check to see which, if any, yield solutions to (1.3). To find positive integral solutions to (1.3), for all squarefree n up to some bound, say $n \leq N$, it is computationally much more efficient however, to rely upon Theorem 2.2. With this approach, we begin by computing fundamental units in $\mathbb{Q}(\sqrt{d})$ for each squarefree $d \leq N$ (see e.g. [22]). For each squarefree n, we then retrieve the data for the $2^{\omega(n)} - 1$ quadratic fields corresponding to nontrivial divisors n_1 of n, and determine $N(n_1, n/n_1)$ by combining Theorem 2.2 with the following lemma due to Lehmer [21]:

LEMMA 5.1. *Let $\varepsilon = T + U\sqrt{d}$ be the fundamental solution to $X^2 - dY^2 = 1$, and $T_k + U_k\sqrt{d} = \varepsilon^k$ for $k \geq 1$. Let p be prime and $\alpha(p)$ denote, as before, the rank of apparition of p in the sequence $\{T_k\}$.*

(i) *If $p = 2$ then $\alpha(p) = 1$ or ∞.*
(ii) *If $p > 2$ divides d then $\alpha(p) = \infty$.*
(iii) *If $p > 2$ fails to divide d then either $\alpha(p) \mid \frac{p - (\frac{d}{p})}{2}$ or $\alpha(p) = \infty$.*

Here $\left(\frac{d}{p}\right)$ denotes the usual Legendre symbol.

We carry out this program with $n \leq N = 10^5$ and note that, in each instance, equation (1.3) has at most three solutions in positive integers x and y. In fact, of the 60794 squarefree n, $1 \leq n \leq 10^5$, only 280 corresponding equations of the shape (1.3) possess positive solutions. Moreover, only for

$$n = 6, 210, 546, 915, 1785, 7230, 13395, 16206, 17490, 20930, 76245$$

do we find more than a single such solution (with the first two values having three positive solutions and the remaining ones having two apiece).

Acknowledgements. The author would like to thank Adolf Hildebrand and Marcin Mazur for various helpful and insightful comments.

References

[1] D. Abramovich, *Uniformity of stably integral points on elliptic curves*, Invent. Math. 127 (1997), 307–317.
[2] W. S. Anglin, *The square pyramid puzzle*, Amer. Math. Monthly 97 (1990), 120–124.

[3] M. A. Bennett and P. G. Walsh, *The Diophantine equation* $b^2X^4 - dY^2 = 1$, Proc. Amer. Math. Soc. 127 (1999), 3481–3491.
[4] Z. F. Cao, *On the Diophantine equations* $x^2 + 1 = 2y^2$, $x^2 - 1 = 2Dz^2$, J. Math. (Wuhan) 3 (1983), 227–235 (in Chinese).
[5] Z. F. Cao and Y. S. Cao, *Solutions of a class of Diophantine equations*, Heilongjiang Daxue Ziran Kexue Xuebao 1985, 22–27 (in Chinese).
[6] Z. F. Cao and Z. Y. Yu, *On a problem of Mordell*, Kexue Tongbao 30 (1985), 558–559.
[7] J. Chahal, *On an identity of Desboves*, Proc. Japan Acad. Ser. A Math. Sci. 60 (1984), 105–108.
[8] —, *Topics in Number Theory*, Plenum Press, New York, 1988.
[9] J. H. E. Cohn, *The Diophantine equation* $x^4 - Dy^2 = 1$, *II*, Acta Arith. 78 (1997), 401–403.
[10] I. Cucurezeanu, *An elementary solution of Lucas' problem*, J. Number Theory 44 (1993), 9–12.
[11] F. Gouvea and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. 4 (1991), 1–23.
[12] K. Győry, R. Tijdeman and M. Voorhoeve, *On the equation* $1^k + 2^k + \ldots + x^k = y^z$, Acta Arith. 37 (1980), 233–240.
[13] C. D. Kang, D. Q. Wan and G. F. Chou, *On the Diophantine equation* $x^4 - Dy^2 = 1$, J. Math. Res. Exposition 3 (1983), 83–84.
[14] C. Ko and Q. Sun, *The Diophantine equation* $x^4 - pqy^2 = 1$, Kexue Tongbao 24 (1979), 721–723 (in Chinese).
[15] —, —, *On the Diophantine equation* $x^4 - Dy^2 = 1$, *I*, Sichuan Daxue Xuebao 1979, 1–4 (in Chinese).
[16] —, —, *On the Diophantine equation* $x^4 - Dy^2 = 1$, *II*, Chinese Ann. Math. 1 (1980), 83–89 (in Chinese).
[17] —, —, *On the Diophantine equation* $x^4 - Dy^2 = 1$, Acta Math. Sinica 23 (1980), 922–926 (in Chinese).
[18] —, —, *On the Diophantine equation* $x^4 - pqy^2 = 1$, *II*, Sichuan Daxue Xuebao 1980, 37–44 (in Chinese).
[19] —, —, *On the Diophantine equation* $x^4 - 2py^2 = 1$, ibid. 1983, 1–3 (in Chinese).
[20] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, 1993.
[21] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), 419–448.
[22] H. W. Lenstra, Jr., *On the calculation of regulators and class numbers of quadratic fields*, in: London Math. Soc. Lecture Note Ser. 56, Cambridge Univ. Press, Cambridge, 1982, 123–150.
[23] W. Ljunggren, *New solution of a problem proposed by E. Lucas*, Norsk Mat. Tidsskr. 34 (1952), 65–72.
[24] É. Lucas, *Problem 1180*, Nouvelles Ann. Math. (2) 14 (1875), 336.
[25] —, *Solution to Problem 1180*, ibid. 16 (1877), 429–432.
[26] D. G. Ma, *An elementary proof of the solutions to the Diophantine equation* $6y^2 = x(x+1)(2x+1)$, Sichuan Daxue Xuebao 1985, 107–116 (in Chinese).
[27] —, *On the Diophantine equation* $6Y^2 = X(X+1)(2X+1)$, Kexue Tongbao (English ed.) 30 (1985), 1266.
[28] L. Mirsky, *On a problem in the theory of numbers*, Simon Stevin 26 (1948), 25–27.
[29] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z. 204 (1990), 45–67.
[30] Moret-Blanc, Nouvelles Ann. Math. (2) 15 (1876), 46–48.

[31] F. R. Nemenzo, *All congruent numbers less than* 40000, Proc. Japan Acad. Ser. A Math. Sci. 74 (1998), 29–31.
[32] P. L. Pacelli, *Uniform bounds for stably integral points on elliptic curves*, Proc. Amer. Math. Soc. 127 (1999), 2535–2546.
[33] J. J. Schäffer, *The equation* $1^p + 2^p + \ldots + n^p = m^q$, Acta Math. 95 (1956), 155–189.
[34] P. Serf, *Congruent numbers and elliptic curves*, in: Computational Number Theory (Debrecen, 1989), de Gruyter, Berlin, 1991, 227–238.
[35] R. J. Stroeker and N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. 67 (1994), 177–196.
[36] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. 72 (1983), 323–334.
[37] N. Tzanakis and B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory 31 (1989), 99–132.
[38] P. G. Walsh, *Diophantine equations of the form* $aX^4 - bY^2 = \pm 1$, in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), de Gruyter, Berlin, 2000, 531–554.
[39] G. N. Watson, *The problem of the square pyramid*, Messenger of Math. 48 (1918), 1–22.

Department of Mathematics
University of Illinois
Urbana, IL 61801, U.S.A.
E-mail: mabennet@math.uiuc.edu

Received on 29.5.2001 (4041)