ACTA ARITHMETICA
126.2 (2007)

Sharp bounds for the number of solutions to simultaneous Pellian equations

by

P. G. Walsh (Ottawa)

1. Introduction. In [1], Bennett proved that the system of Pell equations

$$x^2 - ay^2 = z^2 - by^2 = 1$$

has at most three solutions in positive integers x, y, z. Since then, the result has been improved by Bennett, Cipu, Mignotte and Okazaki in [2], wherein it was shown that this system has at most two solutions in positive integers, which is best possible. The situation is somewhat different for the system of Pell equations

$$x^2 - ay^2 = y^2 - bz^2 = 1,$$

which conjecturally has at most one positive integer solution. The best known general bound for the number of positive integer solutions to this system of equations is 2, proved recently by Cipu and Mignotte in [4]. Progress has recently been made by Yuan in [14], in which it was proved that for $a = 4t(t+1)$, the system has at most one solution.

The purpose of this paper is to consider the more general system of Pellian equations

$$x^2 - (M^2 - c)y^2 = c, \quad y^2 - bz^2 = 1, \quad c \in \{\pm 1, \pm 2, \pm 4\}, \tag{1.1}$$

where M and $b > 1$ are positive integers with b squarefree, and $M^2 - c$ is a positive nonsquare integer. This is motivated not only by the work of Yuan in [14], but also by a recent paper of Katayama and Levesque [7]. In particular, they considered the case $c = -4$, and proved that under the assumption that the number of distinct prime factors of b is at most 4, the system (1.1) has at most one solution in positive integers. They also proved that a substantially stronger result follows from the *abc* conjecture. We prove here the following.

2000 *Mathematics Subject Classification*: Primary 11D25.

Theorem 1.1. *If M, b, c are fixed integers as described above, then the system of Pell equations* (1.1) *has at most one solution in positive integers* x, y, z.

There are many examples of equations of the form (1.1) which have a solution in positive integers. For instance, if $c = 4$ and $b = M^2 - 1$, then the system has the solution $(x, y, z) = (M^2 - 2, M, 1)$. Also, if $c = 1$ and $b = 4M^2 - 1$, then $(X, Y, Z) = (2M^2 - 1, 2M, 1)$ is a solution to (1.1). Consequently, the upper bound of one solution given in Theorem 1.1 is in fact best possible.

2. Preliminary results. Throughout the paper, $c \in \{\pm 1, \pm 2, \pm 4\}$. Let $M \geq 1$ denote a positive integer, which is odd if c is even, and for which $M^2 - c$ is a positive nonsquare integer. Let

$$\alpha = \frac{M + \sqrt{M^2 - c}}{\sqrt{|c|}}, \tag{2.1}$$

and for $i \geq 1$, define sequences $\{V_i\}$ and $\{W_i\}$ by

$$\alpha^i = \frac{V_i + W_i\sqrt{M^2 - c}}{\sqrt{|c|}}. \tag{2.2}$$

Also, for $b > 1$ and squarefree, let $\beta = T + U\sqrt{b}$ denote the smallest unit greater than 1 in $\mathbb{Z}[\sqrt{b}]$ which is of norm 1, and for $j \geq 1$, let

$$\beta^j = T_j + U_j\sqrt{b}.$$

The following is similar to Lemma 2.1 of [14]. The proof of these statements follows from the binomial theorem.

Lemma 2.1.

(i) *If* $|c| = 4$, *then* V_i *and* W_i *are both even if* 3 *divides* i, *and both odd otherwise.*
(ii) W_i *divides* W_j *if and only if* i *divides* j.
(iii) V_i *divides* V_j *if and only if* i/j *is an odd integer.*
(iv) *If* $d = \gcd(i, j)$, *then* $\gcd(W_i, W_j) = W_d$.
(v) *If* $d = \gcd(i, j)$, *then* $\gcd(V_i, V_j) = V_d$ *if* i/d *and* j/d *are odd integers, and* 1 *otherwise.*
(vi) $W_{2i} = V_iW_i$ *if* c *is even, and* $W_{2i} = 2V_iW_i$ *if* c *is odd.*

The following is similar to Lemmas 2.2 and 2.3 from [14]. The proof follows from direct computation, and taking into consideration the facts in the previous lemma.

Lemma 2.2. *Let* k_0, k_1, k_2 *and* q *be positive integers with* $k_2 = 2qk_1 \pm k_0$ *and* $0 \leq k_0 \leq k_1$. *Then*

(i) *If* $|c| \neq 4$, *or if* $|c| = 4$ *and* V_{k_1} *is odd*, *then* $V_{k_2} \equiv \pm V_{k_0} \pmod{V_{k_1}}$.
(ii) *If* $|c| = 4$ *and* V_{k_1} *is even*, *then* $V_{k_2} \equiv \pm V_{k_0} \pmod{V_{k_1}/2}$.
(iii) *If* $|c| \neq 4$, *or if* $|c| = 4$ *and* W_{k_1} *is odd*, *then* $W_{k_2} \equiv \pm W_{k_0} \pmod{W_{k_1}}$.
(iv) *If* $|c| = 4$ *and* W_{k_1} *is even*, *then* $W_{k_2} \equiv \pm W_{k_0} \pmod{W_{k_1}/2}$.

The following is similar to Lemma 2.4 of [14], and is the vital observation underlying the method of this paper. We will provide the details of the proof for $c = -4$, as this is the case that presents the most difficulty.

Assume that (1.1) has a solution in positive integers. Let (x_0, y_0, z_0) denote the solution to (1.1) with z_0 minimal. Let k_0, l_0 denote the positive integers for which $y_0 = W_{k_0}$ and $z_0 = U_{l_0}$. Also, (x, y, z) will denote a different solution to (1.1), and k and l will denote positive integers for which $y = W_k$, and $z = U_l$.

LEMMA 2.3. *Assume that* (M, b) *is not one of* $\{(1,2),(1,3),(1,15)\}$. *Then* $y_0 \mid y$, $z_0 \mid z$, *and* k/k_0 *and* l/l_0 *are odd integers.*

Proof. Assume that k/k_0 and l/l_0 are not odd integers. Then there are integers s, q, t, q_1 for which $0 \leq s < k_0$, $k = 2qk_0 \pm s$, $0 \leq t < l_0, q_1$, and $l = 2q_1 l_0 \pm t$. We find from Lemma 2.2 that

$$y = W_k \equiv \pm W_s \pmod{W_{k_0}/2^\delta} \equiv \pm W_s \pmod{y_0/2^\delta},$$

where $\delta = 0$ if y_0 is even, and $\delta = 1$ if y is odd. Similarly, by Lemma 2.3 in [14],

$$y = T_l \equiv \pm T_t \pmod{T_{l_0}} \equiv \pm T_t \pmod{y_0}.$$

Therefore,

$$W_s \equiv \pm T_t \pmod{y_0/2^\delta}. \tag{2.3}$$

Since k is odd, s is odd. Since k_0 is odd and larger than s, it follows that $k_0 \geq s + 2$. Therefore, by the assumption that $M > 1$ is odd, and a basic estimate for the growth rate of the sequence $\{W_i\}$, it follows that

$$W_s < (1/4)W_{s+2} \leq (1/4)W_{k_0} = (1/4)y_0.$$

Also, because b is not one of $2, 3$ or 15, the growth rate of the sequence $\{T_i\}$ implies that

$$T_t < (1/4)T_{t+1} \leq (1/4)T_{l_0} = (1/4)y_0.$$

Because of these estimates, we see that the minus sign in (2.3) is not possible. Therefore, $W_s \equiv T_t \pmod{y_0/2^\delta}$ must hold. But in this case, the estimates imply that $W_s = T_t$, which contradicts the fact that (x_0, y_0, z_0) is the smallest solution to (1.1). It follows that at least one of k/k_0 or l/l_0 is an odd integer. By the lemma above, k/k_0 is an odd integer if and only if y_0 divides y, and this occurs if and only if l/l_0 is an odd integer. The lemma follows.

The method also uses, in a fundamental way, the results of Voutier [12] and Bilu, Hanrot and Voutier [3] on the existence of primitive divisors in Lucas sequences. Combining the results of those papers yields the following result. We first remind the reader of the notion of a primitive prime factor.

Definition. Let $\{W_i\}$ be the sequence of integers in (2.2). We say that W_i has a *primitive prime factor* if there is a prime factor of W_i which does not divide W_j for all $1 \le j \le i-1$.

The *rank of apparition* $r(m)$ of a positive integer $m > 1$ in the sequence $\{W_i\}$ is the smallest positive integer i for which m divides W_i. Thus we see that if m is prime, then it is a primitive prime factor of $W_{r(m)}$. The main point of these definitions is the well known result that $m > 1$ divides W_k if and only if $r(m)$ divides k.

Lemma 2.4. *Let α be as in (2.1). Then for $i > 1$, W_i has a primitive prime factor except only if $\alpha = (1+\sqrt{5})/2$ and $i \in \{2, 6, 12\}$.*

We finish off this series of lemmata by a result which combines results of Ljunggren [8], Cohn [6], and the author [13]. It essentially solves the problem of determining all instances when the product of two distinct elements in any sequence $\{W_i\}$ is a square.

Lemma 2.5. *Let $C = 1$ if $|c| = 1$ or $|c| = 2$, and $C = 4$ if $|c| = 4$. For any positive integer A, there is at most one positive integer solution X, Y to*

$$X^2 - (M^2 - c)Y^2 = C \tag{2.4}$$

with $Y = A \cdot u^2$, for some integer u, except only in the following cases.

- (i) *$c = 1$, $A = 1$, $M = 2m^2$, in which case $Y \in \{1, (2m)^2\}$.*
- (ii) *$c = 1$, $A = 1$, $M = 169$, in which case $Y \in \{1, (6214)^2\}$.*
- (iii) *$c = 2$, $A = m_1$ with $M = m_1u^2$, and $M^2 - 1 = 2m^2$, in which case $Y \in \{M, (2m)^2M\}$.*
- (iv) *$c = -2$, $A = m_1$ with $M = m_1u^2$, and $M^2 + 1 = 2m^2$, in which case $Y \in \{1, (2m)^2M\}$.*
- (v) *$c = 4$, $M = 1$, $A = 1$, in which case $Y \in \{1, 144\}$, $M = 1$, $A = 2$, in which case $Y \in \{2, 8\}$, or $M = m^2 > 1$, $A = 1$, in which case $Y \in \{1, m^2\}$.*

Proof. We prove this by considering each value of c separately. We retain the notation from (2.4).

Case 1: $c = 1$. Assume that there are two positive indices $k < l$ for which $W_k = Au^2$ and $W_l = Av^2$ for some positive integers u and v. By a recent improvement to Ljunggren's theorem on the equation $X^2 - DY^2 = 1$ in [11], either $A^2(M^2-1) = 1785$, $A^2(M^2-1) = 16 \cdot 1785$, or else $V_k + Au^2\sqrt{M^2-1}$ is the smallest unit greater than 1 in $\mathbb{Z}[\sqrt{M^2-1}]$ which is of norm 1, and

$V_l + Av^2\sqrt{M^2-1}$ is its square. The equation $A^2(M^2-1) = 1785$ is not solvable, while the equation $A^2(M^2-1) = 16 \cdot 1785$ leads to case (ii) in the statement of the lemma. Finally, if the third possibility occurs, then $V_k + Au^2\sqrt{M^2-1} = M + \sqrt{M^2-1}$ and $V_l + Av^2\sqrt{M^2-1} = 2M^2 - 1 + 2M\sqrt{M^2-1}$. Therefore, $A = 1$, $u = 1$, and $v^2 = 2M$, which implies that $M = 2m^2$ for some integer m, resulting in (i) in the statement of the lemma.

CASE 2: $c = -1$. By the same argument as in the previous case, but appealing directly to Ljunggren's theorem in [8] (or see Theorem 9 on p. 270 in [9]), it follows that $V_k + W_k\sqrt{M^2+1}$ is the fundamental unit in $\mathbb{Z}[\sqrt{M^2+1}]$. This is not possible since the fundamental unit in that ring has norm -1.

CASE 3: $c = \pm 2$. The minimal unit in $\mathbb{Z}[\sqrt{M^2 \pm 2}]$ is $M^2 \pm 1 + M\sqrt{M^2 \pm 2}$, and so the argument given to prove Case 2 shows $Au^2 = M$ and $Av^2 = 2(M^2 \pm 1)M$. This forces $M^2 \pm 1 = 2m^2$ for some positive integer m.

CASE 4: $c = 4$. Assume that $M^2 - 4 > 5$, since the case $M = 1$ is not possible and $M = 3$ was dealt with by Ribenboim in [10]. Assume first that the equation $X^2 - A^2(M^2-4)Y^2 = 4$ is solvable in odd integers X, Y and let

$$\alpha_A = \frac{v_1 + w_1\sqrt{A^2(M^2-4)}}{2}$$

denote its minimal solution. For $i \geq 1$, we let

$$\alpha_A^i = \frac{v_i + w_i\sqrt{A^2(M^2-4)}}{2}.$$

Thus there are integers k_1 and l_1 for which $w_{k_1} = u^2$ and $w_{l_1} = v^2$. By Theorem 3 of [6] applied to $d = A^2(M^2-4)$, we find that $k_1 = 1$, $l_1 = 2$ and furthermore that v_1 is a square. But $v_1 = V_k$, and so applying Theorem 1 of [6], we see that $k = 1$. Therefore, $M = m^2$ for some integer m, $A = 1$, and $W_k = 1$, $W_l = m^2$.

Assume now that the equation $X^2 - A^2(M^2-4)Y^2 = 4$ is not solvable in odd integers X, Y. Let $v_k = V_{3k}/2$ and $w_k = W_{3k}/2$, so that $(X, Y) = (v_k, w_k)$ constitute all solutions to $X^2 - (M^2-4)Y^2 = 1$. By assumption, there are indices k and l for which $w_k = (Au^2)/2$ and $w_l = (Av^2)/2$, and it follows from Theorem 1 in [13], with $D = A^2(M^2-4)$, that $k = 1$ and $l = 2$. This in turn implies that $v_k = 2V_{3k}$ is a square, which is not possible by Theorem 2 of [6].

CASE 5: $c = -4$. Again we may assume that $M^2 + 4 > 5$ by the result of Ribenboim [10]. Assume first that the equation $X^2 - A^2(M^2+4)Y^2 = 4$ is solvable in odd integers X, Y and let

$$\alpha_A = \frac{v_1 + w_1\sqrt{A^2(M^2+4)}}{2}$$

denote its minimal solution. For $i \geq 1$, we let

$$\alpha_A^i = \frac{v_i + w_i\sqrt{A^2(M^2+4)}}{2}.$$

Thus there are integers k_1 and l_1 for which $w_{k_1} = u^2$ and $w_{l_1} = v^2$. By Theorem 3 of [5], this forces $k_1 = 1$ and v_1 to be a square. But $v_1 = V_k$, and so by Theorem 1 of [5], either $k = 1$, or $k = 3$ and $A^2(M^2+4) = 13$. The latter is not possible since k is evidently even.

Assume now that the equation $X^2 - A^2(M^2+4)Y^2 = 4$ is not solvable in odd integers X, Y. Let $v_k = V_{3k}/2$ and $w_k = W_{3k}/2$, so that $(X, Y) = (v_k, w_k)$ constitute all solutions to $X^2 - (M^2+4)Y^2 = 1$. By assumption, there are indices k and l for which $w_k = (Au^2)/2$ and $w_l = (Av^2)/2$, and it follows from Theorem 1 in [13], with $D = A^2(M^2+4)$, that $k = 1$ and $l = 2$. This in turn implies that $v_k = 2V_{3k}$ is a square, which is not possible by Theorem 2 of [6].

3. Proof of Theorem 1.1. Assume that (1.1) is solvable in positive integers, and let (x_0, y_0, z_0) denote the smallest positive integer solution to (1.1). Let (x_1, y_1, z_1) denote a larger solution (specifically meaning that $z_0 < z_1$). Let k_0, l_0, k_1, l_1 be the corresponding powers of α and β, as defined at the start of Section 2.

We will first consider the case $c = 1$ in detail. The proof for the other cases will be given with less detail in order to keep the presentation at a reasonable length.

There are two distinct cases to consider depending on the parity of y_0. Assume first that y_0 is odd. It follows from Lemma 2.3 that y_1 is also odd.

Since y_0 is odd, $x_0 + y_0\sqrt{M^2-1}$ is an odd power of $M + \sqrt{M^2-1}$, and so M divides x_0. Subtracting the second equation in (1.1) from the first yields

$$M^2y_0^2 - x_0^2 = bz_0^2. \tag{3.1}$$

Since M divides x_0 and b is squarefree, it follows that M also divides z_0. Put $X_0 = x_0/M$ and $Z_0 = z_0/M$, then (3.1) becomes

$$y_0^2 - X_0^2 = bZ_0^2.$$

We note that V_{2i+1}/V_1 is an odd integer for all $i \geq 0$, which shows that X_0 is odd, and hence also that Z_0 is even. Therefore, there are positive integers A_0, B_0, u_0, v_0, with $b = A_0B_0$ and $Z_0 = 2u_0v_0$, for which

$$y_0 + X_0 = 2A_0u_0^2, \quad y_0 - X_0 = 2B_0v_0^2. \tag{3.2}$$

Since b is squarefree, we note that $\gcd(A_0, B_0) = 1$. Also, since $\gcd(x_0, y_0) = 1$, it follows that $\gcd(y_0 + X_0, y_0 - X_0) = 2$, which yields $\gcd(A_0u_0^2, B_0v_0^2) = 1$.

From (3.2) we see that $y_0 = A_0u_0^2 + B_0v_0^2$, and so substituting y_0 and $z_0 = 2Mu_0v_0$ into the second equation in (1.1), and then simplifying, gives

$$(A_0u_0^2 + (1-2M^2)B_0v_0^2)^2 - (M^2-1)(2MB_0v_0^2)^2 = 1. \tag{3.3}$$

The symmetry of this equation shows that it can also be written as

$$(B_0v_0^2 + (1-2M^2)A_0u_0^2)^2 - (M^2-1)(2MA_0u_0^2)^2 = 1.$$

Therefore, there is a positive integer i_0 for which $W_{i_0} = 2MB_0v_0^2$. Since M divides W_{i_0}, it follows that i_0 is even. Similarly, there is also an even positive integer j_0 for which $W_{j_0} = MA_0u_0^2$. Similarly, the second solution to (1.1), namely (x_1, y_1, z_1), shows the existence of positive integers $A_1, B_1, u_1, v_1, i_1, j_1$, with i_1 and j_1 even, for which $b = A_1B_1$, $z_1 = 2Mu_1v_1$, $W_{i_1} = 2MB_1v_1^2$, and $W_{j_1} = 2MA_1u_1^2$. We remark that, as with the previous solution, $\gcd(A_1, B_1) = 1$ and $\gcd(A_1u_1^2, B_1v_1^2) = 1$. These remarks concerning greatest common divisors imply by Lemma 2.1 that $\gcd(i_0, j_0) = \gcd(i_1, j_1) = 2$, and that $\gcd(W_{i_0}, W_{j_0}) = \gcd(W_{i_1}, W_{j_1}) = W_2 = 2M$.

By Lemma 2.4, since $i_0 > 1$ and $j_0 > 1$, W_{i_0} and W_{j_0} each have a primitive prime factor, which will be denoted as p and q respectively. By Lemma 2.3, z_0 divides z_1, and since $A_0B_0 = A_1B_1$, it follows that p must divide one of W_{i_1} or W_{j_1}. Therefore, by the remarks concerning the rank of apparition in Section 2, i_0 divides one of i_1 or j_1. Similarly, j_0 divides one of i_1 or j_1.

Assume first that both i_0 and j_0 divide i_1. It follows that W_{i_0} and W_{j_0} divide W_{i_1}, and hence that W_{i_0}/M and W_{j_0}/M divide W_{i_1}/M. We claim that this implies that $A_1 = 1$. If p_1 is a prime dividing A_1, then p_1 divides one of A_0 or B_0, and hence it divides at least one of W_{i_0}/M or W_{j_0}/M. Therefore, p_1 divides W_{i_1}/M. But since A_1 divides W_{j_1}/M, it follows that p_1 divides $\gcd(W_{i_1}/M, W_{j_1}/M)$, which is equal to 2 by the remarks above. Thus, $A_1 = 1$ or $A_1 = 2$. If $A_1 = 2$, then the equation $W_i = 4MX^2$ would be solvable, and since $W_2 = 2M \cdot 1^2$, Theorem 1 of [13] applied to $D = M^2(M^2-1)$ implies that $M = 1$, which is not possible. Therefore, $A_1 = 1$ as claimed. Since $W_{j_1} = 2MA_1u_1^2$, it follows that $W_{j_1} = 2Mu_1^2$, and Lemma 2.5 implies that $j_1 = 2$ and $u_1 = 1$. Therefore, from the construction of the integers A_1, u_1 from y_1, X_1, it follows that $y_1 \pm X_1 = 2$, and since $y_1 \geq 2$, it follows that $y_1 - X_1 = 2$. This implies that $My_1 - x_1 = 2M$, from which it follows that $x_1 = M(y_1 - 2)$. Substituting this for x in the first equation in (1.1) and simplifying gives $y_1 = 4M^2 - 1 = W_3$. Since $y_0 > 1$ and odd, it follows that $y_0 = W_{k_0} \geq W_3 = y_1$, contradicting the fact that $y_0 < y_1$.

We can now assume, without loss of generality, that i_0 divides i_1 and j_0 divides j_1. Then W_{i_0} divides W_{i_1} and W_{j_0} divides W_{j_1}, which implies that $B_0u_0^2$ divides $B_1u_1^2$ and $A_0v_0^2$ divides $A_1v_1^2$. Now suppose that p is a prime dividing $\gcd(B_0, A_1)$; then p divides $\gcd(W_{i_1}/(2M), W_{j_1}/(2M)) = 1$, a contradiction. Therefore, B_0 divides B_1, and a similar argument shows that A_0 divides A_1. Since $A_0B_0 = A_1B_1$, the only way this can occur is if $A_0 = A_1$ and $B_0 = B_1$. By Lemma 2.5, this forces $A_0 = B_0 = 1$, and so $b = 1$, which is not possible.

Now assume that y_0 is even. Then y_1 is also even, and all of x_0, x_1, z_0, z_1 are odd. In this case, the factors of the left side in (3.1) are coprime, and so there are odd positive integers $A_0, B_0, A_1, B_1, u_0, v_0, u_1, v_1$, with $b = A_0B_0 = A_1B_1$, $z_0 = u_0v_0$, $z_1 = u_1v_1$, for which

$$My_i - x_i = A_iu_i^2, \quad My_i + x_i = B_iv_i^2 \quad (i = 0, 1), \tag{3.4}$$

and for $i = 0, 1$, $\gcd(A_i, B_i) = \gcd(u_i, v_i) = 1$. This gives

$$y_i = (A_iu_i^2 + B_iv_i^2)/(2M) \quad (i = 0, 1),$$

and substituting this and $z_i = u_iv_i$ into the second equation in (1.1) and simplifying results in the equation

$$\left(\frac{A_iu_i^2 + (1 - 2M^2)B_iv_i^2}{2M}\right)^2 - (M^2 - 1)B_i^2v_i^4 = 1 \quad (i = 0, 1).$$

By symmetry, one also obtains an identical equation, but with the A_i (resp. u_i) and B_i (resp. v_i) interchanged.

Therefore, there are odd positive indices i_0, j_0, i_1, j_1 for which

$$W_{i_0} = B_0v_0^2, \quad W_{j_0} = A_0u_0^2, \quad W_{i_1} = B_1v_1^2, \quad W_{j_1} = A_1u_1^2.$$

As argued in the previous case, Lemmas 2.3 and 2.4 imply that both W_{i_0} and W_{j_0} divide one of W_{i_1} and W_{j_1}. If they both divide say W_{i_1}, it follows, as argued in the previous case, that $A_1 = 1$. Therefore, $W_{j_1} = u_1^2$ is a square, and by Lemma 2.5, it follows that $W_{j_1} = 1$, which in turn implies by (3.4) that $My_1 - x_1 = 1$. Substituting this quantity into the first equation in (1.1) and simplifying shows that $y_1 = 2M = W_2$. Since y_0 is even, we already knew that $y_0 \geq 2M$, and so this contradicts the fact that $y_0 < y_1$.

We now consider the case $c = -1$. In this case, y_0 and y_1 must be odd, and $X_0 = x_0/M$ and $X_1 = x_1/M$ are odd integers. Adding the two equations in (1.1) and dividing by M gives

$$X_i^2 - y_i^2 = bZ_i^2 \quad (i = 0, 1),$$

where $Z_0 = z_0/M, Z_1 = z_1/M$ are even integers. It follows that there exist positive integers A_0, B_0, A_1, B_1 and u_0, u_1, v_0, v_1 for which $b = A_0B_0 = A_1B_1$, $Z_0 = 2u_0v_0, Z_1 = 2u_1v_1$, and

$$X_i - y_i = 2A_iu_i^2, \quad X_i + y_i = 2B_iv_i^2 \quad (i = 0, 1).$$

Solving for y_i, substituting y_i and z_i in the second equation in (1.1), and then simplifying gives

$$(A_iu_i^2 + (1 + 2M^2)B_iv_i^2)^2 - (M^2 + 1)(2MB_iv_i^2)^2 = 1 \quad (i = 0, 1)$$

and

$$(B_i v_i^2 + (1+2M^2)A_i u_i^2)^2 - (M^2+1)(2MA_i u_i^2)^2 = 1 \quad (i=0,1).$$

The rest of the proof follows exactly as in the case $c = 1$ with y_0 odd, and so we forego the details.

Now assume that $c = 2$, in which case M is assumed to be odd. It follows that y_0 and y_1 are odd, z_0 and z_1 are even, and both $X_0 = x_0/M, X_1 = x_1/M$ are odd integers. Subtracting twice the second equation from the first in (1.1) and dividing by M, gives

$$y_i^2 - X_i^2 = 2bZ_i^2 \quad (i=0,1),$$

where $Z_0 = z_0/M, Z_1 = z_1/M$. It follows that there exist positive integers $A_0, B_0, A_1, B_1, u_0, u_1, v_0, v_1$ for which $2b = A_0B_0 = A_1B_1$, $Z_0 = 2u_0v_0, Z_1 = 2u_1v_1$, and

$$y_i - X_i = 2A_i u_i^2, \quad y_i + X_i = 2B_i v_i^2 \quad (i=0,1).$$

Solving for y_i, substituting y_i and z_i in the second equation in (1.1), and then simplifying gives

$$(A_i u_i^2 + (1-M^2)B_i v_i^2)^2 - (M^2-2)(2MB_i v_i^2)^2 = 1 \quad (i=0,1),$$

and by symmetry

$$(B_i v_i^2 + (1-M^2)A_i u_i^2)^2 - (M^2-2)(2MA_i u_i^2)^2 = 1 \quad (i=0,1).$$

The rest of the proof follows exactly as in the case $c = 1$ with y_0 odd, and so we forego the details.

Now assume that $c = -2$, in which case M is assumed to be odd. It follows that y_0 and y_1 are odd, z_0 and z_1 are even, and both $X_0 = x_0/M, X_1 = x_1/M$ are odd integers. Adding twice the second equation to the first in (1.1) and dividing by M gives

$$X_i^2 - y_i^2 = 2bZ_i^2 \quad (i=0,1).$$

It follows that there exist positive integers $A_0, B_0, A_1, B_1, u_0, u_1, v_0, v_1$ for which $2b = A_0B_0 = A_1B_1$, $Z_0 = 2u_0v_0, Z_1 = 2u_1v_1$, and

$$X_i - y_i = 2A_i u_i^2, \quad X_i + y_i = 2B_i v_i^2 \quad (i=0,1).$$

Solving for y_i, substituting y_i and z_i in the second equation in (1.1), and then simplifying gives

$$(A_i u_i^2 - (1+M^2)B_i v_i^2)^2 - (M^2+2)(2MB_i v_i^2)^2 = 1 \quad (i=0,1),$$

and by symmetry

$$(B_i v_i^2 - (1+M^2)A_i u_i^2)^2 - (M^2+2)(2MA_i u_i^2)^2 = 1 \quad (i=0,1).$$

The rest of the proof follows exactly as in the case $c = 1$ with y_0 odd.

Now we consider the case $c = 4$. Let k_0 and k_1 be indices for which $y_0 = W_{k_0}$ and $y_1 = W_{k_1}$. By Lemma 2.3, k_0 and k_1 have the same parity.

Assume first that they are both odd. In this case M divides x_0 and x_1. Multiplying the second equation in (1.1) by 4, subtracting it from the first equation, and dividing the result by M gives

$$y_i^2 - X_i = 4bZ_i \quad (i = 0, 1),$$

where as before, $X_0 = x_0/M$, $X_1 = x_1/M$ and $Z_0 = z_0/M$, $Z_1 = z_1/M$. Therefore,

$$y_i \pm X_i = 2A_i u_i^2, \quad y_i \mp X_i = 2B_i v_i^2 \quad (i = 0, 1),$$

where for $i = 0, 1$, $b = A_i B_i$, $z_i = M u_i v_i$. Solving for each y_i, substituting y_i and z_i into the second equation in (1.1), and simplifying gives

$$(2A_i u_i^2 + (2 - M^2) B_i v_i^2)^2 - (M^2 - 4)(M B_i v_i^2)^2 = 4 \quad (i = 0, 1),$$

and by symmetry,

$$(2B_i v_i^2 + (2 - M^2) A_i u_i^2)^2 - (M^2 - 4)(M A_i u_i^2)^2 = 4 \quad (i = 0, 1).$$

Therefore, there are even indices i_0, i_1, j_0, j_1 for which

$$W_{i_0} = M B_0 v_0^2, \quad W_{j_0} = M A_0 u_0^2,$$
$$W_{i_1} = M B_1 v_1^2, \quad W_{j_1} = M A_1 u_1^2.$$

Suppose that one of W_{i_0}, W_{j_0}, say W_{i_0}, does not have a primitive prime factor. By Lemma 2.4, it follows that $M = 3$ and either $i_0 = 1$ or $i_0 = 6$. Since i_0 is even, we have $W_{i_0} = 144$, from which it follows that $B_0 v_0^2 = 48$. Since B_0 is squarefree, $B_0 = 3$ and $v_0 = 4$. Therefore, from the definition of the values B_0 and v_0, we deduce that $3y_0 \pm x_0 = 288$. If $3y_0 + x_0 = 288$, then it is readily verified that $y_0 = 55$ and $x_0 = 123$. In this case, $3y_0 - x_0 = 42 = 2MA_0 u_0^2$, showing that $A_0 = 7$, and hence $b = 21$. The case $c = 4$, $M = 3$, $b = 21$ was checked using SIMATH, and exactly one positive integer solution exists to (1.1). If $3y_0 - x_0 = 288$, then it is readily verified that $y_0 = 377$ and $x_0 = 843$. In this case, $3y_0 + x_0 = 1974 = 2MA_0 u_0^2$, showing that $A_0 = 329$, and hence $b = 987$. The case $c = 4$, $M = 3$, $b = 987$ was also checked using SIMATH, and in this case there is exactly one solution.

We can therefore assume that W_{i_0} and W_{j_0} each have a primitive prime factor, say p and q respectively. Then by Lemma 2.3, each of p and q divide one of W_{i_1} or W_{j_1}, from which it follows that each of i_0 and j_0 divide one of i_1 or j_1. Suppose that i_0 and j_0 both divide i_1. Then by the argument given in the proof of the case $c = 1$, it follows that $A_1 = 1$, and hence that $W_{j_1} = M u_1^2$. By Lemma 2.5, it follows that $j_1 = 2$ and $u_1 = 1$. This implies that $M y_1 \pm x_1 = 2M$, which upon solving for x_1 and substituting into the first equation in (1.1) gives $y_1 = M^2 - 1 = W_3$. But $y_0 \neq 1 = W_1$, and so $y_1 > y_0 \geq W_3$, which is a contradiction.

We may therefore assume that i_0 divides i_1 and j_0 divides j_1. As argued in the proof of the case $c = 1$, it follows that $A_0 = A_1$ and $B_0 = B_1$, and by Lemma 2.5, this implies that $A_0 = B_0 = 1$, hence $b = 1$, which is not possible.

Assume now that k_0 and k_1 are both even. As in the previous case we obtain

$$M^2y_i^2 - x_2^2 = 4bz_i^2 \quad (i = 0, 1).$$

Since k_0 and k_1 are even, it follows that M does not divide x_i, and so $\gcd(My_i - x_i, My_i + x_i) = 2$. Therefore, there are integers $A_0, B_0, A_1, B_1, u_0, u_1, v_0, v_1$, with $z_i = u_iv_i$ and $b = A_iB_i$, for which

$$My_i \pm x_i = 2A_iu_i^2, \quad My_i \mp x_i = 2B_iv_i^2 \quad (i = 0, 1).$$

Notice that M does not divide either side of these two equations. Solving for y_i, substituting y_i and z_i into the second equation in (1.1), and then simplifying gives

$$((2A_i + (2 - M^2)B_iv_i^2)/M)^2 - (M^2 - 4)B_i^2v_i^4 = 4 \quad (i = 0, 1).$$

By symmetry, this equation can be rewritten as

$$((2B_i + (2 - M^2)A_iu_i^2)/M)^2 - (M^2 - 4)A_i^2u_i^4 = 4 \quad (i = 0, 1).$$

Since M does not divide $B_iv_i^2$ and $A_iu_i^2$, there are odd indices i_0, j_0, i_1, j_1 for which

$$W_{i_0} = B_0v_0^2, \quad W_{j_0} = A_0u_0^2, \quad W_{i_1} = B_1v_1^2, \quad W_{j_1} = A_1u_1^2.$$

Assume that, say W_{i_0}, has no primitive prime factor. By Lemma 2.4, the only possibility is $i_0 = 1$. It follows that $B_0 = v_0 = 1$, and furthermore that $My_0 - x_0 = 2$. Solving this for x_0 and substituting it into (1.1) gives that $x_0 = M^2 - 2 = V_2$ and $y_0 = M = W_2$. Substituting this into $My_0 + x_0 = 2A_0u_0^2$ shows that $A_0u_0^2 = M^2 - 1$, which means precisely that $j_0 = 3$. Since $A_0 > 1$, there is a primitive prime factor, say p, of W_3 which divides A_0. Since p divides one of A_1 or B_1, and $\gcd(W_{i_1}, W_{j_1}) = 1$, it follows that 3 divides only one of i_1 or j_1, say j_1. Therefore, $\gcd(A_0, W_{i_1}) = 1$, and consequently, $A_0 = A_1$. Therefore, $i_1 = 1$, $B_0 = B_1 = v_1 = 1$, and it is deduced as above that $j_1 = 3$, leading to $y_1 = y_0$, a contradiction.

We may therefore assume that both W_{i_0} and W_{j_0} have primitive prime factors. As above it follows that both i_0 and j_0 divide one of i_1 and j_1. Assume first that they both divide i_1. As argued before, it follows that $A_1 = 1$, forcing $u_1 = 1$ and $j_1 = 1$. As in the previous paragraph, this implies that $y_1 = M$. But since $y_1 > y_0 \geq W + 2 = M$, we obtain a contradiction.

We now deal with the case $c = -4$. In this case, x_i divides M, and so we obtain

$$X_i^2 - y_i^2 = 4bZ_i^2 \quad (i = 0, 1),$$

where as before $X_i = x_i/M, Z_i = z_i/M$. Therefore, there are integers, as before, such that

$$X_i \pm y_i = 2A_iu_i^2, \quad X_i \mp y_i = 2B_iv_i^2 \quad (i = 0, 1).$$

Solving for y_i, substituting in the second equation in (1.1), and simplifying yields

$$(2A_iu_i^2 - (2 + M^2)B_iv_i^2)^2 - (M^2 + 4)(MB_iv_i^2)^2 = 4 \quad (i = 0, 1),$$

and by symmetry,

$$(2B_iv_i^2 - (2 + M^2)A_iu_i^2)^2 - (M^2 + 4)(MA_iu_i^2)^2 = 4 \quad (i = 0, 1).$$

Therefore, there are even indices i_0, i_1, j_0, j_1 for which

$$W_{i_0} = MB_0v_0^2, \quad W_{j_0} = MA_0u_0^2,$$
$$W_{i_1} = MB_1v_1^2, \quad W_{j_1} = MA_1u_1^2.$$

We will assume for the moment that $M > 1$, as this case will be proved at the end. By Lemma 2.4, W_{i_0} and W_{j_0} each have a primitive prime factor, say p and q respectively. Then by Lemma 2.3, each of p and q divide one of W_{i_1} or W_{j_1}, from which it follows that each of i_0 and j_0 divide one of i_1 or j_1. Suppose that i_0 and j_0 both divide i_1. Then by the argument given in the proof of the case $c = 1$, it follows that $A_1 = 1$, and hence that $W_{j_1} = Mu_1^2$. By Lemma 2.5, it follows that $j_1 = 2$ and $u_1 = 1$. This implies that $My_1 \pm x_1 = 2M$, which upon solving for x_1 and substituting into the first equation in (1.1) gives $y_1 = M^2 + 1 = W_3$. But $y_0 \neq 1 = W_1$, and so $y_1 > y_0 \geq W_3$, which is a contradiction.

Thus, we deduce that, say, i_0 divides i_1, and j_0 divides j_1. It follows that $\gcd(A_0, B_1) = 1$ and $\gcd(B_0, A_1) = 1$. Therefore, A_0 divides A_1, and B_0 divides B_1, from which it follows that $A_0 = A_1$ and $B_0 = B_1$. By Lemma 2.5, it follows that $i_0 = i_1$ and $j_0 = j_1$, and hence that $z_0 = z_1$.

In the case that $M = 1$, the above argument goes through except if, say, W_{i_0} does not have a primitive prime factor. By Lemma 2.4, this implies that i_0 is one of $2, 6, 12$, in which case $B_0v_0^2$ is one of $1, 8, 144$. By recalling that $2B_0v_0^2 = x_0 \pm y_0$, where in this case, $x_0^2 - 5y_0^2 = -4$, we see that there are six possible pairs of (x_0, y_0) to deal with; namely, those pairs of integers (x_0, y_0) which satisfy $x_0^2 - 5y_0^2 = -4$, and for which $x_0 \pm y_0 \in \{2, 16, 288\}$. In particular,

$$(x_0, y_0) \in \{(1, 1), (3, 1), (11, 5), (29, 13), (199, 89), (521, 233)\}.$$

If $y_0 = 1$, then $b = 0$, which is not possible. If $x_0 + y_0 = 16$, then $(x_0, y_0) = (11, 5)$, in which case $B_0 = 2$, while $x_0 - y_0 = 6$, forcing $A_0 = 3$, and hence $b = 6$. As there is exactly one solution to (1.1) with $c = -4$, $M = 1$, $b = 6$ (checked with SIMATH), this case is settled. In a similar manner it is shown that the other possible values for (x_0, y_0) lead to $b \in \{42, 55, 377\}$, and in each case, (1.1) with $c = -4$ and $M = 1$ has precisely one solution. This completes the proof of the theorem.

Acknowledgements. The author gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada.

References

[1] M. A. Bennett, *On the number of solutions of simultaneous Pell equations*, J. Reine Angew. Math. 498 (1998), 173–199.

[2] M. A. Bennett, M. Cipu, M. Mignotte and R. Okazaki, *On the number of solutions of simultaneous Pell equations II*, Acta Arith. 122 (2006), 407–417.

[3] Y. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. 539 (2001), 75–122.

[4] M. Cipu and M. Mignotte, *On the number of solutions to simultaneous hyperbolic Diophantine equations*, J. Number Theory, to appear.

[5] J. H. E. Cohn, *Eight Diophantine equations*, Proc. London Math. Soc. (3) 16 (1966), 153–166.

[6] —, *Five Diophantine equations*, Math. Scand. 21 (1967), 61–70.

[7] S.-I. Katayama and C. Levesque, *On simultaneous diophantine equations*, Acta Arith. 108 (2003), 369–377.

[8] W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer und rein-biquadratischer Zahlkörper mit Anwendung auf die Lösung einer Klasse unbestimmter Gleichungen vierten Grades*, Oslo Vid.-Akad. Skrifter 1936, no. 12, 1–73.

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

[10] P. Ribenboim, *Square classes of Fibonacci and Lucas numbers*, Portugal. Math. 46 (1989), 159–175.

[11] A. Togbe, P. M. Voutier and P. G. Walsh, *Solving a family of Thue equations with an application to the equation* $x^2 - Dy^4 = 1$, Acta Arith. 120 (2005), 39–58.

[12] P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. 64 (1995), 869–888.

[13] P. G. Walsh, *A note on a theorem of Ljunggren and the Diophantine equations* $x^2 - kxy^2 + y^4 = 1, 4$, Arch. Math. (Basel) 73 (1999), 119–125.

[14] P. Z. Yuan, *On the number of solutions of* $x^2 - 4m(m+1)y^2 = y^2 - bz^2 = 1$, Proc. Amer. Math. Soc. 132 (2004), 1561–1566.

Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, Canada K1N 6N5
E-mail: gwalsh@mathstat.uottawa.ca

Received on 12.2.2006
and in revised form on 26.10.2006 (5140)