ACTA ARITHMETICA
LXXXII.1 (1997)

On integer solutions to $x^2 - dy^2 = 1$, $z^2 - 2dy^2 = 1$

by

P. G. Walsh (Ottawa, Ont.)

1. Introduction. Let d denote a positive integer. In [7] Ono proves that if the number of representations of d by the form $2a^2 + b^2 + 8c^2$ equals twice the number of representations of d by the form $2a^2 + b^2 + 32c^2$, then the system of simultaneous Pell equations

$$x^2 - dy^2 = 1, \qquad z^2 - 2dy^2 = 1 \tag{1}$$

has no solutions in positive integers x, y, z. This is achieved by showing that when the stated condition holds, the associated elliptic curve $Y^2 = X^3 + 3dX^2 + 2d^2X$ has rank equal to zero, whereas a positive integer solution to (1) would give rise to a point of infinite order on this curve. Heuristics show that this condition only applies for a set of integers which has asymptotic density less than $1/2$. This is in contrast to the fact, which we prove under the hypothesis of the abc conjecture, that the set of squarefree integers d for which (1) has a nontrivial solution grows exponentially. Furthermore, there does not seem to be any obviously fast method of checking this condition, at least from the point of view of computational complexity.

The purpose of this paper is to prove several results concerning the solvability of (1) in positive integers x, y, z. We will refer to such solutions as nontrivial. In our first result we describe the set of squarefree integers d for which (1) has a nontrivial solution. Moreover, using a recent result of Cohn on the Diophantine equation $X^4 - dY^2 = 1$, we show that at most one such solution can exist for a given d, and describe that solution explicitly. We remark that Bennett [1] has recently shown that systems of simultaneous Pell equations of the form

$$x^2 - my^2 = 1, \qquad z^2 - ny^2 = 1 \qquad (0 \neq m \neq n \neq 0)$$

have at most 3 nontrivial solutions, and suggested that such systems have

---

1991 *Mathematics Subject Classification*: Primary 11D09.
Supported by an N.S.E.R.C. Postdoctoral Fellowship.

only one nontrivial solution, provided that they are not of a very specific form which is described in [1]. Thus for the system above (with $m = d$ and $n = 2d$), we have a solution of Bennett's problem.

We then prove that if d is squarefree and is a product of less than 5 primes, then a nontrivial solution to (1) exists only for $d = 6,\ 210,\ 1785$ and 60639. We also show that if a nontrivial solution exists for d squarefree, then d is divisible by a prime of the form $4n + 3$. These two results lead to many cases not covered by the result of [7], and moreover, in many of these cases the associated elliptic curve described above has nonzero rank, which means that the method of [7] cannot be used to deal with these cases. As a consequence of the latter result, we show that no nontrivial solution to (1) exists if either of the fundamental units in $\mathbb{Q}(\sqrt{d})$, $\mathbb{Q}(\sqrt{2d})$ have norm equal to -1. Another consequence is that if x, y, z is a nontrivial solution to (1), then $x + y\sqrt{d}$ is the fundamental unit in $\mathbb{Q}(\sqrt{d})$. In the last part of this paper we show that the sequence of squarefree integers $\{d_1, d_2, \ldots\}$ for which (1) has a nontrivial solution grows exponentially if one assumes the abc conjecture. This provides a (heuristic) polynomial-time algorithm for deciding if (1) has a nontrivial solution when d is squarefree.

2. Finding the solutions. In this section we prove a rather simple result which determines the integers d for which (1) has nontrivial solutions. It is clear that we can restrict our attention to finding those squarefree integers d for which (1) has a nontrivial solution. We begin by stating the recent result in [4].

THEOREM A (Cohn, 1996). *Let the fundamental solution of the equation $v^2 - Du^2 = 1$ be $a + b\sqrt{D}$. Then the only possible solutions of the equation $x^4 - Dy^2 = 1$ are given by $x^2 = a$ and $x^2 = 2a^2 - 1$; both solutions occur in only one case, $D = 1785$.*

For a positive integer n we define the *square class* of n, denoted by $\langle n \rangle$, to be the integer m, where m is squarefree and $n = mx^2$ for some integer x.

THEOREM 1. *For $k \geq 0$, let T_k and U_k be integers with $T_k + U_k\sqrt{2} = (1 + \sqrt{2})^k$, and define d_k to be $\langle (T_{2k+1}^2 - 1)/2 \rangle$. Then $\{d_k\}_{k \geq 1}$ is the set of squarefree integers d for which (1) has a nontrivial solution. Moreover, if (1) does have a nontrivial solution, then it is unique and given by*

$$z = T_{2k+1}, \qquad x = U_{2k+1}, \qquad y = ((T_{2k+1}^2 - 1)/(2d_k))^{1/2}.$$

Proof. Assume that d is a squarefree integer, and that x, y, z is a nontrivial solution to (1). We see that $z^2 - 1 = 2(x^2 - 1)$, and so x, z satisfy the Pell equation

$$z^2 - 2x^2 = -1. \tag{2}$$

All solutions in positive integers to (2) are $(z, x) = (T_{2k+1}, U_{2k+1})$, where T_k and U_k are defined above. It follows that $T_{2k+1}^2 - 1 = 2dy^2$, and therefore $d = d_k$. Conversely, if $d = d_k$, then the preceding equations define a solution of (1). To prove the uniqueness of this solution, first notice that the integers x, y, z satisfy $z^4 - d(2xy)^2 = 1$. By Theorem A, there is only one solution of this equation for a given value of d, except for $d = 1785$. The fundamental solution of $X^2 - 1785Y^2 = 1$ is $13^2 + 4\sqrt{1785}$, and its square is $239^2 + 1352\sqrt{1785}$. The proof is completed by noticing that only the second of these leads to a solution $(x, y, z, d) = (169, 4, 239, 1785)$ of (1).

To illustrate the above result, the first few values in the sequence $\{d_k\}$ are given below:

$$\begin{aligned} d_1 &= 6,\\ d_2 &= 210,\\ d_3 &= 1785,\\ d_4 &= 60639,\\ d_5 &= 915530,\\ d_6 &= 184030,\\ d_7 &= 14066106,\\ d_8 &= 80753867670,\\ d_9 &= 10973017315470,\\ d_{10} &= 372759573255306,\\ d_{11} &= 351745902037915,\\ d_{12} &= 11949006236698685. \end{aligned}$$

The above list indicates that the sequence $\{d_k\}_{k\geq 1}$ may grow exponentially. For the sake of interest, we will show in the final section that this exponential growth can be proved under the hypothesis of the abc conjecture.

3. The number of distinct prime factors of d. The purpose of this section is to prove that, with only four exceptions, which we give explicitly, (1) has no nontrivial solutions if d has less than 5 distinct prime factors. We retain all notation from the previous section.

THEOREM 2. *For $k \geq 5$, d_k has at least 5 distinct prime factors.*

Proof. From the definition of T_k and U_k, we find that for all $k \geq 0$,

$$2T_k = \tau^k + (-1/\tau)^k, \qquad 2U_k\sqrt{2} = \tau^k + (-1/\tau)^k, \tag{3}$$

where $\tau = 1 + \sqrt{2}$. From these equations we deduce that for all $k \geq 0$,

$$T_{2k+1}^2 - 1 = 8T_kU_kT_{k+1}U_{k+1}.$$

By definition, d_k is the square class of $T_kU_kT_{k+1}U_{k+1}$. It is evident that no two of these four terms have a common divisor. Therefore, we can write d_k

as

$$d_k = \langle T_k\rangle\langle U_k\rangle\langle T_{k+1}\rangle\langle U_{k+1}\rangle. \tag{5}$$

Consider the case where k is even. Then $U_k = 2T_{k/2}U_{k/2}$, and it follows that

$$d_k = 2\langle T_k\rangle\langle T_{k/2}\rangle\langle U_{k/2}\rangle\langle T_{k+1}\rangle\langle U_{k+1}\rangle,$$

or

$$d_k = (1/2)\langle T_k\rangle\langle T_{k/2}\rangle\langle U_{k/2}\rangle\langle T_{k+1}\rangle\langle U_{k+1}\rangle,$$

depending on whether the power of 2 properly dividing $U_{k/2}$ is even or odd respectively. Our goal is to show that except for the cases stated above, each of the square classes are nontrivial and not equal to 2. By the result on p. 98 of [10], $\langle T_n\rangle = 1$ only for $n = 1$. By the main result of [5], $\langle U_n\rangle = 1$ only for $n = 1$ and $n = 7$. By Theorem 1 of [8], $\langle U_n\rangle = 2$ only for $n = 2$. From these results we deduce that the only possible values of k which may not lead to a product of at least 5 primes are $k = 2, 4, 6, 14$. It is easily verified that d_6 and d_{14} each have at least 5 distinct prime factors, which completes the proof in the case where k is even.

If k is odd, we find that

$$d_k = 2\langle T_k\rangle\langle U_k\rangle\langle T_{k+1}\rangle\langle T_{(k+1)/2}\rangle\langle U_{(k+1)/2}\rangle,$$

or

$$d_k = (1/2)\langle T_k\rangle\langle U_k\rangle\langle T_{k+1}\rangle\langle T_{(k+1)/2}\rangle\langle U_{(k+1)/2}\rangle,$$

depending on whether the power of 2 properly dividing $U_{(k+1)/2}$ is even or odd. We find in this case that the only possible values of k which may not lead to a product of at least 5 distinct prime factors are $k = 1, 3, 13$. It is easily verified that d_{13} has at least 5 distinct prime factors, which completes the proof of the theorem.

This result shows for example that (1) has no nontrivial solutions for $d = 5$. This is of interest since the associated elliptic curve $Y^2 = X^3 + 15X^2 + 50X$ has nonzero rank, and so the method of [7] is not applicable. It is fairly simple task to construct many more examples of this type.

4. The units in $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{2d})$. The purpose of this section is to prove another sufficient condition for (1) to have no nontrivial solutions. We retain all of the notation from the previous sections.

THEOREM 3. *For $k \geq 1$, d_k is divisible by a prime of the form $4n + 3$.*

Proof. It is easy to prove by induction that $T_k \equiv 3 \pmod 4$ if $k \equiv 2, 3 \pmod 4$, and $T_k \equiv 1 \pmod 4$ if $k \equiv 0, 1 \pmod 4$. Therefore, from (5) the result is immediate for $k \equiv 1, 2, 3 \pmod 4$. We must deal with $k \equiv 0 \pmod 4$. Let $k = 2^a l$, where $a \geq 2$, and l is odd. It is easily proved by

induction that $U_k = 2^a U_l T_l T_{2l} \dots T_{2^{a-1}l}$. In fact, it is actually the case that $\langle U_k \rangle = 2^b \langle U_l \rangle \langle T_l \rangle \langle T_{2l} \rangle \dots \langle T_{2^{a-1}l} \rangle$, where b is either 0 or 1. This follows from the fact that for all positive integers t and l, U_l divides U_{tl}, T_l divides U_{2tl}, and $\gcd(T_l, U_l) = 1$. Since $\langle T_{2l} \rangle \equiv 3 \pmod 4$, it follows that $\langle U_k \rangle$ is divisible by a prime of the form indicated in the statement of the result.

As in Theorem 2, this result provides a method to find many values of d for which (1) has no nontrivial solution, and for which the associated elliptic curve has nonzero rank, thereby prohibiting the method of [7] to apply. For example, this result gives a second proof that (1) has no nontrivial solutions for $d = 5$.

A special case of Theorem 3 is the following result.

COROLLARY 1. *If either of the fundamental units* ε_d *and* ε_{2d} *of* $\mathbb{Q}(\sqrt{d})$ *and* $\mathbb{Q}(\sqrt{2d})$ *respectively have norm* -1, *then* (1) *has no nontrivial solutions.*

Proof. Let $m = d$ or $2d$ so that the norm of the fundamental unit in $\mathbb{Q}(\sqrt{m})$ is -1. Then there are integers X, Y such that $X^2 - mY^2 = -1$, and so mY^2 is a sum of two squares which are coprime. It follows that m, and hence d, is not divisible by any prime of the form $4n + 3$, and so by Theorem 3, (1) has no nontrivial solutions.

COROLLARY 2. *Let* (x, y, z) *be a nontrivial solution to* (1). *Then* $x + y\sqrt{d}$ *is the fundamental unit of* $\mathbb{Q}(\sqrt{d})$.

Proof. We have $z^2 + (2xy)\sqrt{d} = (x + y\sqrt{d})^2$, so by Theorem A, $x + y\sqrt{d}$ is the fundamental solution to the Pell equation $X^2 - dY^2 = 1$. By Corollary 1, the Pell equation $X^2 - dY^2 = -1$ is not solvable, so that $x + y\sqrt{d}$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$ or its third power (see p. 64 of [9]). We must show that this latter possibility cannot occur. If $x + y\sqrt{d}$ is the third power of the fundamental unit ε_d, then $\varepsilon_d = (a + b\sqrt{d})/2$, where $a^2 - b^2 d = 4$. Let $(a_k + b_k\sqrt{d})/2 = ((a + b\sqrt{d})/2)^k$; then $a_6 = 2z^2$. By Theorem 2 of [3], this forces $d = 29$. By Theorem 2 above, (1) has no solutions for $d = 29$.

The following result diverges somewhat from the main topic at hand, but nevertheless follows from what has been done so far, and seems to be of interest for its own sake. It would be interesting to know whether a similar result is true for discriminants other than 2.

COROLLARY 3. *For* $k \geq 1$, *let* $T_k + U_k\sqrt{2} = (1 + \sqrt{2})^k$ *be as above, and for* $k > 1$ *let* $U_k^2 + (-1)^k = m_k V_k^2$ *with* m_k *squarefree. Then, except for* $k = 2, 6$, $U_k + V_k\sqrt{m_k}$ *is the fundamental unit in* $\mathbb{Q}(\sqrt{m_k})$. *For* $k = 2, 6$, $U_k + V_k\sqrt{m_k}$ *is the third power of the fundamental unit in* $\mathbb{Q}(\sqrt{m_k})$.

Proof. For k odd we actually have $m_k = d_{(k-1)/2}$, and the result follows from Corollary 2. We must deal with the case where k is even. In

this case, $T_k^2 - 2U_k^2 = 1$, and it follows from this and $U_k^2 + 1 = m_k V_k^2$ that $T_k^2 + 1 = 2m_k V_k^2$. Therefore,

$$T_k^4 - (2U_k V_k)^2 m_k = 1.$$

By Theorem A, $T_k^2 + 2U_k V_k\sqrt{m_k}$ is the fundamental solution of the Pell equation $X^2 - m_k Y^2 = 1$, and so $X = U_k,\ Y = V_k$ is the solution of the Pell equation $X^2 - m_k Y^2 = -1$ with smallest possible positive values X and Y. It follows that $U_k + V_k\sqrt{m_k}$ is the fundamental unit of $\mathbb{Q}(\sqrt{m_k})$ or its third power. By the results of [2] and [3], the latter case can only occur if $m_k = 5$ or 29, which are precisely the cases $k = 2$ and $k = 6$.

5. The growth of $\{d_k\}$. As was shown in Section 2, the set $\{d_k\}$ appears to be growing exponentially, at least for the first few values. We cannot prove this result unconditionally, but we can prove this under the hypothesis of the abc conjecture. Proving exponential growth unconditionally seems to be intractable with current methods. In fact, Stewart [11] has proved a result using the theory of linear forms in the logarithms of algebraic numbers which implies that the sequence $\{d_k\}$ grows at least linearly with k, which is certainly very far from the truth.

Conjecture 1 (Oesterlé–Masser). *Given $\varepsilon > 0$ there exists a positive constant $C = C(\varepsilon)$ depending only on ε such that for all triples (a, b, c) of positive integers with $a = b + c$ and* $\gcd(a, b, c) = 1$,

$$a < C\Big(\prod_{p|abc} p\Big)^{1+\varepsilon}.$$

Using this conjecture we can prove the following result. Once again we use the notation given in Theorem 1 and its proof.

Theorem 4 (assuming the abc conjecture). *If $\tau = 1 + \sqrt{2}$, then for any δ with $0 < \delta < 2$ there exists a positive constant $C = C(\delta)$ depending only on δ such that for all $k \geq 1$,*

$$C(\delta)\tau^{(4-\delta)k} < d_k < \tau^{4k}.$$

Proof. We first prove the second inequality. We know by definition that $T_{2k+1}^2 = 2d_k y^2 + 1$, and so we have $d_k < (1/2)T_{2k+1}^2$. Also, $T_{2k}^2 = 2U_{2k}^2 + 1$, and so $\sqrt{2}U_{2k} < T_{2k}$. Let c be a positive number satisfying $1 + \tau^{-4} < c < 2\sqrt{2}/\tau$. Then

$$\begin{aligned} T_{2k+1} = T_{2k} + 2U_{2k} &< (1+\sqrt{2})T_{2k} = \frac{1+\sqrt{2}}{2}((3+2\sqrt{2})^k + (3-2\sqrt{2})^k) \\ &< \frac{c(1+\sqrt{2})}{2}(3+2\sqrt{2})^k = \frac{c}{2}\tau^{2k+1}, \end{aligned}$$

and so by our choice of c,

$$d_k < (1/2)T_{2k+1}^2 < \frac{c^2}{8}\tau^{4k+2} < \tau^{4k}.$$

For the first inequality, recall from the proof of Theorem 1 that T_{2k+1} satisfies $T_{2k+1}^4 = d_k(2xy)^2 + 1$, so by the abc conjecture we find that for all $\varepsilon > 0$ there exists a positive constant $C_1(\varepsilon)$ such that

$$T_{2k+1}^4 < C_1(\varepsilon)(d_k T_{2k+1} xy)^{1+\varepsilon}.$$

Fix δ and put $\varepsilon = \delta/(8-\delta)$, with $0 < \varepsilon < 1/3$, so that $0 < \delta < 2$. Since $T_{2k+1}^2 + 1 = 2x^2$, we know that $T_{2k+1} \geq x$, and so it follows that

$$T_{2k+1}^{2-2\varepsilon} < C_1(\varepsilon)(d_k y)^{1+\varepsilon}.$$

Since $T_{2k+1}^2 = 2d_k y^2 + 1$, we know that $T_{2k+1} > \sqrt{2}d_k^{1/2} y$, and so because $\delta = 8\varepsilon/(\varepsilon+1)$, it follows that there is a positive constant $C_2(\delta)$ such that for all $k \geq 1$ the inequality

$$C_2(\delta) T_{2k+1}^{2-\delta} < d_k$$

holds. Since

$$\begin{aligned} T_{2k+1} &= T_{2k} + 2U_{2k} > (2+\sqrt{2})U_{2k} = \frac{(2+\sqrt{2})}{2\sqrt{2}}((3+2\sqrt{2})^k - (3-2\sqrt{2})^k) \\ &= (1/2)(\tau^{2k+1} - \tau^{-2k+1}) > (1/4)\tau^{2k+1}, \end{aligned}$$

the result follows by putting $C(\delta) = (1/4)C_2(\delta)$.

Note that this provides an efficient (although heuristic) method for determining for a squarefree positive integer d whether a nontrivial solution to (1) exists. One simply computes $d_1, \ldots, d_k$, where d_k is a few decimal digits larger than d, and checks if d is in the computed list. It is easy to see that the computation of $d_1, \ldots, d_k$ can be performed in time which is polynomial in the number of bits of d.

Acknowledgements. The author would like to thank Mike Bennett, Professor Cohn, Ken Ono, and Paul Voutier for their preprints and the useful discussions we had on this subject matter.

References

[1] M. A. Bennett, *On the number of solutions to simultaneous Pell equations*, J. Reine Angew. Math., to appear.

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

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

[4] —, *The Diophantine equation* $x^4 - Dy^2 = 1$, *II*, Acta Arith. 78 (1997), 401–403.

[5] W. Ljunggren, *Zur Theorie der Gleichung* $x^2+1=Dy^4$, Avh. Norske Vid. Akad. Oslo (1942), 1–27.
[6] D. W. Masser, *Open Problems*, in: Proc. Sympos. Analytic Number Theory, W. W. L. Chen (ed.), London Imperial College, 1985.
[7] K. Ono, *Euler's concordant forms*, Acta Arith. 78 (1996), 101–123.
[8] N. Robbins, *On Pell numbers of the form* px^2, *where* p *is a prime*, Fibonacci Quart. (4) 22 (1984), 340–348.
[9] P. Samuel, *Algebraic Theory of Numbers*, Houghton Mifflin, Boston, 1970.
[10] W. Sierpiński, *Elementary Theory of Numbers*, Państwowe Wydawnictwo Naukowe, Warszawa, 1964.
[11] C. L. Stewart, *On divisors of Fermat*, *Fibonacci*, *Lucas and Lehmer numbers III*, J. London Math. Soc. (2) 28 (1983), 211–217.

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

Received on 18.10.1996
and in revised form on 25.2.1997 (3063)