PRIMITIVE DIVISORS OF LUCAS AND LEHMER SEQUENCES

PAUL M. VOUTIER

ABSTRACT. Stewart reduced the problem of determining all Lucas and Lehmer sequences whose nth element does not have a primitive divisor to solving certain Thue equations. Using the method of Tzanakis and de Weger for solving Thue equations, we determine such sequences for $n \leq 30$. Further computations lead us to conjecture that, for $n > 30$, the nth element of such sequences always has a primitive divisor.

1. INTRODUCTION

Let α and β be algebraic numbers such that $\alpha + \beta$ and $\alpha\beta$ are relatively prime nonzero rational integers and α/β is not a root of unity. The sequence $(u_n)_{n=0}^{\infty}$ defined by $u_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ for $n \geq 0$ is called a *Lucas sequence.*

If, instead of supposing that $\alpha + \beta \in \mathbb{Z}$, we only suppose that $(\alpha + \beta)^2$ is a nonzero rational integer, still relatively prime to $\alpha\beta$, then we define the *Lehmer sequence* $(u_n)_{n=0}^{\infty}$ associated with α and β by

$$u_n = \begin{cases} \dfrac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd}, \\ \dfrac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even}. \end{cases}$$

We say that a prime number p is a *primitive divisor* of a Lucas number u_n if p divides u_n but does not divide $(\alpha - \beta)^2 u_2 \cdots u_{n-1}$. Similarly, p is a primitive divisor of a Lehmer number u_n if p divides u_n but not $(\alpha^2 - \beta^2)^2 u_3 \cdots u_{n-1}$.

There is another sequence, $(v_n)_{n=0}^{\infty}$, associated with every Lucas and Lehmer sequence. However, $v_n = u_{2n}/u_n$, so it has a primitive divisor if and only if u_{2n} does. Therefore, in what follows we need only consider the numbers u_n.

Drawing upon the ideas of Schnizel [16] and refined techniques for determining lower bounds for linear forms in logarithms, Stewart [17, p.80] showed, as a consequence of his Theorem 1, that if $n > C$, then u_n has a primitive divisor, where $C = e^{452}2^{67}$ for Lucas sequences and $C = e^{452}4^{67}$ for Lehmer sequences.

PAUL M. VOUTIER

Moreover, Stewart [17, Theorem 2] also proved that for $n > 6$, $n \neq 8$, 10, 12 there are at most finitely many Lucas and Lehmer sequences whose nth element is without a primitive divisor. And, as Stewart states (see [17, p.80]), for Lucas sequences the conditions on n may be replaced by $n > 4$, $n \neq 6$. He demonstrated this by reducing the problem of finding all Lucas and Lehmer sequences whose nth element has no primitive divisor to solving finitely many Thue equations.

Here, we will use the method of Tzanakis and de Weger [7, 19] to solve these Thue equations and thus enumerate all Lucas and Lehmer sequences whose nth element has no primitive divisor when $n \leq 30$ satisfies the conditions in the previous paragraph.

Notice that if (u_n) is the sequence generated by α and β and (u'_n) is the sequence generated by $-\alpha$ and $-\beta$, then $u_n = \pm u'_n$. We list only one of these pairs in Table 1 below; thus, for each entry (α, β) which generates a sequence whose nth element is without a primitive divisor, the nth element of the sequence generated by $-\alpha$ and $-\beta$ also lacks a primitive divisor.

TABLE 1

n	α, β			
5	$\dfrac{1 \pm \sqrt{5}}{2}$	$\dfrac{1 \pm \sqrt{-7}}{2}$	$1 \pm \sqrt{-10}$	$\dfrac{1 \pm \sqrt{-11}}{2}$
	$\dfrac{1 \pm \sqrt{-15}}{2}$	$6 \pm \sqrt{-19}$	$6 \pm \sqrt{-341}$	
7	$\dfrac{1 \pm \sqrt{-7}}{2}$	$\dfrac{1 \pm \sqrt{-19}}{2}$		
8	$1 \pm \sqrt{-6}$	$\dfrac{1 \pm \sqrt{-7}}{2}$		
10	$1 \pm \sqrt{-2}$	$\dfrac{5 \pm \sqrt{-3}}{2}$	$\dfrac{5 \pm \sqrt{-47}}{2}$	
12	$\dfrac{1 \pm \sqrt{5}}{2}$	$\dfrac{1 \pm \sqrt{-7}}{2}$	$\dfrac{1 \pm \sqrt{-11}}{2}$	
	$1 \pm \sqrt{-14}$	$\dfrac{1 \pm \sqrt{-15}}{2}$	$\dfrac{1 \pm \sqrt{-19}}{2}$	
13	$\dfrac{1 \pm \sqrt{-7}}{2}$			
18	$\dfrac{1 \pm \sqrt{-7}}{2}$			
30	$\dfrac{1 \pm \sqrt{-7}}{2}$			

TABLE 2

n	α, β		
7	$\dfrac{1 \pm \sqrt{-7}}{2}$	$\dfrac{1 \pm \sqrt{-19}}{2}$	$\dfrac{\sqrt{3} \pm \sqrt{-5}}{2}$
	$\dfrac{\sqrt{5} \pm \sqrt{-7}}{2}$	$\dfrac{\sqrt{13} \pm \sqrt{-3}}{2}$	$\dfrac{\sqrt{14} \pm \sqrt{-22}}{2}$
9	$\dfrac{\sqrt{5} \pm \sqrt{-3}}{2}$	$\dfrac{\sqrt{7} \pm \sqrt{-1}}{2}$	$\dfrac{\sqrt{7} \pm \sqrt{-5}}{2}$
13	$\dfrac{1 \pm \sqrt{-7}}{2}$		
14	$\dfrac{\sqrt{3} \pm \sqrt{-13}}{2}$	$\dfrac{\sqrt{5} \pm \sqrt{-3}}{2}$	$\dfrac{\sqrt{7} \pm \sqrt{-1}}{2}$
	$\dfrac{\sqrt{7} \pm \sqrt{-5}}{2}$	$\dfrac{\sqrt{19} \pm \sqrt{-1}}{2}$	$\dfrac{\sqrt{22} \pm \sqrt{-14}}{2}$
15	$\dfrac{\sqrt{7} \pm \sqrt{-1}}{2}$	$\dfrac{\sqrt{10} \pm \sqrt{-2}}{2}$	
18	$\dfrac{1 \pm \sqrt{-7}}{2}$	$\dfrac{\sqrt{3} \pm \sqrt{-5}}{2}$	$\dfrac{\sqrt{5} \pm \sqrt{-7}}{2}$
24	$\dfrac{\sqrt{3} \pm \sqrt{-5}}{2}$	$\dfrac{\sqrt{5} \pm \sqrt{-3}}{2}$	
26	$\dfrac{\sqrt{7} \pm \sqrt{-1}}{2}$		
30	$\dfrac{1 \pm \sqrt{-7}}{2}$	$\dfrac{\sqrt{2} \pm \sqrt{-10}}{2}$	

Similarly, if α and β generate a Lehmer sequence (u_n) and (u'_n) is the Lehmer sequence generated by $i\alpha$ and $i\beta$, then $u_n = \pm u'_n$. Again, we list only one of the four pairs in Table 2, and so for each entry (α, β) generating a sequence whose nth element is without a primitive divisor, the nth element of the sequences generated by $i^k \alpha$ and $i^k \beta$, for $k = 1, 2, 3$, also lack primitive divisors.

Theorem 1. (i) *For* $4 < n \le 30$, $n \ne 6$, *Table* 1 *gives a complete list, up to the sign of* α *and* β, *of all Lucas sequences whose nth element has no primitive divisor.*

(ii) *For* $6 < n \le 30$, $n \ne 8, 10, 12$, *Table* 2 *gives a complete list, up to multiplication of* α *and* β *by a fourth root of unity, of all Lehmer sequences whose nth element has no primitive divisor.*

Using continued fractions and Lemma 6(i) below, we may quickly search for small solutions of Thue equations. By this method, we have determined that for $31 \le n \le 250$ there are no solutions (x, y) of the appropriate Thue equations, $F_n(X, Y) = m$ with $\max(|x|, |y|) < 10^6$ which give rise to Lucas or Lehmer

sequences whose nth element is without a primitive divisor. Notice that 10^6 is quite a bit larger than the entries X_4 and Y_4 in Tables 5–7 (see §6), which give the maximum of $|x|$ and $|y|$ for all solutions (x, y) of each completely solved Thue equation. Moreover, Birkhoff and Vandiver [1] have shown that there are no Lucas sequences generated by $\alpha, \beta \in \mathbb{Z}$ whose nth element does not have a primitive divisor for $n > 6$ and Carmichael [4] proved the same result for $\alpha, \beta \in \mathbb{R}$ with $n > 12$. In the late 1950s, Ward [21] and Durst [9] extended Carmichael's result to Lehmer sequences. Thus it seems reasonable to make the following conjecture.

Conjecture 1. For $n > 30$, the nth element of a Lucas or Lehmer sequence always has a primitive divisor.

In the next section, the lemmas necessary to establish the connection between enumerating Lucas and Lehmer sequences whose nth element has no primitive divisor and solving Thue equations are given as well as some results from algebraic number theory which are necessary to solve these equations. In §3 we consider the values $n = 5, 8, 10$ and 12 for which there are infinitely many Lehmer sequences without a primitive divisor but only finitely many such Lucas sequences. Then, in §4, we give a description of the algorithm of Tzanakis and de Weger for solving Thue equations. In §5, we describe linear dependence relations over $\mathbb{Z}$ between certain numbers which arise in our applications of this algorithm. Finally, tables giving details of the computations for each value of n are provided.

2. SOME PRELIMINARY LEMMAS

Let $\Phi_n(X, Y)$ be the homogeneous cyclotomic polynomial of order n and $\phi_n(X) = \Phi_n(X, 1)$. These polynomials are linked to Lucas and Lehmer sequences by the formula

$$(1) \qquad \alpha^n - \beta^n = \prod_{d \mid n} \Phi_d(\alpha, \beta).$$

Notation 1. For $n > 1$, we let $P(n)$ denote the largest prime divisor of n.

Lemma 1. *Let $n > 4$ and $n \neq 6, 12$. Then u_n has a primitive divisor if and only if $\Phi_n(\alpha, \beta) \neq \pm 1, \pm P(n/(n, 3))$. Furthermore, u_{12} has a primitive divisor if and only if $\Phi_{12}(\alpha, \beta) \neq \pm 1, \pm 2, \pm 3, \pm 6$.*

Proof. This follows immediately from Lemmas 6 and 7 of Stewart [18], using (1). □

It is by means of this lemma that we obtain Thue equations. Indeed,

$$\Phi_n(\alpha, \beta) = \prod_{\substack{j=1 \\ (j, n)=1}}^{n} (\alpha - \zeta_n^j \beta) = \prod_{\substack{j=1 \\ (j, n)=1}}^{n/2} \left(\alpha^2 + \beta^2 - \left(\zeta_n^j + \zeta_n^{-j} \right) \alpha\beta \right).$$

Let $x = \alpha^2 + \beta^2$ and $y = \alpha\beta$. Then $\Phi_n(\alpha, \beta) = F_n(x, y)$, where $F_n(x, y)$ is a binary form of total degree $\varphi(n)/2$ in x and y and $\varphi(n)$ is the Euler phi function. Moreover, since $\zeta_n^j + \zeta_n^{-j} = 2\cos(2\pi j/n)$ is an algebraic integer, $F_n(x, y)$ has rational integer coefficients. By Lemma 1, we have four Thue equations associated with each $n > 4$, $n \neq 6, 12$ to solve. Recall that we assumed $(\alpha + \beta)^2$ and $\alpha\beta$ are integers, so x and y are integers. We can find the values of α and β associated with a given solution (x, y) of these Thue equations as the roots of the polynomial $X^2 - \sqrt{x + 2y}\, X + y$.

We start with some properties of these binary forms.

Lemma 2. (i) *If t is an odd integer, then $F_{2t}(X, Y) = F_t(X, -Y)$.*

(ii) *Let $n = p_1^{r_1} \cdots p_k^{r_k}$ and $m = p_1^{s_1} \cdots p_k^{s_k}$, where $p_1, \ldots, p_k$ are distinct primes and the r_i's and s_i's are positive integers with $1 \leq s_i \leq r_i$. Then $F_n(X, Y) = F_m(X', Y')$, where $Y' = Y^{n/m}$ and X' can be written as a binary form of degree n/m in X and Y with integer coefficients.*

Proof. These two statements follow easily from the analogous statements which hold for the cyclotomic polynomials:

$$\phi_{2t}(X) = \phi_t(-X) \quad \text{and} \quad \phi_n(X) = \phi_m\left(X^{n/m}\right).$$

The first result is part (iv) of Proposition 5.16 from Chapter 2 of Karpilovsky's book [10], while the second is a slight generalization, whose proof is essentially identical, of part (vi) of this same proposition. $\square$

There are two other results we need in order to implement the algorithm of Tzanakis and de Weger. All but one of the Thue equations we consider here split into linear factors in the field $\mathbb{Q}(\cos(2\pi/n))$. We need a factorization of the ideal $(P(n/(3, n)))$ in these fields as well as a system of fundamental units for the ring of integers of these fields.

Lemma 3. (i) *If $n = p^k$ is an odd prime power satisfying $7 \leq p^k \leq 29$, then*

$$(P(n/(3, n))) = (p) = (2 - 2\cos(2\pi/p^k))^{\varphi(p^k)/2}.$$

(ii) *For $n = 15, 21$ and 24, $(P(n/(3, n))) = (1 + 2\cos(2\pi/n))^{\varphi(n)/2}$.*

(iii) *For $n = 16$ and 20, $(P(n/(3, n))) = (2\cos(2\pi/n))^{\varphi(n)/2}$.*

Proof. These factorizations are determined by using a theorem of Dedekind, see Proposition 2.14 of Washington [22]. $\square$

Note 1. Notice that as a consequence of this lemma, any algebraic integer in $\mathbb{Q}(\cos(2\pi/n))$, where n is as stated, with norm equal to $P(n/(3, n))$ must be an associate of the generator of the ideal given in these factorizations.

Lemma 4. (i) *If $n = p^k$, where p is a prime and $\varphi(n) \leq 66$, then*

$$\left\{ \frac{\sin(a\pi/n)}{\sin(\pi/n)} : 1 < a < n/2, (a, n) = 1 \right\}$$

is a system of fundamental units for $\mathbb{Q}(\cos(2\pi/n))$.

In (ii)–(v), put $r = 2\cos(2\pi/n)$.

(ii) *If $n = 15$, then $\{r, r - 1, r^2 - 3\}$ is a system of fundamental units.*

(iii) *If $n = 20$, then $\{r - 1, r - 2, r^2 - 2\}$ is a system of fundamental units.*

(iv) *If* $n = 21$, *then* $\{r, r - 1, r^2 + r - 1, r^2 - 2, r^2 - 3\}$ *is a system of fundamental units.*

(v) *If* $n = 24$, *then* $\{r, 2r - 1, r^2 - r - 1\}$ *is a system of fundamental units.*

Proof. (i) follows from Theorem 8.2 of Washington [22], which states that the index of the group generated by these units in the full unit group is the class number and Theorem 1 of van der Linden [20], which states that the class number of these fields is 1.

The systems of units given in the cases (ii)–(v) were found by the methods of Pohst and Zassenhaus [14]. □

3. THE CASES $n = 5, 8, 10$ AND 12

For $n = 5, 8, 10, 12$, $F_n(X, Y) = m$ is of total degree two and reducible to a Pell equation. Hence, there will be infinitely many solutions (if any) to the Thue equations which arise in these cases. However, for Lucas sequences not only is $(\alpha + \beta)^2$ an integer but so is $\alpha + \beta$; therefore $x + 2y$ must be a perfect square for any solution (x, y) of $F_n(X, Y) = m$. Letting $Z^2 = X + 2Y$ and substituting this expression for X in $F_n(X, Y) = m$, we get an equation which can be transformed into one of the form $aX^2 - bY^4 = c$, where a, b, c are pairwise relatively prime integers with a and b positive.

We start with a lemma stating two results which will be used below and are likely to be difficult for the reader to find. First, a little notation. For a positive odd square-free number A, let (a, b) be the least positive integer solution of $AX^2 - Y^2 = 2$ and put $\mathbb{K}_1 = \mathbb{Q}(\sqrt{A})$, $\mathbb{K}_2 = \mathbb{Q}(\sqrt{b + a\sqrt{A}})$ and $\mathbb{K}_3 = \mathbb{Q}(\sqrt{-b + a\sqrt{A}})$. We also define $\mathscr{U}_2 = \{\alpha \in \mathbb{K}_2 : \mathscr{N}_{K_2/K_1}(\alpha) = 1\} = \{\pm\epsilon_1^n : n \in \mathbb{Z}\}$ and $\mathscr{U}_3 = \{\alpha \in \mathbb{K}_3 : \mathscr{N}_{K_3/K_1}(\alpha) = 1\} = \{\pm\epsilon_2^n : n \in \mathbb{Z}\}$. For $\alpha \in \mathbb{K}_2$ or $\mathbb{K}_3$, we let α' be its real conjugate.

Lemma 5. (i) *Let* A *be a square-free odd positive integer. For positive integers* x *and* y *satisfying* $Ax^2 - y^4 = 2$, *we put* $\vartheta = 2(Ax^2 + y^4 + 2xy^2\sqrt{A})$. *Then either*

$$\vartheta = \epsilon_1 + \epsilon_1' + 2 \quad or \quad \vartheta = \epsilon_2 + \epsilon_2' + 2.$$

(ii) *Let* c *and* D *be positive square-free integers with* $(c, 2) = (c, 3) = (D, 3) = 1$. *The three equations* $8c^2X^4 \pm 4cX^2 + 1 = DY^2$, $c^2X^4 + 1 = 2DY^2$ *have between them at most one solution in positive integers.*

Proof. These results, both due to Ljunggren, are Satz 2 of [11] and Satz VIII of [12], respectively. □

The author apologizes for the rather ad hoc form of this section, but there seems to be no way around this. There is, presently, no elegant and unified theory for solving these equations. One could use the Thue equation approach, used in the case $n = 12$, $k = -2$; however, this apparently would entail formidable computational difficulties for some of the Thue equations.

3.1. The case $n = 5$. Here we have $F_5(X, Y) = X^2 + XY - Y^2 = \pm1, \pm5$. Letting $X + 2Y = Z^2$, where Z is an integer, we obtain the equation $G_5(Y, Z) = Z^4 - 3YZ^2 + Y^2 = k = \pm1, \pm5$. Solving $G_5(Y, Z) - k = 0$ as a quadratic in Y, we find that $2Y = 3Z^2 \pm \sqrt{5Z^4 + 4k}$, so that

$$5Z^4 + 4k = W^2.$$

It is this last equation we shall use.

In the cases of $k = \pm 1$, Cohn [5, Theorem 7] has shown that the complete solution of $5Z^4 \pm 4 = W^2$ in nonnegative integers is $(W, Z) = \{(1, 1), (2, 0), (3, 1), (322, 12)\}$. From this, we can show that the complete solution of $F_5(X, Y) = \pm 1$, $X + 2Y = Z^2$ is $(X, Y) \in \{(-610, 377), (-5, 3), (-3, 2), (-2, 1), (-1, 1), (1, 0), (2, -1), (34, 55)\}$.

If $k = \pm 5$, we may substitute $W = 5V$ and get the equation $Z^4 + 4 = 5V^2$. Here Cohn [5, Theorem 13] has shown that the complete solution in nonnegative integers is $(V, Z) \in \{(1, 1), (2, 2)\}$. Thus we find that the complete solution of $F_5(X, Y) = 5$, $X + 2Y = Z^2$ is $(X, Y) \in \{(-18, 11), (-7, 4), (2, 1), (3, -1)\}$.

The Lucas sequences which arise from these solutions are given in Table 1. Notice that some of these solutions do not give rise to Lucas sequences since for the corresponding values of α and β, we have $\alpha\beta = 0$ or α/β is a root of unity.

3.2. The case $n = 8$. Here we obtain $2Z^4 + 2k = W^2$, where $k = \pm 1, \pm 2$ and $2Y = 2Z^2 \pm \sqrt{2Z^4 + 2k}$. As $W = 2V$, we get the equation

$$Z^4 + k = 2V^2.$$

For $k = 1$, our equation is the third equation in Lemma 5(ii) with $c = D = 1$. Notice that $(V, Z) = (1, 1)$ is a solution in positive integers and hence, by this lemma, the only such solution. This implies that the complete solution of $F_8(X, Y) = 1$ where $X + 2Y$ is a perfect square is $(X, Y) \in \{(-3, 2), (1, 0)\}$.

If $k = -1$, we can factor $Z^4 - 1$, getting $(Z^2 - 1)(Z^2 + 1) = 2V^2$. Notice that Z must be odd, so that $(Z^2 - 1, Z^2 + 1) = 2$. Therefore, one of $Z^2 \pm 1$ is a square and the other twice a square. For $Z \neq 0$, $Z^2 + 1$ is not a square and hence $Z^2 - 1$ must be a square. So $Z = 0, \pm 1$ and we find that the complete solution of $F_8(X, Y) = -1$, $X + 2Y = Z^2$ is $(X, Y) \in \{(-1, 1)\}$.

If $k = 2$, we see that $Z = 2U$ and obtain the equation $8U^4 = V^2 - 1 = (V + 1)(V - 1)$. Notice that V must be odd and so $(V - 1, V + 1) = 2$. Thus either $V - 1 = 2H^4$ and $V + 1 = 4K^4$, or $V - 1 = 4K^4$ and $V + 1 = 2H^4$, from which we deduce that $H^4 - 2K^4 = \pm 1$. Delone and Faddeev [8, Theorem 3, p.374] have shown that the complete solution in nonnegative integers of these equations is $(H, K) \in \{(1, 1), (1, 0)\}$. So we determine that the complete solution of $F_8(X, Y) = 2$ with $X + 2Y$ a perfect square is $(X, Y) \in \{(-10, 7), (-2, 1), (2, -1), (2, 1)\}$.

If $k = -2$, the relation $Z = 2U$ gives us the equation $V^2 - 8U^4 = -1$, which has no solution, since -1 is not a square mod 8.

Computing the values of α and β which correspond to these solutions, we find that Table 1 is complete for $n = 8$.

3.3. The case $n = 10$. Using the same argument as in the previous section, we find that $10Y = 5Z^2 \pm \sqrt{5Z^4 + 20k}$. If $W^2 = 5Z^4 + 20k$, then $W = 5V$, so we consider the equations

$$5V^2 = Z^4 + 4k$$

where again $k = \pm 1, \pm 5$.

Notice that for $k = \pm 1$, we have the same equations as for $n = 5$ and

$k = \pm 5$. So we find the same values of Z. Here $(X, Y) \in \{(-2, 3), (-1, 1),$ $(1, 0), (2, 1)\}$ is the complete solution of $F_{10}(X, Y) = \pm 1$, $X + 2Y = Z^2$.

For $k = \pm 5$, we have $Z = 5U$, which leads to the equation $V^2 = 125U^4 \pm 4$. By the theory of Pell equations, any solution must be the square root of five times a Fibonacci number. Robbins [15, Theorem 3] has shown that the only squares of the form five times a Fibonacci number are 0 and 25. Thus the complete solution of $F_{10}(X, Y) = \pm 5$, $X + 2Y = Z^2$ is $(X, Y) \in \{(-11, 18), (-2, 1), (2, -1), (11, 7)\}$.

Again, the Lucas sequences which arise from these solutions are given in Table 1.

3.4. The case $n = 12$.

We have $F_{12}(X, Y) = X^2 - 2Y^2 = k = \pm 1, \pm 2, \pm 3, \pm 6$ and $Y = 2Z^2 \pm \sqrt{3Z^4 + k}$, so that

$$3Z^4 + k = W^2.$$

First we note that the equations for $k = -1, 2, 3, -6$ have no solutions by considering them mod 3.

Consider next the case of $k = 1$. Here there are precisely two solutions of $3Z^4 + 1 = W^2$ in positive integers, namely $(W, Z) = (1, 2)$ or $(2, 7)$ (see Ljunggren [13]). Thus the complete solution of $F_{12}(X, Y) = 1$ with $X + 2Y = Z^2$ is $(X, Y) \in \{(-26, 15), (-7, 4), (-2, 1), (1, 0), (2, -1), (2, 1)\}$.

If $k = -2$, we convert the equation into a Thue equation. We factor $W^2 + 2 = 3Z^4$ as $(W - \sqrt{-2})(W + \sqrt{-2}) = 3Z^4$. Thus we can write $W - \sqrt{-2} = AU^4$ and $W + \sqrt{-2} = BV^4$, with $AB = 3L^4$, where A, B, L, U and V are algebraic integers in $\mathbb{Q}(\sqrt{2})$, with A and B algebraic conjugates, $U = S - T\sqrt{-2}$ and $V = S + T\sqrt{-2}$. Using the facts that $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$, the only units in $\mathbb{Q}(\sqrt{-2})$ are ± 1 and $(W - \sqrt{-2}, W + \sqrt{-2})$ divides $(2\sqrt{-2})$, we find that S and T give rise to a solution of $W^2 + 2 = 3Z^4$ if and only if

$$F(S, T) = S^4 - 4S^3T - 12S^2T^2 + 8ST^3 + 4T^4 = 1.$$

We will use the method of Tzanakis and de Weger to solve this Thue equation, finding that $(S, T) = (\pm 1, 0)$ are the only solutions. To apply this method, we need a system of fundamental units for the ring of integers of $\mathbb{Q}(\alpha)$ where $F(\alpha, 1) = 0$. We find, by the methods of Pohst and Zassenhaus [14], that $\{\epsilon_1 = (\alpha^3 - 4\alpha^2 - 10\alpha + 12)/4, \epsilon_2 = (2\alpha^3 - 9\alpha^2 - 20\alpha + 26)/4, \epsilon_3 = (2\alpha^3 - 9\alpha^2 - 24\alpha + 26)/4\}$ is such a system. We give some of the details of the computations used to solve this Thue equation in Table 5 of §6. From these solutions of the Thue equation, we find that $(W, Z) = (\pm 1, \pm 1)$ are the only solutions of $W^2 + 2 = 3Z^4$ and thus the complete solution of $F_{12}(X, Y) = -2$ with $X + 2Y = Z^2$ is $(X, Y) \in \{(-5, 3), (-1, 1)\}$.

If $k = -3$, then $W = 3V$ and we obtain the equation $Z^4 - 3V^2 = 1$. Ljunggren [13] has shown that $(V, Z) = (0, \pm 1)$ are the only integer solutions. Therefore the complete solution of $F_{12}(X, Y) = -3$ with $X + 2Y$ a perfect square is $(X, Y) = (-3, 2)$.

For $k = 6$, we have $W = 3V$, which leads to the equation $3V^2 - Z^4 = 2$, the special case $A = 3$ of the equation in Lemma 5(i). The methods of Pohst

and Zassenhaus [14] show that $\epsilon_1 + \epsilon_1' + 2 = 24 + 12\sqrt{3}$, which gives rise to no solutions, and $\epsilon_2 + \epsilon_2' + 2 = 8 + 4\sqrt{3}$, which gives rise to the solutions $(V, Z) = (\pm 1, \pm 1)$. Thus, the complete solution of $F_{12}(X, Y) = 6$ with $X + 2Y$ a perfect square is $(X, Y) \in \{(-9, 5), (3, -1)\}$.

Again, the Lucas sequences which arise from these solutions are given in Table 1.

4. THE ALGORITHM

We now describe the algorithm which is used to solve these Thue equations. We will follow the notation and numbering of constants from the paper of Tzanakis and de Weger [19], except that we use d where they use n and label our linear forms more explicitly. The reader will find in their paper proofs of the lemmas below as well as explicit formulas for the constants mentioned below.

Suppose we wish to solve $F(X, Y) = m$, where

$$F(X, Y) = X^d + f_{d-1}X^{d-1}Y + \cdots + f_0 Y^d \in \mathbb{Z}[X, Y]$$

is a monic irreducible polynomial of total degree $d \geq 3$ and m is a nonzero integer. Let $\xi = \xi^{(1)}, \ldots, \xi^{(d)}$ be the roots of $g(X) = F(X, 1)$, which we shall assume are all real, and let $\mathbb{K} = \mathbb{Q}(\xi)$. Notice that $[\mathbb{K} : \mathbb{Q}] = d$.

It is not necessary to assume that $F(X, Y)$ is monic or that the roots of $g(X)$ are all real in the method of Tzanakis and de Weger but it is true for the Thue equations we consider here and it simplifies the description somewhat.

Let $\{\epsilon_1, \ldots, \epsilon_{d-1}\}$ be a system of fundamental units of $\mathscr{O}_K$, the ring of integers in $\mathbb{K}$. We can partition the set of elements μ of $\mathscr{O}_K$ with $\mathscr{N}_{K/\mathbb{Q}}(\mu) = m$ into finitely many equivalence classes under the relation of being associates (see the corollary to Theorem 5 on p. 90 of [3]) and let $\mathscr{M}$ be a complete set of representatives of these equivalence classes. Notice that if $|m| = 1$, then $\mathscr{M} = \{1\}$. By Lemma 3, for our applications, when $m \neq \pm 1$, $\mathscr{M}$ contains only the generator of the ideal specified in there.

4.1. An initial upper bound via linear forms in logarithms.
For $(x, y) \in \mathbb{Z}^2$ satisfying $F(x, y) = m$, we put $\beta = x - \xi y$. For each i and any choice of j, k satisfying $i \neq j \neq k \neq i$, we let

$$\Lambda(i, j, k, \mu) = \log \left| \frac{\xi^{(i)} - \xi^{(j)}}{\xi^{(i)} - \xi^{(k)}} \frac{\beta^{(k)}}{\beta^{(j)}} \right|,$$

which we will express as a linear form in logarithms. For this purpose notice that

$$\beta = \pm \mu \epsilon_1^{a_1} \cdots \epsilon_{d-1}^{a_{d-1}},$$

where $a_1, \ldots, a_{d-1} \in \mathbb{Z}$ and $\mu \in \mathscr{M}$. Using the notation

$$\alpha_0 = \left| \frac{\xi^{(i)} - \xi^{(j)}}{\xi^{(i)} - \xi^{(k)}} \frac{\mu^{(k)}}{\mu^{(j)}} \right| \quad \text{and} \quad \alpha_i = \left| \frac{\epsilon_i^{(k)}}{\epsilon_i^{(j)}} \right| \quad \text{for } 1 \leq i \leq d - 1,$$

we have

$$\Lambda(i, j, k, \mu) = \log \alpha_0 + a_1 \log \alpha_1 + \cdots + a_{d-1} \log \alpha_{d-1}.$$

Let $A = \max(6, |a_1|, \ldots, |a_{d-1}|)$. The use of 6 here is somewhat arbitrary. To apply the known results to determine a lower bound for the absolute value of these linear forms, we need only have 3 here. However, using 6 will yield some stronger and simpler estimates in what follows, while imposing no significant restrictions.

Lemma 6. *There exist effectively computable constants C_5, C_6, Y_1 and Y_2' depending only on $g(X)$, $\mathbb{K}$ and the elements of $\mathcal{M}$ such that the following statements are true:*

    (i) *If $|y| > Y_1$, then x/y is a convergent from the continued fraction expansion of $\xi^{(i_0)}$ for some $1 \le i_0 \le d$.*

    (ii) *Suppose that $|y| > Y_2'$. Then, for i_0 as in (i), for any choice of j and k satisfying $i_0 \ne j \ne k \ne i_0$ and any $\mu \in \mathcal{M}$, we have*

$$|\Lambda(i_0, j, k, \mu)| < C_6 \exp\left(-\frac{d}{C_5}A\right).$$

Proof. This is a combination of Lemmas 1.1, 1.2, 2.1 and 2.2 of [19]. □

Let $\gamma_1, \ldots, \gamma_r$ be algebraic numbers with $D = [\mathbb{Q}(\gamma_1, \ldots, \gamma_r) : \mathbb{Q}]$ and

$$L = b_1 \log \gamma_1 + \cdots + b_r \log \gamma_r,$$

with $b_1, \ldots, b_r \in \mathbb{Z}$ and $B = \max(|b_1|, \ldots, |b_r|, 3)$. We put

$$h'(\gamma_i) = \max(h(\gamma_i), |\log \gamma_i|/D, 1/D)$$

for $i = 1, \ldots, r$, where $h(\gamma_i)$ is the absolute logarithmic height of γ_i and let $H = h'(\gamma_1) \cdot \cdots \cdot h'(\gamma_r)$. With $K_4 = 18(r+1)! r^{r+1}(32D)^{r+2} \log(2Dr)H$, we can now state a recent result of Baker and Wüstholz.

Lemma 7. *If $L \ne 0$, then*

$$|L| > \exp(-K_4 \log B).$$

Proof. See Baker and Wüstholz [2]. □

One might expect that we will apply this result to the $\Lambda(i_0, j, k, \mu)$'s. However, it will frequently be the case that there are multiplicative relations between the α_i's. These relations will allow us to eliminate some of the terms in the $\Lambda(i_0, j, k, \mu)$'s, obtaining new linear forms, $\Lambda'(i_0, j, k, \mu)$, in fewer terms. It will turn out that $\Lambda'(i_0, j, k, \mu) = t_0 \Lambda(i_0, j, k, \mu)$, where t_0 is a positive integer which depends on the particular form. Also the maximum, A', of the absolute values of the coefficients of the $\Lambda'(i_0, j, k, \mu)$ can be shown to be at most A^2 since $A \ge 6$ (see §4.3).

Tzanakis and de Weger show in the proof of Lemma 2.4 of their paper [19] that, for $|y| > Y_2'$, one has $\Lambda(i_0, j, k, \mu) \ne 0$. Therefore, we can apply Lemma 7 to show that, for $|y| > Y_2'$,

$$|\Lambda'(i_0, j, k, \mu)| > \exp(-K_4 \log A').$$

Thus, for $|y| > Y_2'$,

$$|\Lambda(i_0, j, k, \mu)| > \exp(-2K_4 \log A)/t_0.$$

In accordance with the notation in [19], we shall label this constant $2K_4$ as C_7.

We also mention that the maximal real subfield of a cyclotomic field is a Galois extension of $\mathbb{Q}$, so $D = d$, with the exception of the equation arising from $n = 12$, $k = -2$, where we let $D = 24$.

We can use this lower bound to prove the following lemma.

Lemma 8. *Put*

$$C_9 = \frac{2C_5}{d} \left(\log(t_0 C_6) + C_7 \log\left(\frac{C_5 C_7}{d}\right) \right).$$

If $|y| > Y_2'$, then $A < C_9$.

Proof. This is Lemma 2.4 of [19] except that we replace C_6 by $t_0 C_6$. □

Applying this lemma to our linear forms, we obtain an upper bound for A. By examining the tables at the end of the paper, we see that this bound is very large, too large in fact to allow us to completely determine all solutions of $F(X, Y) = m$ in any naive way. We will use the so-called L^3 algorithm for lattice basis reduction to reduce the size of these upper bounds to the point where a direct search is feasible. Our implementation of this algorithm will be the iterative integer version given by de Weger in §3 of [6]. We then use either Proposition 3.1 or Proposition 3.2 of [19] to obtain an improved upper bound for A.

4.2. An improved upper bound from the L^3 algorithm. Before using the L^3 algorithm, there are two conditions we must check. First we check for linear relations over $\mathbb{Z}$ among $\log\alpha_1, \ldots, \log\alpha_{d-1}$. If such relations exist, then $|\mathbf{b}_1|$ defined below will likely be too small for the hypotheses of Lemmas 9 and 10 to hold. Therefore, we must first eliminate such dependencies. This has an advantage too, as we can replace $\Lambda(i_0, j, k, \mu)$ by a linear form with fewer terms and hence obtain smaller values of C_7 and C_9. Also the L^3 algorithm will run faster since we can then apply it to a smaller matrix with smaller entries.

We must also check whether $\log\alpha_0$ is a linear combination of $\log\alpha_1, \ldots, \log\alpha_{d-1}$ over $\mathbb{Z}$. If this is the case, then the quantity $\|s_k\|$ in Lemma 9 will be too small. We discuss this situation after Lemma 9.

By reordering the α_i's if necessary, we may assume that $\{\log\alpha_1, \ldots, \log\alpha_p\}$, where $p \leq d - 1$, is a $\mathbb{Q}$-linearly independent set. Proceeding as Tzanakis and de Weger do in case (iii) of §II.3 of their paper [19], we can find integers $t_0 > 0$ and t_{ij} for $1 \leq i \leq p$, $p + 1 \leq j \leq d - 1$ such that

$$t_0 \log\alpha_j = \sum_{i=1}^{p} t_{ij} \log\alpha_i \quad \text{for } j = p + 1, \ldots, d - 1$$

(notice that we use t_0 and t_{ij} where Tzanakis and de Weger [19] use d and d_{ij}). Using these relations, we can eliminate the terms for $\alpha_{p+1}, \ldots, \alpha_{d-1}$ from our linear form $\Lambda(i_0, j, k, \mu)$, obtaining

$$\Lambda'(i_0, j, k, \mu) = t_0 \Lambda(i_0, j, k, \mu) = t_0 \log \alpha_0 + \sum_{i=1}^{p} a'_i \log \alpha_i,$$

where

$$a'_i = t_0 a_i + \sum_{j=p+1}^{d-1} t_{ij} a_j.$$

Letting $T = \max(t_0, |t_{ij}| : 1 \le i \le p, p+1 \le j \le d-1)$, we have

$$(2) \qquad |\Lambda'(i_0, j, k, \mu)| < t_0 C_6 \exp\left(\frac{d}{C_4} A\right) \qquad \text{with } A < C_9$$

by Lemmas 6(ii)–8, and

$$|a'_i| \le (d-p) T A \qquad \text{for } i = 1, \ldots, p.$$

With $\log \alpha_1, \ldots, \log \alpha_p$ being $\mathbb{Q}$-linearly independent, we now apply the L^3 algorithm to the matrix

$$\mathscr{A} = \begin{pmatrix} 1 & 0 & \cdots & & 0 \\ 0 & \ddots & 0 & & 0 \\ \vdots & & 0 & 1 & 0 \\ [c_0 \log \alpha_1] & \cdots & & \cdots & [c_0 \log \alpha_p] \end{pmatrix},$$

where c_0 is a real number somewhat larger than C_9^p, and obtain a matrix we will denote by $\mathscr{B}$. Let

$$\mathbf{x} = (0, \ldots, 0, -[c_0 t_0 \log \alpha_0])^T = \sum_{i=1}^{p} s_i \mathbf{b}_i,$$

where $\mathbf{b}_i$ is the vector formed from the ith column of $\mathscr{B}$ and $s_1, \ldots, s_p \in \mathbb{R}$. Let k be the largest integer such $s_k \notin \mathbb{Z}$, and for $x \in \mathbb{R}$ denote by $\|x\|$ the distance from x to the nearest integer.

Lemma 9. *Suppose*

$$2^{-(p-1)/2} \|s_k\| \cdot |\mathbf{b}_1| \ge \sqrt{p^2 + 5p + 3}\,(d-p) T C_9.$$

Then there are no solutions of $|\Lambda(i_0, j, k, \mu)| < C_6 \exp(-dA/C_5)$ *with*

$$A > \frac{C_5}{d} \log\left(\frac{c_0 t_0 C_6}{(d-p) T C_9}\right).$$

Proof. This lemma is a slight modification of Proposition 3.2 of [19] (we obtain a result for A whereas their result pertains to an upper bound for the $|a'_i|$'s). The proof is nearly identical to the proof of Lemma 3.10 in [7], the result upon which Proposition 3.2 of [19] is based, except that at the very end of the proof we use the upper bound for $|\Lambda'(i_0, j, k, \mu)|$ in (2) which is in terms of A to get our result in terms of A. □

As we stated above, if $\log \alpha_0$ is a linear combination of $\log \alpha_1, \ldots, \log \alpha_{d-1}$ over $\mathbb{Z}$, then the quantity $\|s_k\|$ may be quite small. In this case we eliminate $\log \alpha_0$ from our linear forms. This situation only occurs for the Thue equations

we consider with $n = 7$ and $n' = 9$. Let us now describe how we deal with this situation.

Suppose

$$t_0 \log \alpha_0 + \cdots + t_{d-1} \log \alpha_{d-1} = 0,$$

with $t_0, \ldots, t_{d-1} \in \mathbb{Z}$ satisfying $t_0 > 0$, and let $T = \max(|t_0|, \ldots, |t_{d-1}|)$. Letting $a_i' = a_i t_0 - t_i$ for $1 \leq i \leq d - 1$, we have

$$\Lambda'(i_0, j, k, \mu) = t_0 \Lambda(i_0, j, k, \mu) = a_1' \log \alpha_1 + \cdots + a_{d-1}' \log \alpha_{d-1}.$$

Notice that $A' = \max(3, |a_1'|, \ldots, |a_{d-1}'|) \leq T(A + 1) < 1.17 T A$, since $A \geq 6$.

Thus, we have

$$|\Lambda'(i_0, j, k, \mu)| < t_0 C_6 \exp\left(-\frac{6d}{7C_5 T} A'\right) \quad \text{with } A' < 1.17 T C_9,$$

by Lemmas 6(ii)–8.

For the Thue equations arising from $n = 7$ and 9, we have that $\log \alpha_1, \ldots, \log \alpha_{d-1}$ are linearly independent over $\mathbb{Q}$. Thus, we are ready to apply the L^3 algorithm, our use of which shall be similar to the previous case: we apply the algorithm to the same matrix $\mathcal{A}$ as before, here with $p = d - 1$, obtaining the matrix $\mathcal{B}$.

Lemma 10. *Suppose*

$$2^{(d-2)/2} |\mathbf{b}_1| > 1.17 \sqrt{d^2 + d - 2}\, T C_9.$$

Then there are no solutions of $|\Lambda(i_0, j, k, \mu)| < C_6 \exp(-dA/C_5)$ *with*

$$A > \left(\frac{1.16 C_5 T}{d} \log\left(\frac{0.85 c_0 C_6}{C_9}\right) + T\right) / t_0.$$

Proof. Letting $q = d - 1$, we have $q^2 + q - 1 = d^2 - d - 1$, and so the hypothesis of Proposition 3.1 from [19] holds. Thus, we see that

$$A' > \frac{1.16 C_5 T}{d} \log\left(\frac{c_0 t_0 C_6}{1.17 T C_9}\right).$$

Since $T \geq t_0$, our bound for A now follows from the fact that our definition of the a_i''s shows that $A \leq (A' + T)/t_0$. □

4.3. Searching for solutions of $F(X, Y) = m$**.** We construct linear forms in logarithms as in §4.1 and using the methods described above, get a good upper bound for the size of the coefficients of these linear forms. We must do this for each i_0 between 1 and d and each $\mu \in \mathcal{M}$. However, because of the large bound we obtain from Lemma 8, the L^3 algorithm takes a long time to run when d is large. But one notices that only α_0 depends on i_0 and μ, so the matrix $\mathcal{A}$ defined in §4.2 depends only on the j and k defined in §4.1. When $d \geq 4$, we can choose (j_1, k_1) and (j_2, k_2) with $(j_1, k_1) \neq (j_2, k_2)$ so that we need only apply the L^3 algorithm to two matrices of the form $\mathcal{A}$: if $i_0 = j_1$ or $i_0 = k_1$, we let $j = j_2$ and $k = k_2$, otherwise we let $j = j_1$ and $k = k_1$. We choose (j_1, k_1) and (j_2, k_2) so that $\epsilon_i^{(k_1)}/\epsilon_i^{(j_1)}$ and $\epsilon_i^{(k_2)}/\epsilon_i^{(j_2)}$

are conjugates for $i = 1, \ldots, d - 1$. This simplifies the height calculations necessary for Lemma 7. And more importantly, we choose them to minimize the number of $\mathbb{Q}$-linearly independent $\log \alpha_i$'s.

We then compute the quantities C_5, C_6, Y_1 and Y_2'. Next we apply Lemma 7 to the $\Lambda'(i_0, j, k, \mu)$'s to determine K_4. Notice that this lemma will give us a lower bound in terms of A'. We saw in §4.2 that either $A' \leq (d - p)TA$ or $A' \leq 1.1TA$. An examination of the relations in the next section shows that both $(d - p)T$ and $1.1T$ are at most 6 and, since we have assumed $A \geq 6$, we have $A' \leq A^2$. Thus, for C_7 we use $2K_4$. From these quantities we find C_9. Applying the L^3 algorithm as described above considerably reduces the upper bound for A, and then applying the L^3 a second time, using this new upper bound for A in place of C_9, we obtain a still smaller upper bound. At this point we wish to determine an upper bound for $|y|$ from this last upper bound for A. We use the following lemma.

Lemma 11. *Suppose* $(x, y) \in \mathbb{Z}^2$ *is a solution of* $F(X, Y) = m$ *and* $A < C_{10}$. *Then*

$$|y| \leq Y_3 = \min_{1 \leq j_1 < j_2 \leq d} \left(\mu_+ \frac{E_{j_1}^{C_{10}} + E_{j_2}^{C_{10}}}{\xi^{(j_1)} - \xi^{(j_2)}} \right),$$

where $E_j = \prod_{i=1}^{d-1} \left| \epsilon_i^{(j)} \right|^{v_{ij}}$, $\mu_+ = \max_{1 \leq i \leq d, \mu \in \mathcal{M}} |\mu^{(i)}|$ *and* $v_{ij} = \pm 1$ *whichever makes* $\left| \epsilon_i^{(j)} \right|^{v_{ij}} \geq 1$.

Proof. This is proven on p. 118 of the paper [19] of Tzanakis and de Weger. □

Now we perform a direct search for solutions with $|y| \leq Y_1$ and then check whether (x, y) is a solution of $F(X, Y) = m$, where x/y is a convergent of $\zeta^{(i)}$ with $|y| \leq Y_3$ for each $1 \leq i \leq d$. In this manner we are able to determine the complete solution of the Thue equation $F(X, Y) = m$.

5. DEPENDENCE RELATIONS

In §4.2, we described what to do when dependence relations arise among the $\log \alpha_i$'s. Here we give the relations that were found in our applications. These relations were found either by making use of the nice form of the α_i's when n is a prime power and by direct search otherwise.

Let us first establish an ordering of the units and their conjugates. In the case of $n \neq 12$, let $a_1 = 1, \ldots, a_{\varphi(n)/2-1}$ be the increasing sequence of positive integers less than $n/2$ which are relatively prime to n. In accordance with Lemma 4, we let

$$\epsilon_i^{(j)} = \pm \frac{\sin(a_{i+1}a_j\pi/n)}{\sin(a_j\pi/n)}$$

denote the jth conjugate of the ith fundamental unit. Notice that for our purposes here, knowledge of the conjugates up to sign suffices, for the α_i's are defined to be the absolute value of quotients of these conjugates.

For the Thue equation which arises from $n = 12$, we order the roots of $F(S, 1)$ as follows: $\alpha^{(1)} = 1 + \sqrt{3} + \sqrt{6 + 2\sqrt{3}}$, $\alpha^{(2)} = 1 + \sqrt{3} - \sqrt{6 + 2\sqrt{3}}$, $\alpha^{(3)} = 1 - \sqrt{3} + \sqrt{6 - 2\sqrt{3}}$ and $\alpha^{(4)} = 1 - \sqrt{3} - \sqrt{6 - 2\sqrt{3}}$. The meaning of $\epsilon_i^{(j)}$ is then clear, using the labelling of the fundamental units in §3.4.

We now consider the dependence relations themselves.

For $n = 7$ and 9, we let $(j, k) = (2, 3)$ when $i_0 = 1$, $(j, k) = (1, 3)$ when $i_0 = 2$, and $(j, k) = (1, 2)$ when $i_0 = 3$. As we mentioned in §4.2, $\log \alpha_0$, $\log \alpha_1$ and $\log \alpha_2$ are linearly dependent over $\mathbb{Q}$. When $n = 7$ and $m = \pm 1$, we have

$$3 \log \alpha_0 = \log \alpha_1 - 2 \log \alpha_2,$$

for each choice of i_0, j and k. When $n = 7$ and $m = \pm 7$, we have

$$\log \alpha_0 = -\log \alpha_1 - 2 \log \alpha_2,$$

for each choice of i_0, j and k. So we let $t_0 = 3$ and $T = 6$.

When $n = 9$ and $m = \pm 1$, we have

$$3 \log \alpha_0 = 2 \log \alpha_1 - \log \alpha_2,$$

for each choice of i_0, j and k. When $n = 9$ and $m = \pm 3$, we have

$$\log \alpha_0 = -\log \alpha_2,$$

for each choice of i_0, j and k. Here we can use $t_0 = 3$ and $T = 3$.

For $n = 11$, we let $(j, k) = (1, 2)$ if $i_0 \neq 1, 2$ and $(j, k) = (3, 5)$ otherwise. With this choice, $\log \alpha_1$, $\log \alpha_2$, $\log \alpha_3$, $\log \alpha_4$ are $\mathbb{Q}$-linearly independent.

For $n = 12$ with $k = -2$, we let $(j, k) = (1, 3)$ if $i_0 \neq 1, 3$ and $(j, k) = (2, 4)$ otherwise. In both cases, $\log \alpha_1$, $\log \alpha_2$, $\log \alpha_3$ are $\mathbb{Q}$-linearly independent, and so we let $\Lambda' = \Lambda$.

For $n = 13$, we let $(j, k) = (1, 5)$ if $i_0 \neq 1, 5$ and $(j, k) = (2, 3)$ otherwise. In both cases, we have

$$\alpha_1 = \alpha_3 \alpha_5 / \alpha_2 \quad \text{and} \quad \alpha_4 = \alpha_3 \alpha_5.$$

We let

$$\Lambda' = \log \alpha_0 + a_1' \log \alpha_2 + a_2' \log \alpha_3 + a_3' \log \alpha_5.$$

For $n = 15$, we let $(j, k) = (1, 2)$ if $i_0 \neq 1, 2$ and $(j, k) = (3, 4)$ otherwise. With this choice, $\log \alpha_1$, $\log \alpha_2$, $\log \alpha_3$ are $\mathbb{Q}$-linearly independent.

For $n = 16$, we let $(j, k) = (1, 4)$ if $i_0 \neq 1, 4$ and $(j, k) = (2, 3)$ otherwise. In both cases, we have $\alpha_3 = \alpha_1 \alpha_2$. So we let

$$\Lambda' = \log \alpha_0 + a_1' \log \alpha_1 + a_2' \log \alpha_2.$$

For $n = 17$, we let $(j, k) = (1, 4)$ if $i_0 \neq 1, 4$ and $(j, k) = (2, 8)$ otherwise. In both cases, we have

$$\alpha_1 = \alpha_5 \alpha_6 / \alpha_7, \quad \alpha_2 = \alpha_5 \alpha_6 / \alpha_4 \quad \text{and} \quad \alpha_3 = \alpha_5 \alpha_6.$$

So we let

$$\Lambda' = \log \alpha_0 + a_1' \log \alpha_4 + a_2' \log \alpha_5 + a_3' \log \alpha_6 + a_4' \log \alpha_7.$$

For $n = 19$, we let $(j, k) = (1, 7)$ if $i_0 \neq 1, 7$ and $(j, k) = (2, 5)$ otherwise. In both cases, we have

$$\alpha_3 = \alpha_1 \alpha_2 \alpha_4 / (\alpha_5 \alpha_8) \quad \text{and} \quad \alpha_6 = \alpha_1 \alpha_2 \alpha_4 / \alpha_7.$$

So we let

$$\Lambda' = \log\alpha_0 + a_1'\log\alpha_1 + a_2'\log\alpha_2 + a_3'\log\alpha_4 + a_4'\log\alpha_5 + a_5'\log\alpha_7 + a_6'\log\alpha_8.$$

For $n = 20$, we let $(j, k) = (1, 2)$ if $i_0 \neq 1, 2$ and $(j, k) = (3, 4)$ otherwise. With this choice, $\log\alpha_1$, $\log\alpha_2$ and $\log\alpha_3$ are $\mathbb{Q}$-linearly independent, so we let $\Lambda' = \Lambda$.

For $n = 21$, we let $(j, k) = (1, 5)$ if $i_0 \neq 1, 5$ and $(j, k) = (2, 4)$ otherwise. In both cases, we have

$$\alpha_4 = \alpha_3/\alpha_1 \quad \text{and} \quad \alpha_5 = 1/\alpha_1.$$

So we let

$$\Lambda' = \log\alpha_0 + a_1'\log\alpha_1 + a_2'\log\alpha_2 + a_3'\log\alpha_3.$$

For $n = 23$, we let $(j, k) = (1, 2)$ if $i_0 \neq 1, 2$ and $(j, k) = (3, 6)$ otherwise. With this choice, $\log\alpha_1, \ldots, \log\alpha_{10}$ are $\mathbb{Q}$-linearly independent.

For $n = 24$, we let $(j, k) = (1, 2)$ if $i_0 \neq 1, 2$ and $(j, k) = (3, 4)$ otherwise. In both cases, we have $\alpha_2\alpha_3 = \alpha_1^3$. So

$$\Lambda' = 3\log\alpha_0 + a_2'\log\alpha_2 + a_3'\log\alpha_3.$$

For $n = 25$, we let $(j, k) = (2, 9)$ if $i_0 \neq 2, 9$ and $(j, k) = (4, 3)$ otherwise. In both cases, we have

$$\alpha_1 = \alpha_5/\alpha_8, \qquad \alpha_2 = \alpha_5/\alpha_3,$$
$$\alpha_4 = \alpha_5/\alpha_6 \text{ and } \alpha_7 = \alpha_5/\alpha_9.$$

So we let

$$\Lambda' = \log\alpha_0 + a_1'\log\alpha_3 + a_2'\log\alpha_5 + a_3'\log\alpha_6 + a_4'\log\alpha_8 + a_5'\log\alpha_9.$$

For $n = 29$, we let $(j, k) = (1, 12)$ if $i_0 \neq 1, 12$ and $(j, k) = (2, 5)$ otherwise. In both cases, we have

$$\alpha_1 = \alpha_{10}\alpha_{12}/\alpha_4, \qquad \alpha_2 = \alpha_{10}\alpha_{12}/\alpha_6,$$
$$\alpha_3 = \alpha_{10}\alpha_{12}/\alpha_9, \qquad \alpha_5 = \alpha_{10}\alpha_{12}/\alpha_{13},$$
$$\alpha_7 = \alpha_{10}\alpha_{12}/\alpha_8 \text{ and } \alpha_{11} = \alpha_{10}\alpha_{12}.$$

So we let

$$\Lambda' = \log\alpha_0 + a_1'\log\alpha_4 + a_2'\log\alpha_6 + a_3'\log\alpha_8$$
$$+ a_4'\log\alpha_9 + a_5'\log\alpha_{10} + a_6'\log\alpha_{12} + a_7'\log\alpha_{13}.$$

6. Tables of results

6.1. Equations solved by the algorithm of Tzanakis and de Weger.
For $n = 7, 9, 11, 13, 15, 16, 17, 19, 20, 21, 23, 24, 25$ and 29, as well as $n = 12$ with $k = -2$, we used the method of Tzanakis and de Weger as described in §4 to solve the Thue equations which arise. The method was implemented using the MAPLE V Computer Algebra System on an 80486 DX2 based IBM-compatible PC running at 50 MHz. In Tables 3 and 4 we list the equations solved by

TABLE 3

n	$F_n(X, Y) = m$
7	$X^3 + X^2Y - 2XY^2 - Y^3 = \pm1, \pm7$
9	$X^3 - 3XY^2 + Y^3 = \pm1, \pm3$
11	$X^5 + X^4Y - 4X^3Y^2 - 3X^2Y^3 + 3XY^4 + Y^5 = \pm1, \pm11$
12	$X^4 - 4X^3Y - 12X^2Y^2 + 8XY^3 + 4Y^4 = 1$
13	$X^6 + X^5Y - 5X^4Y^2 - 4X^3Y^3 + 6X^2Y^4 + 3XY^5 - Y^6 = \pm1, \pm13$
15	$X^4 - X^3Y - 4X^2Y^2 + 4XY^3 + Y^4 = \pm1, \pm5$
16	$X^4 - 4X^2Y^2 + 2Y^4 = \pm1, \pm2$
17	$X^8 + X^7Y - 7X^6Y^2 - 6X^5Y^3 + 15X^4Y^4$
	$+10X^3Y^5 - 10X^2Y^6 - 4XY^7 + Y^8 = \pm1, \pm17$

TABLE 4

n	$F_n(X, Y) = m$
19	$X^9 + X^8Y - 8X^7Y^2 - 7X^6Y^3 + 21X^5Y^4$
	$+15X^4Y^5 - 20X^3Y^6 - 10X^2Y^7 + 5XY^8 + Y^9 = \pm1, \pm19$
20	$X^4 - 5X^2Y^2 + 5Y^4 = \pm1, \pm5$
21	$X^6 - X^5Y - 6X^4Y^2 + 6X^3Y^3 + 8X^2Y^4 - 8XY^5 + Y^6 = \pm1, \pm7$
23	$X^{11} + X^{10}Y - 10X^9Y^2 - 9X^8Y^3 + 36X^7Y^4 + 28X^6Y^5$
	$-56X^5Y^6 - 35X^4Y^7 + 35X^3Y^8 + 15X^2Y^9 - 65XY^{10} - Y^{11} = \pm1, \pm23$
24	$X^4 - 4X^2Y^2 + Y^4 = \pm1, \pm2$
25	$X^{10} - 10X^8Y^2 + 35X^6Y^4 + X^5Y^5 - 50X^4Y^6$
	$- 5X^3Y^7 + 25X^2Y^8 + 5XY^9 - Y^{10} = \pm1, \pm5$
29	$X^{14} + X^{13}Y - 13X^{12}Y^2 - 12X^{11}Y^3 + 66X^{10}Y^4$
	$+55X^9Y^5 - 165X^8Y^6 - 120X^7Y^7 + 210X^6Y^8 + 126X^5Y^9$
	$-126X^4Y^{10} - 56X^3Y^{11} + 28X^2Y^{12} + 7XY^{13} - Y^{14} = \pm1, \pm29$

this method. These are followed by three tables (Tables 5–7) containing an abridgement of the output from these programs for each equation solved. The entries in these latter tables have been rounded up or down, as appropriate. Requests for more information regarding these computations are, of course, welcome.

The first entries in Tables 5–7, before d_1, are listed using the notation of §4. As mentioned above, the L^3 algorithm was used twice. The first time we let $c_0 = 10^{d_1}$ from which we obtained $A \le A_1$. The second time, we let $c_0 = 10^{d_2}$ and found that $A \le A_2$. These quantities, A_1, A_2, d_1 and d_2, are listed in these tables. Finally, we used Lemma 11 to obtain an upper bound for $|y|$ from $A \le A_2$. This is listed in Tables 5–7 under the entry Y_3. The entry X_4 (resp. Y_4) is the maximum of the absolute value of x (resp. y) for all solutions (x, y) to the Thue equations which arise for each n. A complete list of solutions has

TABLE 5

n	7	9	11	12($k = -2$)	13
d	3	3	5	4	6
Y_1	49	19	6	2	5
Y_2'	49	19	12	2	17
d/C_5	1.127	1.508	1.584	2.171	1.834
C_6	5900	18000	$5 \cdot 10^8$	48000	$2 \cdot 10^{11}$
H	0.218	0.317	0.0373	1.162	0.132
C_7	$8 \cdot 10^{10}$	$1.2 \cdot 10^{11}$	$1.6 \cdot 10^{23}$	$6 \cdot 10^{24}$	$1.2 \cdot 10^{20}$
C_9	$4 \cdot 10^{12}$	$4 \cdot 10^{12}$	$2 \cdot 10^{25}$	$3 \cdot 10^{27}$	$6 \cdot 10^{21}$
d_1	29	29	120	90	77
A_1	61	84	150	72	82
d_2	8	8	20	18	16
A_2	30	42	38	22	31
Y_3	$8 \cdot 10^{13}$	$3 \cdot 10^{27}$	10^{33}	$3 \cdot 10^{36}$	$3 \cdot 10^{32}$
(X_4, Y_4)	$(9, 9)$	$(3, 3)$	$(2, 1)$	$(1, 0)$	$(3, 2)$
time	70 s	62 s	94 s	81 s	60 s

TABLE 6

n	15	16	17	19	20
d	4	4	8	9	4
Y_1	9	4	4	4	6
Y_2'	11	4	29	37	7
d/C_5	1.034	1.738	2.265	2.564	0.869
C_6	610000	30000	$7 \cdot 10^{16}$	$6 \cdot 10^{19}$	$5.6 \cdot 10^7$
H	0.129	0.671	0.0887	0.0207	0.333
C_7	$8.7 \cdot 10^{18}$	$5.2 \cdot 10^{15}$	$1.2 \cdot 10^{25}$	$1.2 \cdot 10^{34}$	$2.3 \cdot 10^{19}$
C_9	$8 \cdot 10^{20}$	$3 \cdot 10^{21}$	$6 \cdot 10^{26}$	$7 \cdot 10^{35}$	$3 \cdot 10^{21}$
d_1	70	48	130	240	74
A_1	122	46	121	200	159
d_2	13	7	24	37	16
A_2	37	12	38	48	57
Y_3	$9 \cdot 10^{30}$	$8 \cdot 10^{10}$	$5 \cdot 10^{56}$	$9 \cdot 10^{83}$	$2 \cdot 10^{60}$
(X_4, Y_4)	$(4, 3)$	$(2, 1)$	$(2, 1)$	$(2, 1)$	$(2, 1)$
time	64 s	34 s	139 s	583 s	68 s

been omitted to save space; however, X_4 and Y_4 are sufficiently small that the interested reader could easily determine all solutions. The last entry gives the CPU time used for each n. We believe that the time is of interest, showing as it does that the method of Tzanakis and de Weger is practical even for Thue equations of moderate degree, provided the necessary system of fundamental units and factorization of m are known.

TABLE 7

n	21	23	24	25	29
d	6	11	4	10	14
Y_1	4	3	5	4	3
Y_2'	22	54	5	63	85
C_6	$7 \cdot 10^9$	$6 \cdot 10^{25}$	300000	$4 \cdot 10^{24}$	$2 \cdot 10^{35}$
d/C_5	0.833	2.89	0.758	2.07	3.854
H	0.260	0.00026	0.903	0.125	0.0177
C_7	$2.3 \cdot 10^{20}$	10^{53}	$7 \cdot 10^{15}$	$3.4 \cdot 10^{30}$	$5.5 \cdot 10^{40}$
C_9	$3 \cdot 10^{22}$	$8 \cdot 10^{54}$	$7 \cdot 10^{17}$	$3 \cdot 10^{32}$	$3 \cdot 10^{42}$
d_1	76	588	45	182	342
A_1	173	445	96	193	199
d_2	16	63	11	29	42
A_2	63	68	41	56	44
Y_3	$2 \cdot 10^{87}$	$9 \cdot 10^{149}$	$8 \cdot 10^{51}$	$3 \cdot 10^{123}$	$3 \cdot 10^{127}$
(X_4, Y_4)	(2, 1)	(2, 1)	(2, 2)	(2, 1)	(2, 1)
time	169 s	11356 s	51 s	595 s	2847 s

TABLE 8

n	14	18	22	26	27	28	30
m	7	9	11	13	9	14	15
(X_4, Y_4)	(9, 9)	(3, 3)	(2, 1)	(3, 2)	(2, 1)	(2, 1)	(4, 3)

6.2. Solutions of the equations with $n \equiv 2 \bmod 4$ or nonsquarefree.

With the notation of Lemma 2, if $n \geq 4$ is not a power of three with $m = 3$, then $P(n/(3, n)) = P(m/(3, m))$. If $\varphi(m)/2 \geq 3$ and we have determined all solutions of $F_m(X, Y) = \pm 1, \pm P(m/(3, m))$, then we can use Lemma 2(ii) to find all solutions of $F_n(X, Y) = \pm 1, \pm P(n/(n, 3))$.

Similarly, if $n = 2m$ where m is odd, we use Lemma 2(i). In Table 8 we give the values of m, X_4 and Y_4, where X_4 and Y_4 are as in the previous tables, when $14 \leq n \leq 30$ is nonsquarefree or $n \equiv 2 \bmod 4$.

BIBLIOGRAPHY

1. G. D. Birkhoff and H.S. Vandiver, *On the integral divisors for $a^n - b^n$*, Ann. of Math. (2) **5** (1904), 173–180.

2. A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. **442** (1993), 19–62.

3. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966.

4. R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, Ann. of Math. (2) **15** (1913), 30–70.

5. J. H. E. Cohn, *Squares in some recurrent sequences*, Pacific J. Math. **41** (1972), 24–28.

6. B. M. M. de Weger, *Solving exponential diophantine equations using lattice basis reduction algorithms*, J. Number Theory **26** (1987), 325–367.

7. B. M. M. de Weger, *Algorithms for Diophantine equations*, CWI-Tract No. 65, Centre for Mathematics and Computer Science, Amsterdam, 1989.

8. B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Transl. Math. Monos., vol. 10, Amer. Math. Soc., Providence, RI, 1963.

9. L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. **9** (1959), 437–441.

10. G. Karpilovsky, *Field theory: Classical foundations and multiplicative groups*, Marcel Dekker, New York, 1988.

11. W. Ljunggren, *Über die unbestimmte Gleichung* $Ax^2 - By^4 = C$, Arch. Math. Naturv. **XLI, 10** (1938).

12. _____, *Einige Sätze über unbestimmte Gleichungen von der Form* $Ax^4 + Bx^2 + C = Dy^2$, Skrifter utgitt av Det Norske Videnskaps-Akademi I Oslo I. Mat.-Naturv. Klasse. **9** (1942).

13. _____, *Some remarks on the Diophantine equations* $x^2 - Dy^4 = 1$ *and* $x^4 - Dy^2 = 1$, J. London Math. Soc. **41** (1966), 542–544.

14. M. Pohst and H. Zassenhaus, *On effective computation of fundamental units. I and II*, Math. Comp. **38** (1982), 275–291, 293–329.

15. N. Robbins, *Fibonacci numbers of the form* PX^2 , *where* P *is prime*, Fibonacci Quart. **21** (1983), 266–271.

16. A. Schnizel, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, J. Reine Angew. Math. **268/269** (1974), 27–33.

17. C. L. Stewart, *Primitive divisors of Lucas and Lehmer sequences*, Transcendence Theory: Advances and Applications (A. Baker and D.W. Masser, eds.), Academic Press, New York, 1977, pp. 79–92.

18. C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1977), 425–447.

19. N. Tzanakis and B. M. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), 99–132.

20. F. J. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), 693–707.

21. M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) **62** (1955), 230–236.

22. L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.

PROBLÈMES DIOPHANTIENS, UNIVERSITÉ P. ET M. CURIE (PARIS VI), MATHÉMATIQUES, UFR 920, TOUR 45-46, 5ÈME ETAGE, B.P. 172, 4, PLACE JUSSIEU, F-75252 PARIS CEDEX 05, FRANCE
E-mail address: voutier@moka.ccr.jussieu.fr