ACTA ARITHMETICA
152.3 (2012)

Using Lucas sequences to generalize a theorem of Sierpiński

by

Lenny Jones (Shippensburg, PA)

1. Introduction. The following concept, originally due to Erdős [11], is crucial to all results in this article.

Definition 1.1. A *covering* of the integers is a system of congruences $x \equiv r_i \pmod{m_i}$ such that every integer satisfies at least one of the congruences. A covering is said to be *finite* if contains only finitely many congruences.

Remark 1.2. Since all coverings in this paper are finite, we omit the word "finite".

In 1960, using a particular covering, Sierpiński [28] published a proof of the fact that there exist infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all natural numbers n. Any such value of k is called a *Sierpiński number*. Since then, several authors [5–9, 13–17, 19, 20] have investigated generalizations and variations of this result. We should also mention a paper of Riesel [25], which actually predates the paper of Sierpiński, in which Riesel proves a similar result for the sequence of integers $k \cdot 2^n - 1$. We give a proof of Sierpiński's original theorem since it provides an easy introduction to the techniques used in this paper.

Theorem 1.3 (Sierpiński [28]). *There exist infinitely many odd positive integers k such that $k \cdot 2^n + 1$ is composite for all integers $n \geq 1$.*

Proof. Consider the following covering $n \equiv r_i \pmod{m_i}$:

i	1	2	3	4	5	6	7
r_i	1	2	4	8	16	32	0
m_i	2	4	8	16	32	64	64

For each i, when $n \equiv r_i \pmod{m_i}$ and $k \equiv b_i \pmod{p_i}$ (from below),

2010 *Mathematics Subject Classification*: Primary 11B37, 11B39; Secondary 11D59.
Key words and phrases: coverings, Sierpiński numbers, Lucas sequences.

DOI: 10.4064/aa152-3-6

i	1	2	3	4	5	6	7
b_i	1	1	1	1	1	1	-1
p_i	3	5	17	257	65537	641	6700417

it is easy to check that $k \cdot 2^n + 1$ is divisible by p_i. Now, apply the Chinese remainder theorem to the system $k \equiv b_i \pmod{p_i}$. Then, for any integer $n \geq 0$, and any such solution k, we see that $k \cdot 2^n + 1$ is divisible by at least one prime from the set $\{3, 5, 17, 257, 641, 65537, 6700417\}$. ∎

This paper is concerned with generalizations of Theorem 1.3 which involve Lucas sequences. A pair (α, β) of algebraic integers, where $\alpha + \beta$ and $\alpha\beta$ are nonzero relatively prime rational integers, and α/β is not a root of unity, is called a *Lucas pair*. For $n \geq 0$, we can then define a sequence of rational integers

$$U_n(\alpha, \beta) := \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

When the values of α and β are general, or they are clear from the context of the discussion, we simply write U_n. Such a sequence is known as a *Lucas sequence of the first kind*. Unless otherwise stated, we assume throughout this paper, without loss of generality, that $\alpha > \beta$. The observation that

$$2^n = U_n(2, 1) + (2 - 1)^2$$

provides the motivation for the results in this paper. We replace 2^n with $U_n(\alpha, \beta) + (\alpha - \beta)^2$, and investigate when there exist infinitely many values of k such that the sequence

$$k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$$

is composite for all integers $n \geq 1$.

This paper is organized as follows. In Section 2, our focus is on the Lucas pairs (α, β) where α is a rational integer and $\beta = 1$. In Section 3, we consider Lucas pairs (α, β) where α and β are not necessarily rational. The rational Lucas pairs (α, β) covered in Section 3 have the property that $\alpha - \beta = 1$. Although the Lucas pair $(2, 1)$ from Theorem 1.3 falls into this category, the actual method used in the proof of Theorem 3.1 in Section 3 does not "capture" this particular Lucas pair. However, the technique can be modified to achieve this goal. In Section 4, we develop a more general approach. Theoretically, the techniques there can be used for any Lucas pair. However, it is difficult to categorize the Lucas pairs for which the methods will actually be successful.

A key idea in the proof of Theorem 1.3 is the availability of enough useful primes: a unique prime p corresponding to each congruence in the covering that allows us to reduce the power 2^n modulo p to an unambiguous value. In all main theorems in this article, we need such a set of primes. However,

the way these primes are "manufactured" is quite different in each section. Our approach in Section 2 is more typical of theorems of this nature. We use the concept of a *primitive divisor*; see Section 2 for a full explanation. But in Sections 3 and 4, the methods used to produce the desired primes appear to be new. In fact, it seems unlikely that traditional applications of primitive divisors could be used to prove the results in Sections 3 and 4.

2. Generalization I. In this section, we present a generalization of Theorem 1.3 whose proof utilizes the concept of a primitive divisor. As previously mentioned, primitive divisors are often useful in proving theorems similar to Theorem 1.3, and various related applications [6, 8, 9, 10, 19, 20, 31, 32].

DEFINITION 2.1. For any Lucas pair (α, β), we define a *primitive* (*prime*) *divisor* of U_n to be a prime p such that both of the following conditions hold:

- $U_n \equiv 0 \pmod{p}$,
- $(\alpha - \beta)^2 U_1 U_2 \cdots U_{n-1} \not\equiv 0 \pmod{p}$.

We say that the Lucas pair (α, β) is *n-defective* if U_n has no primitive divisor.

The following result, originally due to Zsigmondy [33], provides us with conditions in certain situations under which these primitive divisors exist.

THEOREM 2.2. *Let α and β be coprime positive rational integers with $\alpha > \beta$, and let $n \geq 2$ be an integer. Then there exists at least one prime p such that $\alpha^n - \beta^n \equiv 0 \pmod{p}$ and $\alpha^m - \beta^m \not\equiv 0 \pmod{p}$ for all positive integers $m < n$, with the following exceptions:*

- *$\alpha = 2$, $\beta = 1$ and $n = 6$,*
- *$\alpha + \beta$ is a power of 2 and $n = 2$.*

Theorem 2.2 is a generalization of the case when $\beta = 1$, which is due to Bang [1]. Birkhoff and Vandiver [3] proved Theorem 2.2 independently of Zsigmondy.

From Definition 2.1, the following corollary of Theorem 2.2 is immediate.

COROLLARY 2.3. *Let (α, β) be a rational Lucas pair, and let $n \geq 2$ be an integer. Then U_n has a primitive divisor, with the only exceptions being those noted in Theorem 2.2.*

The situation when α and β are not rational integers is much more difficult. When (α, β) is a real Lucas pair, Carmichael [4] showed that U_n has a primitive divisor for all $n > 12$. Much later, Schinzel [27] proved, for arbitrary Lucas pairs, that U_n has a primitive divisor for all $n \geq n_0$, where n_0 is an absolute constant independent of the Lucas pair. Stewart [29] made the work of Schinzel explicit by showing that $n_0 = e^{452}4^{67}$ would suffice, and reduced the problem to a finite computation. Strongly influenced by this

work of Stewart, Voutier [30] was able to improve this bound to $n_0 = 30030$, and more recently, Bilu, Hanrot and Voutier [2], have shown that U_n has a primitive divisor for all $n \geq 30$. They have also determined all n-defective Lucas pairs.

In this section, our focus is on Lucas pairs $(\alpha, 1)$, where α is a rational integer. The approach is somewhat conventional, in that we use a covering that is constructed by means of primitive divisors. However, complications arise in the proof, and we are forced to show the existence of a second primitive divisor in certain situations. In general, it is still a mystery as to exactly when U_n possesses a second primitive divisor. The best known results in this direction, when α and β are rational, are due to Schinzel [26], but unfortunately, they are not applicable in all of our situations. We state below, without proof, some well-known results that relate these particular Lucas sequences to values of certain cyclotomic polynomials. These facts are useful here to help establish the existence of a second primitive divisor. We let $\Phi_n(x)$ denote the nth cyclotomic polynomial, and U_n denote $U_n(\alpha, 1)$, where $\alpha \geq 2$ is an integer.

The following theorem is due to Legendre [24].

THEOREM 2.4. *Let q be a prime divisor of $\Phi_n(\alpha)$, and let $\mathrm{ord}_q(\alpha)$ denote the order of α modulo q. If $\mathrm{ord}_q(\alpha) < n$, then q divides n.*

Since

$$(\alpha - 1)U_n = \prod_{d|n} \Phi_d(\alpha),$$

the following corollary is immediate from Theorem 2.4.

COROLLARY 2.5.

(1) *A prime divisor q of U_n is a primitive divisor of U_n if and only if $\Phi_m(\alpha) \not\equiv 0 \pmod{q}$ for all proper divisors m of n.*
(2) *If q is a primitive divisor of U_n, then $\Phi_n(\alpha) \equiv 0 \pmod{q}$.*
(3) *If $\Phi_n(\alpha) \equiv 0 \pmod{q}$ and $n \not\equiv 0 \pmod{q}$, then q is a primitive divisor of U_n.*

The main result of this section is the following:

THEOREM 2.6. *Let $\alpha \geq 2$ be a rational integer. Then there exist infinitely many positive integers k such that*

$$k(U_n(\alpha, 1) + (\alpha - 1)^2) + 1$$

is composite for all integers $n \geq 1$.

Proof. Since $\alpha = 2$ corresponds to Sierpiński's original theorem, we assume that $\alpha \geq 3$. Note that, by Corollary 2.3, the only n-defective pairs that are of concern to us here are $(\alpha, \beta) = (2^c - 1, 1)$, which are 2-defective. So, the proof is broken into two main cases: $\alpha \neq 2^c - 1$ and $\alpha = 2^c - 1$.

A different covering $\{n \equiv r_i \pmod{m_i}\}$ is used in each of these cases. We use a covering with minimum modulus 3 in the case when $\alpha = 2^c - 1$, to circumvent the fact that these sequences are 2-defective. In both cases, we let p_i denote a primitive divisor of U_{m_i}. Then, when $n \equiv r_i \pmod{m_i}$, we have

$$U_n + (\alpha - 1)^2 \equiv U_{r_i} + (\alpha - 1)^2 \pmod{p_i}.$$

For brevity of notation, we define $A_i := U_{r_i} + (\alpha - 1)^2$. It is crucial for our arguments that A_i be invertible modulo p_i. In other words, we need $A_i \not\equiv 0 \pmod{p_i}$ for all i.

Assume first that $\alpha \neq 2^c - 1$, and use the covering

i	1	2	3	4	5
r_i	0	0	1	1	11
m_i	2	3	4	6	12

Next, we verify for each $i \neq 3$ that $A_i \not\equiv 0 \pmod{p_i}$. This is clear when $i = 1, 2$, since $A_i \equiv (\alpha - 1)^2 \not\equiv 0 \pmod{p_i}$.

For $i = 4$, we have $A_4 = \alpha^2 - 2\alpha + 2$. Since p_4 is a primitive divisor of U_6, Corollary 2.5(2) tells us that $\alpha^2 - \alpha + 1 \equiv 0 \pmod{p_4}$. If $A_4 \equiv 0 \pmod{p_4}$, then

$$0 \equiv \alpha^2 - \alpha + 1 - (\alpha^2 - 2\alpha + 2) \equiv \alpha - 1 \pmod{p_4},$$

which contradicts the fact that p_4 is primitive.

Now consider $i = 5$. Since p_5 is a primitive divisor of U_{12}, we see, by Corollary 2.5(2), that $\alpha^6 \equiv -1 \pmod{p_5}$. Using this fact, it is easy to show that

$$0 \equiv (-2\alpha^3 - \alpha^2 + 2\alpha)A_5 \equiv 5(\alpha - 1) \pmod{p_5}.$$

Hence, $p_5 = 5$, since $\alpha - 1 \not\equiv 0 \pmod{p_5}$. Thus,

$$\Phi_{12}(\alpha) = \alpha^4 - \alpha^2 + 1 \equiv 0 \pmod{5},$$

from Corollary 2.5(2). But then, since $\alpha \not\equiv 0 \pmod{p_5}$, we arrive at the contradiction that 2 is a square modulo 5.

Finally, to finish the proof when $\alpha \neq 2^c - 1$, we examine the case of $i = 3$. Suppose that $A_3 \equiv 0 \pmod{p_3}$. Since p_3 is a primitive divisor of U_4, we deduce from Corollary 2.5(2) that $\alpha^2 \equiv -1 \pmod{p_3}$. Then

$$0 \equiv A_3 = \alpha^2 - 2\alpha + 2 \equiv -2\alpha + 1 \pmod{p_3}.$$

Clearly, $p_3 \neq 2$, and so $\alpha \equiv 1/2 \pmod{p_3}$. Substituting this quantity back into $\alpha^2 \equiv -1 \pmod{p_3}$ implies that $p_3 = 5$, and therefore $\alpha \equiv 3 \pmod 5$. Unfortunately, no contradiction is achieved here. We use Corollary 2.5(3) to show in this situation that there is a second odd primitive divisor $q \neq 5$ of U_4. Then we can conclude that $A_3 \not\equiv 0 \pmod{q}$. We consider two cases: $\alpha \equiv 3 \pmod{10}$ and $\alpha \equiv 8 \pmod{10}$.

First suppose that $\alpha \equiv 3 \pmod{10}$. Then $\alpha^2 + 1 \equiv 2 \pmod 4$. Le [21] proved that there are at most two pairs (α, n) of natural numbers such that

$$\alpha^2 + 1 = 2 \cdot 5^n. \tag{2.1}$$

Thus, the pairs $(3, 1)$ and $(7, 2)$ are the only solutions to equation (2.1). The solution $(7, 2)$ is of no concern to us here, since $7 \not\equiv 3 \pmod{10}$. Hence, when $\alpha > 3$, there exists an odd prime $q \neq 5$ such that $\alpha^2 + 1 \equiv 0 \pmod q$. To show that q is indeed a primitive divisor of U_4, it is enough, by Corollary 2.5(1), to show that q does not divide either $\Phi_1(\alpha)$ or $\Phi_2(\alpha)$. But the only prime q that can divide either $\Phi_1(\alpha)$ or $\Phi_2(\alpha)$, and also divide $\alpha^2 + 1$, is $q = 2$. Recall that the case $\alpha = 3$ is not an issue here since we are assuming that $\alpha \neq 2^c - 1$.

Next, suppose that $\alpha \equiv 8 \pmod{10}$. Then $\alpha^2 + 1$ is odd, and we need to examine the equation

$$\alpha^2 + 1 = 5^n. \tag{2.2}$$

Lebesgue [22] proved that there exists at most one pair of natural numbers (α, n) that satisfies (2.2). Thus $(2, 1)$ is the only solution to (2.2), and as above, $\alpha^2 + 1$ has a second odd primitive divisor $q \neq 5$.

Then, choosing p_3 to be the appropriate primitive divisor of U_4 so that $A_3 \not\equiv 0 \pmod{p_3}$, we can apply the Chinese remainder theorem to the system of congruences $k \equiv -1/A_i \pmod{p_i}$, to complete the proof in this case.

Now we turn our attention to the case when $\alpha = 2^c - 1$. The Lucas pair $(2^c - 1, 1)$ is 2–defective, and so we cannot use the previous covering since $m_1 = 2$ there. To avoid the 2-defective situation, we use a covering with minimum modulus 3:

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14
r_i	0	0	1	5	6	3	10	4	11	2	7	35	25	55
m_i	3	4	5	6	8	10	12	15	20	24	30	40	60	120

It is easy to check that this is indeed a covering. First note that $\alpha - 1 = 2^c - 2 \equiv 0 \pmod 2$, so that 2 is not a primitive divisor of U_{m_i} for any i. To ensure that $A_i \not\equiv 0 \pmod{p_i}$, it is enough, by Corollary 2.5(2), to show that

$$\gcd(\Phi_{m_i}(\alpha), A_i) \not\equiv 0 \pmod{p_i}. \tag{2.3}$$

Tedious, but straightforward, arguments similar to the previous case show that (2.3) is satisfied for all i in this covering. Fortunately, no Diophantine equations must be considered here to show the existence of additional primitive divisors. Coverings with fewer congruences can be chosen with minimum modulus 3, but they all seem to incur the Diophantine considerations. Since the arguments in this case are similar to the previous case, we omit the details. ∎

REMARK 2.7. In the proof of Theorem 2.6 we showed that if $\alpha \equiv 3 \pmod 5$ and $\alpha \neq 2^c - 1$, then $U_4(\alpha, 1)$ has at least two distinct odd primitive divisors. This fact overlaps with a result of Schinzel [26] when α is twice a square.

3. Generalization II. In this section, we generalize Theorem 1.3 using an approach different from the one in Section 2. The main theorem here is:

THEOREM 3.1. *There are infinitely many Lucas pairs (α, β), not produced by Theorem* 2.6*, for which there exist infinitely many positive integers k such that*

$$k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$$

is composite for all integers $n \geq 1$.

The only rational Lucas pairs (α, β) that can be generated using the techniques in the proof of Theorem 3.1 are such that $\alpha - \beta = 1$, and thus the only conceivable overlap with Theorem 2.6 is the Lucas pair $(2, 1)$. Unfortunately, the algorithm, as described in the proof, does not directly capture this pair. However, a slight modification to the algorithm does the job (see Example 3.4), and so Theorem 3.1 can, in some sense, be viewed as a generalization of Theorem 1.3. Although primitive divisors were used successfully in the proof of Theorem 2.6, they are more difficult to harness when α and β are not rational. For this reason, we abandon the use of primitive divisors in the proof of Theorem 3.1, in favor of a strategy that is somewhat opposite in nature. In the primitive-divisor situation, the primes we use (the primitive divisors themselves) depend on the particular values of α and β, while in the new approach, we start with a set of primes, and then construct the values of α and β. Although these methods produce rational, irrational, and nonreal Lucas pairs, depending on the covering used, there is an inherent weakness in the algorithm. Even allowing modifications to the algorithm, it seems that, in general, there is no way of determining ahead of time whether a particular Lucas pair can be captured by this procedure. In fact, there seem to be certain Lucas pairs that cannot be produced by these techniques (see Section 4).

The proof of Theorem 3.1 is straightforward. Simply choose a particular covering, and use the algorithm to generate an explicit Lucas pair (α, β) that satisfies the conditions of the theorem. The algorithm is such that there are infinitely many choices from an arithmetic progression for values of a and b, where $\alpha = (a + \sqrt{b})/2$, so that the algorithm automatically produces infinitely many values of α and β. Then there are infinitely many values of k from an arithmetic progression that satisfy the conditions of the theorem for all values of α and β. In the proof of Theorem 3.1, we give a very specific version of the algorithm which can be used to generate irrational Lucas pairs. However, slight modifications will produce rational or nonreal Lucas

pairs. We indicate these versions after the proof, and we provide examples in Section 3.1.

Proof of Theorem 3.1. We describe a version of the algorithm that will generate a Lucas pair; then we justify the steps; and finally, we use the algorithm with a particular covering to illustrate the process. Let $\{n \equiv r_i \pmod{m_i}\}$ be a covering with distinct moduli m_i, such that $p_i := m_i + 1$ is prime for all i. For each i, we choose integers a_i and b_i according to the following prescription:

(3.1)
1. If $r_i = 1$ or $r_i \equiv 0 \pmod 2$, then let $a_i = 0$ and $b_i = 1$.
2. If $r_i = 3$, then let $a_i = 0$ and $b_i = 1$,
   unless $p_i = 5$, in which case let $a_i = 1$ and $b_i = 1$.
3. If $r_i \geq 5$ and $r_i \equiv 1 \pmod 2$, then let $a_i = 0$ and $b_i = 4$.

Then, use the Chinese remainder theorem to solve the two systems of congruences

$$\text{(3.2)} \qquad \begin{cases} x \equiv a_i \pmod{p_i}, \\ x \equiv 1 \pmod 2, \end{cases} \qquad \begin{cases} y \equiv b_i \pmod{p_i}, \\ y \equiv 1 \pmod 4. \end{cases}$$

Let a and b be respective solutions to the systems in (3.2), and let $\alpha = (a + \sqrt{b})/2$ and $\beta = (a - \sqrt{b})/2$. At this juncture, we must verify that (α, β) is a legitimate Lucas pair. Clearly, $\alpha + \beta = a \in \mathbb{Z}$. Observe that $\alpha\beta = (a^2 - b)/4$. Since $a \equiv 1 \pmod 2$ and $b \equiv 1 \pmod 4$, we see that $\alpha\beta \in \mathbb{Z}$. Next, since $\gcd(\alpha + \beta, \alpha\beta) = 1$ if and only if $\gcd(a, b) = 1$, we need to be able to select solutions a and b of (3.2) that are relatively prime. To accomplish this task, first solve for a in the first system of (3.2), and then add additional congruences, if necessary, to the second system in (3.2) to guarantee that $\gcd(a, b) = 1$. Then we must check that α/β is not a root of unity. Finally, use the Chinese remainder theorem to solve the system of congruences $k \equiv -1/A_i \pmod{p_i}$, where

$$A_i := \frac{\alpha^{r_i} - \beta^{r_i}}{\alpha - \beta} + (\alpha - \beta)^2.$$

Then we claim that $k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$ is composite for all $n \geq 1$. In fact, we have

$$\text{(3.3)} \qquad k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1 \equiv 0 \pmod{p_i}, \text{ when } n \equiv r_i \pmod{m_i}.$$

To prove that (3.3) is true, we verify the validity of the steps of the algorithm, and show that $A_i \not\equiv 0 \pmod{p_i}$ for all i. First note that the conditions in (3.1) guarantee that $b_i \not\equiv 0 \pmod{p_i}$ for all i. Consequently, $b \not\equiv 0 \pmod{p_i}$ and $\alpha - \beta \not\equiv 0 \pmod{p_i}$ for all i. For each i, let $\alpha_i = (a_i + \sqrt{b_i})/2$, $\beta_i = (a_i - \sqrt{b_i})/2$, and

$$\bar{A}_i := \frac{\alpha_i^{r_i} - \beta_i^{r_i}}{\alpha_i - \beta_i} + (\alpha_i - \beta_i)^2 = \frac{\alpha_i^{r_i} - \beta_i^{r_i}}{\alpha_i - \beta_i} + b_i.$$

Since b_i is a square modulo p_i, and $m_i = p_i - 1$ for all i, it follows from Fermat's little theorem (even if $\alpha \equiv 0 \pmod{p_i}$ or $\beta \equiv 0 \pmod{p_i}$, which could happen if $n \equiv 3 \pmod 4$ is a congruence in the covering) that

$$U_n(\alpha, \beta) + (\alpha - \beta)^2 \equiv A_i \equiv \bar{A}_i \pmod{p_i},$$

when $n \equiv r_i \pmod{m_i}$. First assume that $a_i = 0$. Then straightforward calculations give

$$\bar{A}_i = \frac{\left(\sqrt{b_i}\right)^{r_i-1}(1-(-1)^{r_i})}{2^{r_i}} + b_i = \begin{cases} b_i & \text{if } r_i \equiv 0 \pmod 2, \\ \dfrac{(\sqrt{b_i})^{r_i-1}}{2^{r_i-1}} + b_i & \text{if } r_i \equiv 1 \pmod 2. \end{cases} \tag{3.4}$$

We refer to the menu (3.1). It is clear that $\bar{A}_i \not\equiv 0 \pmod{p_i}$ in (3.4) when $r_i \equiv 0 \pmod 2$, since $b_i = 1$. When $r_i \equiv 1 \pmod 2$, there are three cases to consider. If $r_i = 1$, then $b_i = 1$, and so $\bar{A}_i = 2 \not\equiv 0 \pmod{p_i}$. If $r_i = 3$, then $b_i = 1$ and $\bar{A}_i = 5/4 \not\equiv 0 \pmod{p_i}$, since $p_i \neq 5$. Next, if $r_i \geq 5$, then $p_i \geq 7$. Then, since $b_i = 4$ from (3.1), we have $\bar{A}_i = 5 \not\equiv 0 \pmod{p_i}$.

Now assume that $a_i = 1$. Then $r_i = 3$, $p_i = 5$, and $b_i = 1$ from (3.1). In this case, either $\alpha = 0$ and $\beta = 1$, or $\alpha = 1$ and $\beta = 0$. In either situation, we have $\bar{A}_i = 1 \not\equiv 0 \pmod 5$.

We finish the proof with an example. Consider the covering

i	1	2	3	4	5	6	7	8	9	10	11	12	13
r_i	0	1	5	7	3	7	1	19	55	31	139	13	103
m_i	2	4	6	10	12	18	30	36	60	108	180	270	540

Applying the algorithm to this situation gives

$$\alpha = \frac{57735618045574774305 + \sqrt{41575375575250122841}}{2},$$
$$k = 37170467875892126822,$$

The first three terms of the sequence $k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$, in factored form, with p_i in bold, are given in Table 1.

Table 1. Factored terms of $k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$

n	$k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$
1	$\mathbf{5}^4 \cdot 7 \cdot 11 \cdot 19 \cdot 31 \cdot 37 \cdot 61 \cdot 109 \cdot 181 \cdot 271 \cdot 541$ $\cdot 22409 \cdot 372668347052399$
2	$\mathbf{3} \cdot 24691 \cdot 4983510993352233298899978363 5863781$
3	$7 \cdot 11 \cdot \mathbf{13} \cdot 19 \cdot 37 \cdot 61 \cdot 109 \cdot 181 \cdot 271 \cdot 541 \cdot 2127299$ $\cdot 2258992037077 \cdot 155744538873346913742671$

■

In general, the algorithm given in the proof of Theorem 3.1 will produce an irrational Lucas pair. However, if all residues in the covering are even, or if the only odd residues that appear in the covering are $r_i = 1$, then $b_i = 1$ for all i, and we can take $b = 1$. The algorithm generates a rational Lucas pair in this situation (see Example 3.2). Also, it is easy to see that there is room for modification of the algorithm. For example, we chose $a_i = 0$, for most values of i, since it is easier to prove that A_i is invertible modulo p_i in that situation. But to produce the Lucas pair $(2, 1)$, we can choose all $a_i = 3$ and all $b_i = 1$, with an appropriate covering (see Example 3.4). To generate a nonreal Lucas pair, we can let b be a negative value in the arithmetic progression produced by solving the second system in (3.2) (see Example 3.3). Other modifications to the algorithm are possible, depending on the covering chosen, but these modifications could result in a more complicated set of conditions for $\bar{A}_i$ to be invertible modulo p_i.

3.1. Additional examples. This section contains some more examples illustrating the algorithm used in the proof of Theorem 3.1, and some modified versions of it. To keep the numbers reasonably small, we have chosen coverings in which the maximum modulus is 180 and the greatest common divisor of the moduli is 360.

Example 3.2. This example shows how the algorithm in Theorem 3.1 can be used to produce a rational Lucas pair. We use the covering

i	1	2	3	4	5	6	7	8	9	10	11	12
r_i	1	0	0	0	10	8	2	2	14	38	50	86
m_i	2	4	6	10	12	18	30	36	40	60	72	180

Observe that the only odd residue is $r_1 = 1$. Applying the algorithm gives

$$\alpha = 5406640414743068, \quad \beta = 5406640414743067,$$
$$k = 3604426943162044.$$

The first three terms of the sequence $k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$, in factored form, with p_i in bold, are given in Table 2.

Table 2. Factored terms of $k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$

n	$k(U_n(\alpha, \beta) + (\alpha - \beta)^2) + 1$
1	$\mathbf{3}^2 \cdot 1708529 \cdot 468814849$
2	$5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot \mathbf{31} \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 181 \cdot 2179 \cdot 62143 \cdot 4697417$
3	$\mathbf{3} \cdot 8707 \cdot 15328919 \cdot 83120546683 \cdot 94973563958527677862666 93$

Example 3.3. This example shows how to produce a nonreal Lucas pair. We start with the covering

i	1	2	3	4	5	6	7	8	9	10	11	12
r_i	0	3	1	3	9	11	17	5	1	5	53	89
m_i	2	4	6	10	12	18	30	36	40	60	72	180

We take the smallest positive value of b produced by the algorithm and subtract the least common multiple of the moduli in the second system in (3.2) to get the negative value of $b = -10777658998435559$. Then

$$\alpha = \frac{6487968497691681 + \sqrt{-10777658998435559}}{2},$$
$$k = 1314262889709437.$$

The first three terms of the sequence $k(U_n(\alpha,\beta) + (\alpha-\beta)^2) + 1$, in factored form, with p_i in bold, are given in Table 3.

Table 3. Factored terms of $k(U_n(\alpha,\beta) + (\alpha-\beta)^2) + 1$

n	$k(U_n(\alpha,\beta) + (\alpha-\beta)^2) + 1$
1	$-5 \cdot \mathbf{7} \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 41 \cdot 61 \cdot 73 \cdot 181 \cdot 499 \cdot 51131 \cdot 1694253179$
2	$-\mathbf{3} \cdot 5 \cdot 557 \cdot 3319249 \cdot 203297622608681319 03$
3	$\mathbf{5} \cdot 11 \cdot 13 \cdot 19 \cdot 31 \cdot 37 \cdot 61 \cdot 73 \cdot 181 \cdot 50257221163$ $\cdot 65736741235555550052593$

Example 3.4. This example shows how the algorithm in Theorem 3.1 can be modified to capture the Lucas pair $(\alpha,\beta) = (2,1)$ and give an alternative proof of Theorem 1.3. We start with the covering

i	1	2	3	4	5	6	7	8	9	10	11	12
r_i	0	1	1	5	11	15	9	3	23	51	27	27
m_i	2	4	6	10	12	18	30	36	40	60	72	180

We modify the algorithm by choosing $a_i = 3$ and $b_i = 1$ for all i, and in addition, we replace the congruence $x \equiv 1 \pmod 2$ in (3.2) with the congruence $x \equiv 3 \pmod 4$. The algorithm then produces $\alpha = 2$, $\beta = 1$, and $k = 9579495527398457$. The first three terms of the sequence $k(U_n(\alpha,\beta) + (\alpha-\beta)^2) + 1$, in factored form, with p_i in bold, are given in Table 4.

Table 4. Factored terms of $k(U_n(\alpha,\beta) + (\alpha-\beta)^2) + 1$

n	$k(U_n(\alpha,\beta) + (\alpha-\beta)^2) + 1$
1	$\mathbf{5} \cdot 7^2 \cdot 43 \cdot 1459 \cdot 607147 \cdot 2053$
2	$\mathbf{3} \cdot 907 \cdot 14082316100549$
3	$\mathbf{37} \cdot 41 \cdot 1399 \cdot 36110153179$

REMARK 3.5. The Sierpiński number k produced by the procedure in Example 3.4 is considerably smaller than the smallest Sierpiński number generated in Sierpiński's original proof.

4. Another approach. The algorithm used to prove Theorem 3.1 (and any modification) appears to be too restrictive to produce certain Lucas pairs. For example, it seems unlikely that the famous Lucas pair $((1+\sqrt{5})/2, (1-\sqrt{5})/2)$, which generates the Fibonacci sequence $\{F_n\}$, can be captured using this algorithm. One reason for this is that Fermat's little theorem does not apply if 5 is not a square modulo $p_i = m_i + 1$. However, constructing a covering by replacing such "bad" moduli with distinct moduli m_i, such that $m_i + 1$ is prime, and for which 5 is a square modulo $m_i + 1$, is most certainly a difficult task at best, and perhaps even impossible. We have been unsuccessful in our attempts to construct such a covering.

The approach used in this section is quite different from the methods used in the previous sections. Instead of directly using primitive divisors, or a covering where each modulus is one less than a prime, we exploit the well-known fact that Lucas sequences U_n are periodic modulo any prime [12]. The idea is to construct a covering where each modulus is a period of U_n modulo some prime. If U_n has period m modulo the prime p, then $U_m \equiv 0 \pmod{p}$, but p might or might not be a primitive divisor of U_m. However, there is always a least positive integer $a(p)$, called the *restricted period* [12] of U_n modulo p, such that p is a primitive divisor of $U_{a(p)}$. So, we are using primitive divisors in some sense, but certainly not in the traditional way. Just as U_n may have more than one primitive divisor, U_n can have the same period modulo more than one prime. Thus, our covering can have repeated moduli, and we make use of this phenomenon to establish Theorem 4.1.

However, constructing the covering is still somewhat tricky, since, depending on the particular sequence U_n, there can be many positive integers m for which there is no prime p such that U_n has period m modulo p. For example, the only odd period for $\{F_n\}$ is $m = 3$. Although we are unable to determine, in general, when this process will be successful, we illustrate that the method does work in certain situations by establishing that the procedure is successful in the case of the Fibonacci sequence $\{F_n\}$. Helpful in the construction of the covering here is the fact, which follows from a result of Lengyel [23], that given any even number $m \notin \{2, 4, 6, 12, 24\}$, there exists at least one prime p such that the period of $\{F_n\}$ modulo p is m. The main result of this section is:

THEOREM 4.1. *Let $\{F_n\}$ denote the Fibonacci sequence, defined recursively by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Then there exist infinitely many positive integers k such that the sequence $k(F_n + 5) + 1$ is composite for all integers $n \geq 1$.*

Proof. We use a slightly different format to present the covering $\mathcal{C}$ here. The 133 elements of $\mathcal{C}$ are indicated by ordered triples (r_i, m_i, p_i), where the congruence in the covering corresponding to this ordered triple is $n \equiv r_i \pmod{m_i}$. The prime p_i in the ordered triple is the prime such that $\{F_n\}$ modulo p_i has period m_i. Then, for each congruence $n \equiv r_i \pmod{m_i}$ in the covering, we have $F_n \equiv F_{r_i} \pmod{p_i}$. We must then check that $F_{r_i} + 5 \not\equiv 0 \pmod{p_i}$. Finally, we use the Chinese remainder theorem to solve for k the system of 133 congruences $k \equiv -1/(F_{r_i} + 5) \pmod{p_i}$. The covering we use here is

$$\begin{aligned}\mathcal{C} = \{ &(0,3,2), (0,8,3), (1,10,11), (6,14,29), (6,16,7), (5,18,19), (3,20,5), (2,28,13),\\ &(19,30,31), (12,32,47), (29,36,17), (27,40,41), (22,42,211), (20,48,23), (5,50,101),\\ &(45,50,151), (35,54,5779), (18,56,281), (37,60,61), (0,70,71), (12,70,911),\\ &(47,72,107), (14,80,2161), (10,84,421), (89,90,181), (85,90,541), (92,96,1103),\\ &(13,100,3001), (53,108,53), (17,108,109), (42,112,14503), (7,120,2521),\\ &(40,126,1009), (124,126,31249), (42,140,141961), (100,144,103681),\\ &(85,150,12301), (115,150,18451), (78,160,1601), (46,160,3041), (50,162,3079),\\ &(140,162,62650261), (122,168,83), (50,168,1427), (73,180,109441), (75,200,401),\\ &(175,200,570601), (110,210,21211), (196,210,767131), (4,216,11128427),\\ &(158,224,10745088481), (193,240,241), (133,240,20641), (82,252,35239681),\\ &(29,270,271), (17,270,811), (119,270,42391), (209,270,119611),\\ &(154,280,12317523121), (28,288,10749957121), (25,300,230686501),\\ &(124,324,2269), (232,324,4373), (148,324,19441), (26,336,167),\\ &(206,336,65740583), (98,350,54601), (168,350,560701), (28,350,7517651),\\ &(238,350,51636551), (133,360,10783342081), (88,378,379), (130,378,85429),\\ &(214,378,912871), (52,378,1258740001), (393,400,9125201), (153,400,5738108801),\\ &(278,420,8288823481), (292,432,6263), (196,432,177962167367), (215,450,221401),\\ &(35,450,15608701), (335,450,3467131047901), (446,480,23735900452321),\\ &(268,504,1461601), (436,504,764940961), (107,540,1114769954367361),\\ &(306,560,118021448662479038881), (73,600,601), (433,600,87129547172401),\\ &(92,630,631), (476,630,1051224514831), (260,630,1983000765501001),\\ &(340,648,1828620361), (364,648,6782976947987), (638,672,115613939510481515041),\\ &(658,700,701), (474,700,17231203730201189308301), (13,720,8641),\\ &(515,720,13373763765986881), (700,756,38933), (472,756,955921950316735037),\\ &(715,800,124001), (315,800,6996001), (782,800,3160438834174817356001),\\ &(742,810,1621), (94,810,4861), (580,810,21871), (418,810,33211),\\ &(256,810,31603395781), (34,810,7654861102843433881), (194,840,721561),\\ &(266,840,140207234004601), (508,864,3023), (412,864,19009), (14,864,447901921),\\ &(686,864,48265838239823), (242,900,11981661982050957053616001), (46,1008,503),\\ &(494,1008,4322424761927), (830,1008,571385160581761), (302,1050,1051),\\ &(722,1050,9346455940780547345401), (512,1050,14734291702642871390242051),\end{aligned}$$

$(590, 1080, 12315241), (950, 1080, 100873547420073756574681), (942, 1120, 6135922241),$
$(270, 1120, 164154312001), (750, 1120, 13264519466034652481), (428, 1134, 89511254659),$
$(680, 1134, 1643223059479), (806, 1134, 68853479653802041437170359),$
$(1058, 1134, 5087394106095783259)\}$.

The smallest positive value of k found using the Chinese remainder theorem has 949 digits.

We do not give the first three terms of the sequence $k(F_n + 5) + 1$ in factored form since they are too large. ∎

REMARK 4.2. As far as the author knows, the covering $\mathcal{C}$ used in the proof of Theorem 4.1 is the first covering to appear in the literature such that each modulus is a period of the Fibonacci sequence modulo a prime. The covering $\mathcal{C}$ has been used recently to prove that there are infinitely many positive integers that cannot be written in either of the forms $F_n + p$ or $F_n - p$, where F_n is a Fibonacci number, and p is a prime [18].

5. A nonlinear variation. Given a nonlinear polynomial $f(k)$, we can ask whether there exist infinitely many positive integers k such that $f(k) \cdot 2^n + 1$ is composite for all integers $n \geq 1$. With $f(k) = k^r$, Chen [8] proved that the answer is affirmative for $r \not\equiv 0, 4, 6, 8 \pmod{12}$. Using a different approach, Filaseta, Finch and Kozek [14] have been able to lift Chen's restriction on r. More recently, Finch, Harrington and the author (in an unpublished manuscript) have established a similar result with $f(k) = k^r + 1$, when r is not divisible by 8 or 17449. We should point out that Chen, and Filaseta, Finch and Kozek also addressed other concerns in their respective papers. For example, these authors actually showed that each composite term in the sequence has at least two distinct prime divisors.

We end this paper with a nonlinear variation using Lucas sequences.

THEOREM 5.1. *Let $m = \prod_{i=1}^{11} p_i$, where the p_i are given in Table 5. Let $\alpha \equiv 5 \pmod{m}$ be a positive integer. Then there exist infinitely many positive integers k such that*

$$k^2(U_n(\alpha, 1) + (\alpha - 1)^2) + 1$$

is composite for all integers $n \geq 1$.

Table 5. The covering with the primitive divisors p_i of U_{m_i}

i	1	2	3	4	5	6	7	8	9	10	11
r_i	1	1	0	1	2	6	0	12	14	18	0
m_i	2	3	4	6	8	9	12	18	24	36	72
p_i	3	31	13	7	313	19	601	5167	390001	37	73

Proof. The covering $\{n \equiv r_i \pmod{m_i}\}$ we use here is given in Table 5. The prime p_i is a primitive divisor of U_{m_i}. For each i, let $A_i = U_{r_i} + (\alpha - 1)^2$,

so that $U_n + (\alpha - 1)^2 \equiv A_i \pmod{p_i}$ when $n \equiv r_i \pmod{m_i}$. It is then easy to verify that $A_i \not\equiv 0 \pmod{p_i}$, and that $-1/A_i$ is a square modulo p_i for all i. We solve each of the congruences $k^2 \equiv -1/A_i \pmod{p_i}$, and choose a solution s_i. This gives a system of congruences $k \equiv s_i \pmod{p_i}$, and we can apply the Chinese remainder theorem to this system to find infinitely many values of k. The smallest positive value of k produced by this process is $k = 117050073288612071969896$. The first three terms of the sequence $k^2(U_n(5,1)+16)+1$, in factored form, with p_i in bold, are given in Table 6.

Table 6. Factored terms of $k^2(U_n(5,1) + 16) + 1$

n	$k^2(U_n(5,1) + 16) + 1$
1	$\mathbf{3} \cdot 7 \cdot 23 \cdot 31 \cdot 53 \cdot 199 \cdot 431 \cdot 3132881 \cdot 3384559190303 \cdot 322723988351788951$
2	$\mathbf{313} \cdot 571 \cdot 853 \cdot 1459 \cdot 5931337 \cdot 336267671 \cdot 18194404469 \cdot 37342701311$
3	$\mathbf{3}^3 \cdot 17 \cdot 377843803411203610837 \cdot 37129256102600967621319 91$

■

REMARK 5.2. The computer calculations and verifications needed in this paper were done using either MAGMA or Maple.

Acknowledgements. The author thanks the referee for the valuable comments.

References

[1] A. S. Bang, *Taltheoretiske Undersøgelser*, Tidsskr. Mat. 5 IV (1886), 70–80, 130–137.
[2] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers* (with an appendix by M. Mignotte), J. Reine Angew. Math. 539 (2001), 75–122.
[3] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* $a^n - b^n$, Ann. of Math. (2) 5 (1904), 173–180.
[4] P. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n \pm \beta^n$, ibid. 15 (1913/14), 30–70.
[5] Y. G. Chen, *On integers of the form* $2^n \pm p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, Proc. Amer. Math. Soc. 128 (2000), 1613–1616.
[6] —, *On integers of the form* $k2^n + 1$, ibid. 129 (2001), 355–361.
[7] —, *On integers of the forms* $k - 2^n$ *and* $k2^n + 1$, J. Number Theory 89 (2001), 121–125.
[8] —, *On integers of the forms* $k^r - 2^n$ *and* $k^r 2^n + 1$, ibid. 98 (2003), 310–319.
[9] —, *On integers of the forms* $k \pm 2^n$ *and* $k2^n \pm 1$, ibid. 125 (2007), 14–25.
[10] Y. G. Chen, R. Feng and N. Templier, *Fermat numbers and integers of the form* $a^k + a^l + p^\alpha$, Acta Arith. 135 (2008), 51–61.
[11] P. Erdős, *On integers of the form* $2^k + p$ *and some related problems*, Summa Brasil. Math. 2 (1950), 113–123.

[12] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, Math. Surveys Monogr. 104, Amer. Math. Soc., 2003.
[13] M. Filaseta, *Coverings of the integers associated with an irreducibility theorem of A. Schinzel*, in: Number Theory for the Millennium, II, A. K. Peters, 2002, 1–24.
[14] M. Filaseta, C. Finch and M. Kozek, *On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture*, J. Number Theory 128 (2008), 1916–1940.
[15] M. Filaseta, K. Ford and S. Konyagin, *On an irreducibility theorem of A. Schinzel associated with coverings of the integers*, Illinois J. Math. 44 (2000), 633–643.
[16] M. Filaseta and M. Matthews Jr., *On the irreducibility of* $0,1$*-polynomials of the form* $f(x)x^n + g(x)$, Colloq. Math. 99 (2004), 1–5.
[17] A. S. Izotov, *A note on Sierpiński numbers*, Fibonacci Quart. 33 (1995), 206–207.
[18] L. Jones, *Fibonacci variations of a conjecture of Polignac*, Integers 12 (2012), A11.
[19] —, *Polynomial variations on a theme of Sierpiński*, Int. J. Number Theory 5 (2009), 999–1015.
[20] —, *Variations on a theme of Sierpiński*, J. Integer Seq. 10 (2007), article 07.4.4, 15 pp.
[21] M.-H. Le, *On the diophantine equation* $(x^3-1)/(x-1) = (y^n-1)/(y-1)$, Trans. Amer. Math. Soc. 351 (1999), 1063–1074.
[22] V.-A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math. 1 (1850), 178–181.
[23] T. Lengyel, *The order of the Fibonacci and Lucas numbers*, Fibonacci Quart. 33 (1995), 234–239.
[24] P. Ribenboim, *The New Book of Prime Number Records*, Springer, 1996.
[25] H. Riesel, *Några stora primtal*, Elementa 39 (1956), 258–260.
[26] A. Schinzel, *On primitive prime factors of* $a^n - b^n$, Proc. Cambridge Philos. Soc. 58 (1962), 555–562.
[27] —, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), 27–33.
[28] W. Sierpiński, *Sur un problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math. 15 (1960), 73–74.
[29] C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, in: Transcendence Theory: Advances and Applications (Cambridge, 1976), Academic Press, 1977, 79–92.
[30] P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. 64 (1995), 869–888.
[31] K. J. Wu and Z. W. Sun, *Covers of the integers with odd moduli and their applications to the forms* $x^m - 2^n$ *and* $x^2 - F_{3n}/2$, ibid. 78 (2009), 1853–1866.
[32] S. M. Yang and Z. W. Sun, *Covers with less than 10 moduli and their applications*, J. Southeast Univ. (English Ed.) 14 (1998), 106–114.
[33] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. 3 (1892), 265–284.

Lenny Jones
Department of Mathematics
Shippensburg University
Shippensburg, PA 17257, U.S.A.
E-mail: lkjone@ship.edu

Received on 10.6.2011
and in revised form on 19.8.2011 (6725)