Cullen Numbers in Binary Recurrent Sequences

Florian Luca [1] *and* *Pantelimon Stănică* [2] *

[1] IMATE-UNAM, Ap. Postal 61-3 (Xangari), CP 58 089
Morelia, Michoacán, Mexico; e-mail: fluca@matmor.unam.mx
[2] Auburn University Montgomery, Department of Mathematics,
Montgomery, AL 36124-4023, USA; e-mail: stanica@sciences.aum.edu

February 24, 2003

Abstract

In this paper, we prove that the generalized Cullen numbers, $C_n(s,l) := s_n \cdot 2^n + l$, where l is an integer and $s := (s_n)_{n\geq 0}$ is a sequence of integers satisfying $\log |s_n| < 2^{n-1} + O(1)$, occur only finitely many times in binary recurrent sequences $(u_n)_{n\geq 0}$ whose characteristic roots are quadratic units and that satisfy some additional conditions. We also generalize this result in some sense to show that if we take any finite set of prime numbers $\mathcal{P}$ and any integer l, and we write $u_n - l = PQ$, where P is a product of powers of the primes from $\mathcal{P}$, and Q is free of primes from $\mathcal{P}$, then there exist two computable constants c_1 and c_2 depending only on the sequence $(u_n)_{n\geq 0}$, the number l, and the given set of primes $\mathcal{P}$, such that for $n > c_1$ we have $\log |Q| > |P|^{c_2}$. Finally, we find *all* Cullen numbers, i.e., numbers of the form $n\cdot 2^n + 1$ and all Woodall numbers, i.e., the numbers of the form $n \cdot 2^n - 1$, that are either Fibonacci or Pell numbers.

*Also Associated to the Institute of Mathematics of Romanian Academy, Bucharest, Romania

1 Introduction

Mentioned in the excellent book of R. Guy [5], the *Cullen numbers* are elements of the sequence $C_n := n \cdot 2^n + 1$ (see Section **B20** of [5]). They happen to be composite (see [2] and [8]) for all $1 \leq n < 412000$, except for $n = 1$, 141, 4713, 5795, 6611, 18496, 32292, 32469, 59656, 90825, 262419, 361275. John Conway (cited in [5]) observes that the Cullen number C_n is divisible by $p = 2n - 1$ if p is a prime of the form $8k \pm 3$. Hooley [6] showed that almost all Cullen numbers are composite. In spite of the fact that the primes in this sequence are rare, it is still believed that there are infinitely many Cullen primes. Related to these are the *Woodall numbers* (or *Cullen numbers of the second kind*) given by $W_n := n \cdot 2^n - 1$. The number W_n is prime for $n = 2$, 3, 6, 30, 75, 81, 115, 123, 249, 362, 384, 462, 512, 751, 822, 5312, 7755, 9531, 12379, 15822, 18885, 22971, 23005, 98726, 143018, 151023 and for no other n with $n < 416000$ (see [1] for details). We also mention that in [9] it is shown that $\log \gcd(C_n, C_m) \ll \sqrt{m \log m}$ holds for all $m > n > 0$ and a similar result holds for the Woodall numbers. Here, and elsewhere throughout this paper, we use the Vinogradov symbols $\gg$ and $\ll$, as well as the Landau symbols O and o with their usual meanings, and for a real number $x \geq 1$ we use $\log x$ for the natural logarithm of x.

2 The Results

We fix a nonzero integer l and a sequence of integers $s := (s_n)_{n \geq 0}$. We define the (s, l)-*Cullen numbers* as

$$C_n(s, l) := s_n \cdot 2^n + l \qquad \text{for all } n \geq 0.$$

Notice that when $s_n := n$ for all n, then the $(s, 1)$-Cullen numbers are simply the regular Cullen numbers, while the $(s, -1)$-Cullen numbers are simply the regular Woodall numbers. Throughout this paper, we let $(u_n)_{n\geq 0}$ be a nondegenerate binary recurrent sequence of integers. That is, $(u_n)_{n\geq 0}$ is a sequence of integers such that there exist two integers a and b such that the recurrence formula

$$u_{n+2} = au_{n+1} + bu_n \qquad \text{holds for all } n \geq 0.$$

We also assume that $\Delta := a^2 + 4b > 0$. It is then well known that there exist two constants A and B so that the formula $u_k = A\alpha^k - B\beta^k$ holds for all $k \geq 0$, where α and β are the roots of the *characteristic equation* $x^2 - ax - b = 0$. This formula is sometimes referred to as *Binet's formula*. Notice that since $\Delta > 0$, it follows that α and β are real. The sequence $(u_n)_{n\geq 0}$ is called *nondegenerate* if $AB\alpha\beta \neq 0$ and $\alpha \neq -\beta$. We shall also assume that $a > 0$. Notice that this is not a real obstruction, for if $a < 0$, then we may replace the sequence $(u_n)_{n\geq 0}$ by the sequence $((-1)^n u_n)_{n\geq 0}$ which has the same arithmetic properties as our initial sequence $(u_n)_{n\geq 0}$, and which satisfies the same recurrence relation as $(u_n)_{n\geq 0}$ does with a replaced by $-a$. The case $a = 0$ is not allowed because this leads to $\alpha = -\beta$. We shall also adopt the convention that α is the largest root of the characteristic equation. Notice that $\alpha > \max\{|\beta|, 1\}$. Specifically, $\alpha = \frac{1}{2}(a + \sqrt{a^2 + 4b})$, $\beta = \frac{1}{2}(a - \sqrt{a^2 + 4b})$, and the values of A and B are given by $A = \dfrac{u_1 - u_0\beta}{\alpha - \beta}$, $B = \dfrac{u_1 - u_0\alpha}{\alpha - \beta}$. The binary recurrent sequence $(v_n)_{n\geq 0}$ whose starting values are $v_0 := 0$ and $v_1 := 1$ is called *the Lucas sequence* with parameters a and b. We reserve the notation $(v_n)_{n\geq 0}$ for the Lucas sequence. When $a = b = 1$, the Lucas sequence is precisely the *Fibonacci sequence* $(F_n)_{n\geq 0}$, while when $a = 2$ and $b = 1$, the Lucas sequence is precisely the *Pell sequence* $(P_n)_{n\geq 0}$. Some of our

results address also *almost Lucas sequences*, i.e., binary recurrent sequences $(u_n)_{n\geq 0}$ for which $u_0 := 0$ and $u_1 \geq 1$. Notice that in this case the formula $u_n = u_1 v_n$ holds for all $n \geq 0$, and the numbers A and B satisfy $A = B = \dfrac{u_1}{\alpha - \beta}$.

In the present paper, we investigate the occurrence of (s, l)-Cullen numbers in such binary recurrent sequences. As applications, we find all regular Cullen and Woodall numbers that are also either Fibonacci or Pell numbers. We also give a slightly more general result pertaining to the arithmetic structure of binary recurrent sequences having $b := \pm 1$.

Theorem 1. *Let $(v_n)_{n\geq 0}$ be a Lucas sequence for which $a > 0$ is odd and $b \equiv 1 \pmod{16}$. Assume also, that $(s_n)_{n\geq 0}$ is a sequence of positive integers satisfying $s_n = O(\alpha^{2^{n-1}})$, and assume that N is a nonnegative integer such that $v_N \equiv 3 \pmod 4$ or $v_N \equiv 0 \pmod 8$. Then, there exists an effectively computable constant $c_1 := c_1(\alpha, s, N)$, depending only on α, s and N, such that all positive integer solutions of the diophantine equation $C_n(s, v_N) = v_k$ satisfy $\max\{n, k\} < c_1$.*

The proof of our Theorem 1 is entirely elementary. Notice that the sequence $(s_n)_{n\geq 0}$ itself is not that important, rather what matters about it is that it does not grow too fast, that is, that it satisfies $\log s_n \leq 2^{n-1} \log \alpha + O(1)$. So, the above theorem can be reformulated by saying that if N is a fixed positive integer and if m is a large positive integer such that $2^n \mid v_m - v_N$, then $\log \dfrac{v_m - v_N}{2^n} - 2^{n-1} \log \alpha \gg 1$. In fact, it will be plain from our argument that the result continues to hold in a somewhat larger range for s, namely when s satisfies $\log s_n < c \cdot 2^{n-1} + O(1)$ with any constant c strictly smaller than $\dfrac{3}{2} \cdot \log \alpha \geq \dfrac{3}{2} \log\Big(\dfrac{1+\sqrt{5}}{2}\Big) \approx 1.12573$. Here, we used the well-known fact that $\alpha \geq \dfrac{1+\sqrt{5}}{2}$. In particular, c can be chosen to be $c := 1$, and under this form we obtain the result

announced in the abstract, i.e., without a dependence on α in the upper bound for $\log s_n$. By nonelementary methods, we prove the following theorem.

Theorem 2. *Let $(u_n)_{n\geq 0}$ by any nondegenerate binary recurrent sequence of integers with $b := \pm 1$. Let l be any integer and $p_1 < \cdots < p_t$ be any fixed prime numbers. For any positive integer m write*

$$u_m - l = PQ,$$

where P is the largest divisor of $u_m - l$ composed only from the primes $p_1, \ldots, p_t$ and Q is coprime to $p_1 \cdot \cdots \cdot p_t$. Then there exist two computable constants c_1 and c_2 depending only on the sequence $(u_n)_{n\geq 0}$, the number l, and on the prime numbers $p_1, \ldots, p_t$, such that for $m > c_1$ we have $\log |Q| > |P|^{c_2}$.

The proof of Theorem 2 uses the theory of lower bounds for linear forms in logarithms of algebraic numbers, and a very good introduction to this topic is [11]. Since such lower bounds usually involve some astronomical constants, the constant c_1 turns out to be very large, while the constant c_2 turns out to be very small. In a certain sense, Theorem 2 is an extension of Theorem 1 when $b := \pm 1$. Indeed, when $b := \pm 1$, take $t := 1$ and $p_1 := 2$ in the statement of Theorem 2. The conclusion of Theorem 2 asserts that if l is any fixed integer (like $l := u_N$ for some fixed N, for example), then there exists a computable constant c_2 which depends only on the sequence $(u_n)_{n\geq 0}$ and the number l, such that the diophantine equation of the form $u_m = s2^n + l$ with m and n positive integers and s an integer such that $|s| \leq \exp(2^{n/c_2}) = 2^{(1/\log 2)2^{n/c_2}}$ has only finitely many effectively computable positive integer solutions m and, in fact, all such solutions have $m < c_1$, where c_1 is the constant appearing in the statement of Theorem 2. Thus, Theorem 2 is somewhat

similar to Theorem 1 when $b := \pm 1$. Of course, even in this case Theorem 1 is better, but there l has a very particular value, $t := 1$, $p_1 := 2$, and a and b satisfy some restrictive congruence conditions. In the general case, i.e., with an arbitrary value of b, it seems to be hard to obtain good lower bounds on Q in terms of P comparable to the ones in the case $b := \pm 1$, where P and Q are defined in the statement of Theorem 2. However, at least when the two roots of the characteristic equation of $(u_n)_{n\geq 0}$ are real, or when the coefficients a and b of the recurrence relation for $(u_n)_{n\geq 0}$ are not coprime and $l \neq 0$, one can use similar methods as in the proof of Theorem 2 to show that there exist two effectively computable constants c_1 and c_2, depending again only on $(u_n)_{n\geq 0}$, l, and $\mathcal{P}$, such that the inequality $\log |Q| > c_2\Big(\dfrac{m}{\log m}\Big)$ holds for all $m > c_1$. Finally, in the worst case, in which the two roots of the characteristic equation of $(u_n)_{n\geq 0}$ are complex conjugates and a and b are coprime, it is an immediate application of the Subspace Theorem (see [10]) that for every $\varepsilon > 0$ the inequality $|Q| > |u_m|^{1-\varepsilon}$ holds for all but finitely many values of the positive integer m. We do not give further details in this direction and restrict ourselves to presenting the proof of Theorem 2 as stated above.

Returning to elementary arguments, by using the method of proof of Theorem 1, we have the following result for the case in which $(v_n)_{n\geq 0}$ is the Fibonacci or Pell sequence.

Theorem 3. (*i*) *There are only three Fibonacci numbers that are also Cullen numbers, namely* $F_1 = F_2 = 1$ *and* $F_4 = 3$. *There are only two Fibonacci numbers that are also Woodall numbers, namely* $F_1 = F_2 = 1$.

(*ii*) *There is only one Pell number that is also a Cullen number, namely* $P_1 = 1$. *There is only one Pell number that is also a Woodall number, namely* $P_1 = 1$.

3 The Proof of the Theorems

We start with the nonelementary proof of Theorem 2.

Proof of Theorem 2. Throughout this proof, all constants which appear are positive, effectively computable, and labelled increasingly as $c_3,\ c_4,\ \ldots$. We reserve the notation c_1 and c_2 for the final constants asserted in the statement of Theorem 2.

Write

$$u_n = A\alpha^n - B\beta^n.$$

Since $b := \pm 1$, we get that $\beta = \pm\alpha^{-1}$. Recall that we are assuming that $a > 0$, for otherwise we may replace a by $-a$, l by $\pm l$, and $(u_n)_{n\geq 0}$ by $((-1)^n u_n)_{n\geq 0}$. In particular, $\alpha > 1 > |\beta|$. We treat only the case of the parameter $l \neq 0$ since the other case is even easier. Let m be a large positive integer and write $z := \alpha^m$, therefore

$$u_m = Az \pm Bz^{-1}.$$

In particular,

$$u_m - l = Az \pm Bz^{-1} - l = Az^{-1}(z - z_1)(z - z_2),$$

where $z_{1,2}$ are the roots of the equation

$$x^2 - \frac{l}{A}x \pm \frac{B}{A} = 0.$$

Let $\mathbf{K}$ be the smallest number field containing all the numbers α, β and z_1, z_2 for both choices of signs $\pm$ above. Let p be any of the prime numbers $p_1, \ldots, p_t$, and let π be any prime ideal of $\mathcal{O}_{\mathbf{K}}$ sitting above p, where we use $\mathcal{O}_{\mathbf{K}}$ for the ring of algebraic integers inside

K. It is easy to see that the inequality

$$|u_m| > c_3\alpha^m \tag{1}$$

holds for sufficiently large values of m, where one can take $c_3 := |A|/2$. In particular, for large m, we have

$$|u_m| > 2|l|, \tag{2}$$

and therefore $u_m - l$ is nonzero. Thus, none of the factors $z - z_1$ and $z - z_2$ is zero either. For any algebraic number γ in **K** and any prime ideal π in $\mathcal{O}_{\mathbf{K}}$ we write $\mathrm{ord}_\pi(\gamma)$ for the order at which π appears in the factorization in prime ideals of the fractional ideal $[\gamma]$ generated by γ inside **K**. Using a linear form in p-adic logarithms (immediate application of Theorem 1 in [12]), we get that both inequalities

$$\mathrm{ord}_\pi(z - z_1) = \mathrm{ord}_\pi(\alpha^m - z_1) < c_4 \log m,$$

and

$$\mathrm{ord}_\pi(z - z_2) = \mathrm{ord}_\pi(\alpha^m - z_2) < c_4 \log m$$

hold with some constant c_4 depending on the sequence $(u_n)_{n\geq 0}$, the number l, as well as the prime number p. The constant c_4 can be taken to be of the form $c_5 \cdot p^2$, where c_5 is absolute. Since p can take only finitely many values, we get that if we write

$$P := p_1^{\alpha_1} \cdot \cdots \cdot p_t^{\alpha_t},$$

then the inequality

$$\max\{\alpha_i \mid i = 1, \ldots, t\} < c_6 \log m$$

holds with some computable constant c_6, which can be taken to be $c_6 := c_5 \cdot p_t^2$. Now

$$u_m - l = PQ,$$

therefore

$$\log |u_m - l| = \log |P| + \log |Q|.$$

Since for large m we have

$$|u_m - l| > c_7 \alpha^m \tag{3}$$

with $c_7 := |A|/2$, we get

$$c_8 m - c_9 < \log |u_m - l| = \log |P| + \log |Q| < c_{10} \log m + \log |Q|.$$

Here, one can take $c_8 := \log \alpha > 0, c_9 := |\log(|A|/2)| > 0$, and $c_{10} := c_6 \log(p_1 \cdot \cdots \cdot p_t)$. The above inequality implies that

$$\log |Q| > c_8 m - c_9 - c_{10} \log m.$$

However, the inequality

$$c_8 m - c_9 - c_{10} \log m > c_{11} m \tag{4}$$

clearly holds for large values of m, where c_{11} can be chosen to be any fixed constant strictly smaller than c_8. So, let us just take $c_{11} := c_8/2$, and let us write c_1 for the computable constant so that all the inequalities (1) - (4) hold for $m > c_1$. Thus, on the one hand we have that $\log |Q| > c_{11} m$, while on the other hand we have that $|P| < \exp(c_{10} \log m) = m^{c_{10}}$, which imply that $\log |Q| > c_{11} |P|^{1/c_{10}}$. It is now clear that this last inequality implies the conclusion of Theorem 2 with any constant c_2 strictly smaller than $1/c_{10}$. □

To prove Theorem 1, we need to recall some known facts about the distribution of the Lucas sequence $(v_k)_{k\geq 0}$ modulo 2^n.

Lemma 4. *If $a > 0$ is odd and $b \equiv 1 \pmod{16}$ then the Lucas sequence $(v_k)_{k\geq 0}$ satisfies the following properties:*

(i) if $v_N \equiv 3 \pmod 4$ and $v_k \equiv v_N \pmod{2^n}$, $n \geq 6$, $k > N$, then $k \equiv N \pmod{3 \cdot 2^{n-1}}$,

(ii) if $v_N \equiv 0 \pmod 8$ and $v_k \equiv v_N \pmod{2^n}$, $n \geq 6$, $k > N$, then $k \equiv N \pmod{3 \cdot 2^{n-2}}$.

Proof. It is well known (see [3], for instance), that under the assumptions of the lemma, the period of $(v_k)_{k\geq 0}$ modulo 2^n is $3 \cdot 2^{n-1}$. Theorem 1.1 of [3] shows that every residue r modulo 2^n satisfying $r \equiv 3 \pmod 4$ appears only once in every period of $(v_k)_{k\geq 0}$ modulo 2^n, which implies (i). To see (ii), we use again the same Theorem 1.1 of [3] which says that every residue r modulo 2^n satisfying $r \equiv 0 \pmod 8$ appears exactly twice in every period of $(v_k)_{k\geq 0}$ modulo 2^n. From the proof of that same theorem (p. 303), we deduce that the distance between two such *consecutive* residues is $3 \cdot 2^{n-2}$, which completes the proof of our lemma. □

Remark. The previous lemma implies that if $k > N \geq 0$ are consecutive indices satisfying $v_k \equiv v_N \pmod{2^n}$ and $v_N \equiv 0 \pmod 8$, then $k - N = 3 \cdot 2^{n-2}$.

For the purpose of the next lemma, we assume that $(u_n)_{n\geq 0}$ is an almost Lucas sequence with $a > 0$. Write $\gamma := \sqrt{\Delta} = \sqrt{a^2 + 4b} = \alpha - \beta$. Observe that $1 \leq \gamma = \alpha - \beta$. We will not be using all inequalities from the next lemma, but we thought they might have an interest of their own.

Lemma 5. *The inequalities*

$$A\alpha^{k-1} \leq u_k = A(\alpha^k - \beta^k) \leq u_1\alpha^{k-1}, \text{ if } b > 0 \tag{5}$$

$$u_1\alpha^{k-1} \leq u_k = A(\alpha^k - \beta^k) \leq \frac{au_1}{\gamma}\alpha^{k-1}, \text{ if } b < 0 \tag{6}$$

hold for all positive integers k.

Proof. Since $u_1 \geq 1$ and $u_n = u_1 v_n$ holds for all $n \geq 0$, we may divide both inequalities (5) and (6) across by u_1 and restrict our attention to proving these inequalities for the sequence $(v_n)_{n\geq 0}$.

If $b > 0$, then since $b = -\alpha\beta$, we get that $\beta < 0$. Thus,

$$A(\alpha^k - \beta^k) = \frac{\alpha^k - \beta^k}{\alpha - \beta} = \frac{\alpha^k - \beta^k}{\alpha + |\beta|}.$$

Clearly,

$$\frac{\alpha^k - \beta^k}{\alpha + |\beta|} \leq \frac{\alpha^k + |\beta|^k}{\alpha + |\beta|} \leq \alpha^{k-1},$$

with the last inequality holding because $\alpha > |\beta|$, which takes care of the inequality from the right hand side of (5). The inequality from the left hand side of (5) is implied by

$$\alpha^k - |\beta|^k > \alpha^{k-1},$$

which is equivalent to $\alpha^{k-1}(\alpha - 1) > |\beta|^k$. The previous inequality is implied by $\alpha^{k-1} > |\beta|^{k-1}$ and $\alpha - 1 > |\beta|$, with the last inequality being true because $\alpha - |\beta| = \alpha + \beta = a \geq 1$. When $b < 0$, then $\alpha > \beta > 0$, therefore the inequality from the right hand side of (6) is simply

$$\frac{\alpha^k - \beta^k}{\alpha - \beta} < \frac{\alpha^{k-1}(\alpha + \beta)}{\alpha - \beta},$$

which is obvious because $\alpha^{k-1}(\alpha+\beta) > \alpha^k > \alpha^k - \beta^k$. The inequality from the left hand side of (6) is simply

$$\alpha^{k-1} < \frac{\alpha^k - \beta^k}{\alpha - \beta},$$

which is also obvious because it is equivalent to $\alpha^{k-1}\beta > \beta^k$. □

Proof of Theorem 1. Let k and n be nonnegative integers such that $v_k = C_n(s, v_N)$. Thus,

$$v_k = s_n \cdot 2^n + v_N. \tag{7}$$

We may certainly assume that $n \geq 6$ and that $k \geq 1$. Equation (7) implies that $v_k \equiv v_N \pmod{2^n}$. By Lemma 4, we get that if $k > N$, then

$$k \geq N + 3 \cdot 2^{n-1}, \text{ if } v_N \equiv 3 \pmod 4, \tag{8}$$

$$k \geq N + 3 \cdot 2^{n-2}, \text{ if } v_N \equiv 0 \pmod 8. \tag{9}$$

Using Lemma 5, inequalities (8) and (9), together with the fact that $A = \dfrac{1}{\alpha - \beta} \geq \dfrac{1}{2\alpha}$ when $b > 0$ (clearly, this last inequality holds when $b < 0$ as well, but we shall need it only in the case $b > 0$), we deduce that

$$s_n \cdot 2^n + v_N = v_k \geq A\alpha^{k-1} \geq \frac{1}{2} \cdot \alpha^{3\cdot 2^{n-1}+N-2}, \text{ if } b > 0 \text{ and } v_N \equiv 3 \pmod 4, \tag{10}$$

$$s_n \cdot 2^n + v_N = v_k \geq A\alpha^{k-1} \geq \frac{1}{2} \cdot \alpha^{3\cdot 2^{n-2}+N-2}, \text{ if } b > 0 \text{ and } v_N \equiv 0 \pmod 8, \tag{11}$$

$$s_n \cdot 2^n + v_N = v_k \geq v_1\alpha^{k-1} \geq \alpha^{3\cdot 2^{n-1}+N-1}, \text{ if } b < 0 \text{ and } v_N \equiv 3 \pmod 4, \tag{12}$$

$$s_n \cdot 2^n + v_N = v_k \geq v_1\alpha^{k-1} \geq \alpha^{3\cdot 2^{n-2}+N-1}, \text{ if } b < 0 \text{ and } v_N \equiv 0 \pmod 8. \tag{13}$$

But $\alpha > 1$, and $s_n = O(\alpha^{2^{n-1}})$, therefore the previous inequalities are false for $n > c_1$ where c_1 is some computable constant depending only on α, s and N. In fact, it is clear

that the dependence on s is encrypted only in the constant understood in the inequality $s_n = O(\alpha^{2^{n-1}})$. Theorem 1 is therefore proved. □

Remark. Any polynomial with integer coefficients in the variable n is an example of a sequence $(s_n)_{n\geq 0}$.

Although Theorem 3 is not a direct application of Theorem 1, the proof of this result can be achieved along the same lines. We need the following lemma.

Lemma 6.

(i) If $n \geq 3$, then $F_k \equiv \pm 1 \pmod{2^n}$ if and only if $k \equiv \pm 1, \pm 2 \pmod{3 \cdot 2^{n-1}}$.

(ii) If $n \geq 2$, then $P_k \equiv 1 \pmod{2^n}$ if and only if $k \equiv \pm 1 \pmod{2^n}$.

Proof. (i) This is well known (see [7]). (ii) By Theorem 3.1(a) of [4], the sequence $(P_k)_{k\geq 0}$ has period 2^n modulo 2^n. Thus, if $n = 2$, then looking at the first four terms of the Pell sequence, we get that the sequence $(P_k)_{k\geq 0}$ is congruent to $0, 1, 2, 1$ modulo 4. Thus, $P_k \equiv 1 \pmod 4$ if and only if $k \equiv \pm 1 \pmod 4$. Assume now that $n > 2$ and proceed by induction. By Lemma 4.3 of [4] and the induction hypothesis, the residue 1 appears exactly twice in one period of $(P_k)_{k\geq 0}$ modulo 2^{n+1}, so it is sufficient to prove that $P_1 \equiv P_{2^{n+1}-1} \equiv 1 \pmod{2^{n+1}}$. Since $P_1 = 1$, it suffices to show that $P_{2^{n+1}-1} \equiv 1 \pmod{2^{n+1}}$. Using the relation

$$P_{m+n} = P_{m-1}P_n + P_m P_{n+1},$$

we obtain $P_{2^n+2^n-1} = (P_{2^n-1})^2 + (P_{2^n})^2$. By the induction hypothesis, $P_{2^n-1} \equiv 1 \pmod{2^n}$, therefore $(P_{2^n-1})^2 \equiv 1 \pmod{2^{n+1}}$. By Proposition 2.4$(a)$ of [4], $P_{2^n} \equiv 0 \pmod{2^{n+1}}$. Thus, $P_{2^{n+1}-1} \equiv 1 \pmod{2^{n+1}}$. □

Proof of Theorem 3. We first look at the case of the Fibonacci numbers. Assume that k and n are nonnegative integers such that $F_k = n \cdot 2^n + 1$. When $n = 0,\ 1$, we obtain the obvious solutions $(k, n) = (1, 0), (2, 0), (4, 1)$. The case $n = 2$ does not render a solution, so, from here on, we assume that $n \geq 3$, and therefore that $k \geq 5$. Thus

$$F_k \equiv 1 \pmod{2^n},$$

which implies, by Lemma 6, that $k \equiv \pm 1, \pm 2 \pmod{3 \cdot 2^{n-1}}$. Since $k \geq 5$, it follows that

$$k + 2 \geq 3 \cdot 2^{n-1}. \tag{14}$$

Since the inequality

$$\frac{\alpha^k}{\sqrt{5}} - \frac{1}{2} \ < \ F_k < \frac{\alpha^k}{\sqrt{5}} + \frac{1}{2},$$

holds, where $\alpha := (1 + \sqrt{5})/2$ is the golden section, we get

$$n \cdot 2^n + 1 = F_k > \frac{\alpha^k}{\sqrt{5}} - \frac{1}{2} \geq \frac{\alpha^{3 \cdot 2^{n-1}-2}}{\sqrt{5}} - \frac{1}{2}.$$

Therefore, n must satisfy the inequality

$$\sqrt{5} \cdot n \cdot 2^{n+1} + 3\sqrt{5} > 2 \cdot \alpha^{3 \cdot 2^{n-1}-2}, \tag{15}$$

which is impossible because the function

$$x \longmapsto 2 \cdot \alpha^{3 \cdot 2^{x-1}-2} - \sqrt{5} \cdot x \cdot 2^{x+1} - 3\sqrt{5}$$

is positive for all $x \geq 3$ (in fact, the largest positive zero of the above function is $x_0 \approx 2.71031$).

The argument for the case of the Pell sequence is entirely similar. Let again k and n be nonnegative integers satisfying the equation $P_k = n \cdot 2^n + 1$. When $n = 0,\ 1,\ 2$ we only

get the solution $(k, n) = (1, 0)$. Assume now that $n \geq 3$. If $P_k = n \cdot 2^n + 1$, then $P_k \equiv 1 \pmod{2^n}$. This implies, by Lemma 6 (ii), that $k + 1 \geq 2^n$, and employing Lemma 5, we get

$$n \cdot 2^n + 1 = P_k \geq \frac{\sqrt{2}}{4}(1 + \sqrt{2})^{2^n - 2}, \tag{16}$$

which is impossible for $n \geq 3$ because the largest positive zero of the function

$$x \longmapsto \frac{\sqrt{2}}{4}(1 + \sqrt{2})^{2^x - 2} - x \cdot 2^x - 1$$

is $x_1 \approx 2.69847$.

The analysis of the diophantine equations involving Woodall rather than Cullen numbers and Fibonacci or Pell numbers is entirely similar. □

Acknowledgements. Our deepest thanks go the referee whose detailed and helpful comments significantly improved both the quality as well as the presentation of the present paper. The first author was partly supported by grants ECOS-ANUIES M02-M01, SEP-CONACYT 37259-E and SEP-CONACYT 37260-E. The second author was partially supported by a research grant from the School of Sciences at his institution.

References

[1] R. Ballinger, *Proth Search Page*, http://www.prothsearch.net/woodall.html.

[2] C. Caldwell, *The Prime Pages*, http://primes.utm.edu/.

[3] W. Carlip, E. Jacobson, *On the stability of certain Lucas sequences modulo* 2^k, The Fibonacci Quart. **34**, No. 4 (1996), 298-305.

[4] W. Carlip, E. Jacobson, *Stability of two-term recurrence sequences with even parameter*, Finite Fields Appl. **3** (1997), 70-83.

[5] R. Guy, Unsolved Problems in Number Theory (2nd ed.), Springer-Verlag, New York, 1994.

[6] C. Hooley, Applications of the sieve methods to the theory of numbers, Cambridge University Press, Cambridge, 1976.

[7] E. Jacobson, *Distribution of the Fibonacci numbers modulo* 2^k, The Fibonacci Quart. **30**, No. 3 (1992), 211-215.

[8] W. Keller, *New Cullen Primes*, Math. Comput. **64** (1995), 1733-1741.

[9] F. Luca, *On the greatest common divisor of two Cullen numbers*, preprint, 2002.

[10] H.P. Schlickewei, *S-unit equations over number fields*, Inventiones Math. **102** (1990), 95–107.

[11] T.N. Shorey, R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, 1986.

[12] K. Yu, *Linear forms in p-adic logarithms. III*, Compositio Math. **91** (1994), no. 3, 241–276.

2000 *Mathematics Subject Classification.* 11B37, 11B39, 11B83, 11J86, 11K31.