2015-11-06

On a divisibility relation for Lucas sequences

Komatsu, Takao

American Mathematical Society

arXic:1511.01970v1 [math.NT] 6 Nov 2015
http://hdl.handle.net/10945/47534

On a divisibility relation for Lucas sequences

Takao Komatsu[1], Florian Luca[2]
Amalia Pizarro-Madariaga[3], Pantelimon Stănică[4*]

[1] School of Mathematics and Statistics, Wuhan University
Wuhan 430072 China;
Email: komatsu@whu.edu.cn
[2] School of Mathematics, University of the Witwatersrand,
Private Bag X3, Wits 2050, South Africa;
Email: florian.luca@wits.ac.za
[3] Instituto de Matemáticas,
Universidad de Valparaiso, Chile;
Email: amalia.pizarro@uv.cl
[4] Naval Postgraduate School, Applied Mathematics Department,
Monterey, CA 93943–5216, USA;
Email: pstanica@nps.edu

November 9, 2015

Abstract

In this note, we study the divisibility relation $U_m \mid U_{n+k}^s - U_n^s$, where $\mathbf{U} := \{U_n\}_{n\geq 0}$ is the Lucas sequence of characteristic polynomial $x^2 - ax \pm 1$ and k, m, n, s are fixed positive integers.

Keywords. Lucas sequence, roots of unity, divisibility
Mathematics Subject Classification (2010). 11B39

---

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

1 Introduction

Let $\mathbf{U} := \mathbf{U}(a,b) = \{U_n\}_{n\geq 0}$ be the Lucas sequence given by $U_0 = 0,\ U_1 = 1$ and

$$U_{n+2} = aU_{n+1} + bU_n \quad \text{for all} \quad n \geq 0, \quad \text{where} \quad b \in \{\pm 1\}. \tag{1}$$

Its characteristic equation is $x^2 - ax - b = 0$ with roots

$$(\alpha, \beta) = \left(\frac{a + \sqrt{a^2+4b}}{2}, \frac{a - \sqrt{a^2+4b}}{2} \right).$$

When $a \geq 1$, we have that $\alpha > 1 > |\beta|$. We assume that $\Delta = a^2 + 4b > 0$ and that α/β is not a root of unity. This only excludes the pairs $(a,b) \in \{(0,\pm 1),\ (\pm 1,-1),\ (2,-1)\}$ from the subsequent considerations. Here, we look at the relation

$$U_m \mid U_{n+k}^s - U_n^s, \tag{2}$$

with positive integers $k,\ m,\ n,\ s$. Note that when $(a,b) = (1,1)$, then $U_n = F_n$ is the nth Fibonacci number. Taking $k = 1$ and using the relations

$$\begin{aligned} F_{n+1} - F_n &= F_{n-1}, \\ F_{n+1} + F_n &= F_{n+2}, \\ F_{n+1}^2 + F_n^2 &= F_{2n+1}, \end{aligned}$$

it follows that relation (2) holds with $s = 1, 2, 4$, and $m = n-1,\ n+1,\ 2n+1$, respectively. Further, in [3], the authors assumed that m and n are coprime positive integers. In this case, F_n and F_m are coprime, so the rational number F_{n+1}/F_n is defined modulo F_m. Then it was shown in [3] that if this last congruence class above has multiplicative order s modulo F_m and $s \notin \{1, 2, 4\}$, then

$$m < 500s^2. \tag{3}$$

In this paper, we study the general divisibility relation (2) and prove the following result.

Theorem 1. *Assume* $b \in \{\pm 1\}$, $(a,b) \notin \{(0,\pm 1),\ (\pm 1,-1),\ (\pm 2,-1)\}$ *and that divisibility* (2) *holds. Then*

$$m < \max\{9(n+k), 1440000(sk)^2\}. \tag{4}$$

2 Preliminary results

We put $\mathbf{V} := \mathbf{V}(a,b) = \{V_n\}_{n\ge 0}$ for the Lucas companion of $\mathbf{U}$ which has initial values $V_0 = 2,\ V_1 = a$ and satisfies the same recurrence relation $V_{n+2} = aV_{n+1} + bV_n$ for all $n \ge 0$. The Binet formulas for U_n and V_n are

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n = \alpha^n + \beta^n \qquad \text{for all} \qquad n \ge 0. \tag{5}$$

The next result addresses the period of $\{U_n\}_{n\ge 0}$ modulo U_m, where $m \ge 1$ is fixed.

Lemma 2. *The congruence*

$$U_{n+4m} \equiv U_n \pmod{U_m} \tag{6}$$

holds for all $n \ge 0$, $m \ge 2$.

Proof. This follows because of the following identity

$$U_{n+4m} - U_n = U_m V_m V_{n+2m},$$

which can be easily checked using the Binet formulas (5). □

The following is Lemma 1 in [3]. It has also appeared in other places.

Lemma 3. *Let $X \ge 3$ be a real number. Let a and b be positive integers with $\max\{a,b\} \le X$. Then there exist integers u, v not both zero with $\max\{|u|,|v|\} \le \sqrt{X}$ such that $|au + bv| \le 3\sqrt{X}$.*

Lemma 4. *Let v be any positive integer and $\zeta \ne 1$ be such that $\zeta^v = 1$. Then $1 - \zeta$ divides v in $\mathbb{Q}(e^{2\pi i/v})$.*

Proof. Clearly,

$$1 - \zeta \mid \prod_{\substack{\eta^v = 1\\ \eta \ne 1}} (1 - \eta) = \frac{d}{dX}(X^v - 1)\Big|_{X=1} = v.$$

□

Let $\zeta = e^{2\pi i u/v}$ be a primitive root of unity of order $v \ge 1$, where $1 \le u \le v$ is an integer coprime to v. The following lemma is the workhorse of our argument.

Lemma 5. *Let $a \geq 1$. Assume further that*

$$\alpha \qquad \text{and} \qquad \frac{\alpha^k - (-b)^k \overline{\zeta}}{\alpha^k - \zeta} \tag{7}$$

are multiplicatively dependent. Then

(i) $(-b)^k = -1$, $v = 4$;

(ii) $(a, b, k) = (1, -1, 1)$, $(2, -1, 1)$, *and* $v \in \{1, 2\}$;

(iii) $(-b)^k = 1$, $v \in \{1, 2\}$;

(iv) $(a, b, k) = (4, -1, 1)$, *and* $v \in \{3, 4, 6\}$;

Proof. We follow the method of proof of Lemma 2 from [3]. Note that α and α^k are already multiplicatively dependent. Thus, putting $(\alpha_1, \beta_1) := (\alpha^k, \beta^k)$, and noting that $-b_1 = \alpha_1\beta_1 = (-b)^k$, it suffices to first find all instances when

$$\alpha_1^m = \left(\frac{\alpha_1 - (-b_1)\overline{\zeta}}{\alpha_1 - \zeta}\right)^n \tag{8}$$

holds with some integers m, n not both zero. We distinguish two cases according to the sign of b_1.

Case 1. $b_1 = 1$.

This is possible only when $b = 1$ and k is odd. This case is similar with Lemma 2 in [3]. Let us reproduce the details here. If $n = 0$, then $\alpha_1^m = 1$, therefore $m = 0$, which is impossible. So, we assume that $n \neq 0$. Let $Ł = \mathbb{Q}(e^{2\pi i/v}) = \mathbb{Q}(\zeta)$. Let $\mathbb{K} = \mathbb{Q}(\alpha)$.

Assume first that $\mathbb{K}$ is not contained in Ł. Then $\mathbb{K}$ and Ł are both Galois extensions of $\mathbb{Q}$ whose intersection is trivial (i.e., equal to $\mathbb{Q}$). Thus, every Galois automorphism σ of $G = \mathrm{Gal}(Ł/\mathbb{Q})$ can be extended to a Galois automorphism of the compositum $\mathbb{M} = \mathbb{K}Ł$ of $\mathbb{K}$ and Ł in such a way that $\sigma(\alpha) = \alpha$. Applying an arbitrary such $\sigma \in G$ to (8), we deduce that equation (8) holds when we replace ζ by any conjugate of it. In particular, given $u_1, u_2 \in \{1, \ldots, v\}$ both coprime to v, we have

$$\left(\frac{\alpha_1 + e^{-2\pi i u_1/v}}{\alpha_1 - e^{2\pi i u_1/v}}\right)^m = \alpha^n = \left(\frac{\alpha_1 + e^{-2\pi i u_2/v}}{\alpha_1 - e^{2\pi i u_2/v}}\right)^m. \tag{9}$$

Taking absolute values in (9) and then extracting mth roots, we get

$$\begin{aligned}
-1+\frac{2\alpha_1^2+2}{\alpha_1^2-2\alpha_1\cos(2\pi u_1/v)+1} &= \frac{\alpha_1^2+2\alpha_1\cos(2\pi u_1/v)+1}{\alpha_1^2-2\alpha_1\cos(2\pi u_1/v)+1}\\
&= \left|\frac{\alpha_1+e^{-2\pi i u_1/v}}{\alpha_1-e^{2\pi i u_1/v}}\right|^2 = \left|\frac{\alpha_1+e^{-2\pi i u_2/v}}{\alpha_1-e^{2\pi i u_2/v}}\right|^2\\
&= \frac{\alpha_1^2+2\alpha_1\cos(2\pi u_2/v)+1}{\alpha_1^2-2\alpha_1\cos(2\pi u_2/v)+1}\\
&= -1+\frac{2\alpha_1^2+2}{\alpha_1^2-2\alpha_1\cos(2\pi u_2/v)+1},
\end{aligned}$$

giving

$$\cos(2\pi u_1/v)=\cos(2\pi u_2/v).$$

This gives

$$\begin{aligned}
\sin(2\pi u_1/v) &= \pm\sqrt{1-\cos(2\pi u_1/v)^2}=\pm\sqrt{1-\cos(2\pi u_2/v)^2}\\
&= \pm\sin(2\pi u_2/v).
\end{aligned}$$

This argument shows that there exist at most 2 primitive roots of unity of order v, therefore $\phi(v)\le 2$. Thus, $v\in\{1,2,3,4,6\}$. Further,

$$\frac{\alpha_1+\overline{\zeta}}{\alpha_1-\zeta}$$

is a unit so $\alpha_1-\zeta$ is associated to $\alpha_1+\overline{\zeta}$. Thus,

$$\alpha_1-\zeta \mid \alpha_1+\overline{\zeta}=(\alpha_1-\zeta)+(\zeta+\overline{\zeta}),$$

giving

$$\alpha_1-\zeta \mid \zeta+\overline{\zeta}. \tag{10}$$

The case $\zeta+\overline{\zeta}=0$ gives $\zeta=\varepsilon i$ for some $\varepsilon\in\{\pm1\}$. Then

$$\frac{\alpha_1+\overline{\zeta}}{\alpha-\zeta}=\frac{\alpha_1-\varepsilon i}{\alpha_1-\varepsilon i}=1,$$

and so (8) holds with $m=0$ and any n. This is instance (i).

Assume now that $\zeta\not\in\{\pm i\}$. Then the number on the right–hand side of (10) above belongs to $\{\pm1,\pm2\}$ so it divides the integer 2. Since $\mathbb{K}\not\subset Ł$, it follows that there is an automorphism of $\mathbb{M}$ mapping α to β and fixing ζ. Hence, we have that $\beta_1 - \zeta \mid 2$ as well, therefore

$$(\alpha_1 - \zeta)(\beta_1 - \zeta) \mid 4,$$

or

$$-1 - \zeta(\alpha_1 + \beta_1) + \zeta^2 \mid 4.$$

Looping over the finitely many possibilities for ζ and the divisors of 4 in $\mathbb{Q}(\zeta)$, the above relation gives us that $\alpha_1 + \beta_1 = \alpha^k + \beta^k \in \{1, 2\}$. Since $\alpha^k + \beta^k = U_{2k}/U_k$, by the Primitive Divisor Theorem of Carmichael (see [2]), we get that if $k \geq 7$, then U_{2k}/U_k is divisible by a primitive prime factor of U_{2k} which is at least as large as $2k - 1 \geq 13$. Since $\alpha_1 + \beta_1 \in \{1, 2\}$, we infer that $k \leq 6$. Now trying all possibilities we only get that $k = 1$ and $a \in \{1, 2\}$. Further, trying out all values of $\zeta = e^{2\pi i u/v}$ with $v \in \{1, 2, 3, 6\}$ and u coprime to v and checking whether or not $(\alpha + \overline{\zeta})/(\alpha - \zeta)$ is multiplicatively dependent over α, we only get the examples shown at (ii).

A similar argument applies when $\mathbb{K} \subseteq \mathbb{L}$. In this case, $\mathbb{M} = \mathbb{L}$ and $G = \mathrm{Gal}(\mathbb{M}/\mathbb{Q})$ is isomorphic with the group of invertible elements modulo v which has order $\phi(v)$. Further, by Galois theory, there are exactly $\phi(v)/2$ Galois automorphisms σ such that $\sigma(\alpha) = \alpha$. We deduce that there exists a subset $\mathcal{U} \subset \{1, 2, \ldots, v\}$ of positive integers coprime to v having exactly $\phi(v)/2$ elements, such that equation (8) holds for all $\zeta = e^{2\pi i u/v}$ with all $u \in \mathcal{U}$. The preceding argument shows that

$$\cos(2\pi u_1/v) = \cos(2\pi u_2/v) \quad \text{holds for all} \quad u_1, u_2 \in \mathcal{U},$$

therefore

$$\sin(2\pi u_1/v) = \pm \sin(2\pi u_2/v) \quad \text{holds for all} \quad u_1, u_2 \in \mathcal{U}.$$

This shows that the number of elements in $\mathcal{U}$ is at most 2, so $\phi(v) \leq 4$. Hence, $v \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Further, here we have the additional information that $\mathbb{L}$ contains the real quadratic field $\mathbb{K}$. It then follows that:

- (i) $v = 5, 10$, $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, and $\alpha = ((1 + \sqrt{5})/2)^\ell$ for some positive integer ℓ;
- (ii) $v = 8$, $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, and $\alpha = (1 + \sqrt{2})^\ell$ for some positive integer ℓ;
- (iii) $v = 12$, $\mathbb{K} = \mathbb{Q}(\sqrt{3})$, and $\alpha = (2 + \sqrt{3})^\ell$ for some positive integer ℓ.

Since $b=1$ and k is odd, case (iii) above is not possible. Only case (i) and (ii) are possible and then ℓ is odd. As before, we get the relation

$$\alpha_1 - \zeta \mid \zeta + \overline{\zeta}.$$

We take norms in Ł and using (i) and (ii) above, we get a certain number of possibilities for k and for ℓ (therefore, also for a). In fact we always get $k=\ell=1$ and $(u,v)\in\{(2,5),\ (3,5),\ (3,10),\ (7,10),\ (3,8),\ (5,8)\}$. We now checked that in fact for these six cases of $\zeta = e^{2\pi i u/v}$ and corresponding α, the elements α and $(\alpha+\overline{\zeta})/(\alpha-\zeta)$ are in fact not multiplicatively dependent.

Case 2. $b_1 = -1$.

In this case, either $b=1$ and k is even, or $b=-1$. Here, we need to study when α_1 and $(\alpha_1-\overline{\zeta})/(\alpha_1-\zeta)$ are multiplicatively dependent. When $\zeta\in\{\pm 1\}$ the second number is 1, so they are multiplicatively dependent (we can take $n=0$ and any m in relation (8)). This is instance (iii).

So, assume that ζ is non real, therefore that $v\geq 3$. Since α_1 is real, we get that $(\alpha_1-\overline{\zeta})/(\alpha_1-\zeta)$ has absolute value 1. Thus, taking absolute values in equation (8) we get $\alpha_1^m = 1$, therefore $m=0$. Thus, $n\neq 0$, therefore

$$\frac{\alpha_1-\overline{\zeta}}{\alpha_1-\zeta} = \eta, \tag{11}$$

where η is a root of unity. Let us exploit this relation. As before, we put $\mathbb{K}=\mathbb{Q}(\alpha)$, Ł $=\mathbb{Q}(\zeta)$ and distinguish two cases.

Subcase 2.1 $\mathbb{K}\not\subseteq$ Ł.

Relation (11) implies that

$$\alpha_1-\zeta \mid \alpha_1-\overline{\zeta} = (\alpha_1-\zeta)+(\zeta-\overline{\zeta}),$$

so $\alpha_1-\zeta \mid \overline{\zeta}-\zeta = \zeta^{-1}(1-\zeta^2)$. The last number divides v by Lemma 4. Further, since $\alpha\notin\mathbb{L}$, it follows that every Galois automorphism σ of Ł can be lifted to a Galois automorphism of the compositum $\mathbb{M}=\mathbb{K}$Ł such that $\sigma(\alpha)=\alpha$. In particular,

$$\alpha_1-\zeta' \mid v,$$

for all primitive roots of unity ζ' of order v. Since $\beta_1 = 1/\alpha_1$ is positive, the above relation implies that

$$(\sqrt{\alpha_1}-\zeta'\sqrt{\beta_1}) \mid v$$

in the number field $\mathbb{Q}(\zeta, \sqrt{\alpha})$. Here, $\sqrt{\alpha_1}$ and $\sqrt{\beta_1}$ denote the positive determinations of these two square roots. Multiplying the above relations over all primitive roots of unity ζ' of order v, we get

$$\Phi_v(\sqrt{\alpha_1}, \sqrt{\beta_1}) \mid v,$$

where $\Phi_n(X, Y)$ stands for the homogenization of the cyclotomic polynomial $\Phi_n(X)$. Since $\Phi_v(X, Y)$ is symmetric in X and Y, it follows from the Fundamental Theorem of Symmetric Polynomials that $\Phi_v(X+Y) = R(X+Y, XY)$ for some polynomial $R(X, Y) \in \mathbb{Z}[X, Y]$. Thus,

$$\Phi_v(\sqrt{\alpha_1}, \sqrt{\beta_1}) = R(\sqrt{\alpha_1} + \sqrt{\beta_1}, 1).$$

Since the degree of $\Phi_v(X, Y)$ which is $\phi(v)$ is even, it follows that $R(S, 1)$ contains only monomials of even degree in S. Therefore, since

$$(\sqrt{\alpha_1} + \sqrt{\beta_1})^2 = \alpha_1 + \beta_1 + 2$$

is a positive integer, we get that $\Phi_v(\sqrt{\alpha_1}, \sqrt{\beta_1})$ is an integer divisor of v. From the Primitive Divisor Theorem, or more precisely from the proof of it, $\Phi_v(\sqrt{\alpha_1}, \sqrt{\beta_1})$ captures all the primitive prime factors of the vth term of the Lehmer sequence $\mathbf{L} = \{L_n\}_{n\geq 0}$ of parameters $(\alpha_2, \beta_2) = (\sqrt{\alpha_1}, \sqrt{\beta_1})$ whose general term is given by

$$L_n = \begin{cases} \frac{\alpha_2^n - \beta_2^n}{\alpha_2 - \beta_2} & \text{if} \quad n \equiv 1 \pmod 2; \\ \frac{\alpha_2^n - \beta_2^n}{\alpha_2^2 - \beta_2^2} & \text{if} \quad n \equiv 0 \pmod 2). \end{cases}$$

Recall that a primitive prime divisor of L_k has the property that it is congruent to $\pm 1 \pmod k$. It thus follows that L_v has no primitive divisors. By a version of the Primitive Divisor Theorem first proved by Ward [5] (see also [1]), we get that $v \in \{3, 4, 5, 6, 8, 10, 12\}$. This gives a certain number of possibilities for u. We now need to discuss η. Since $\mathbb{K} \not\subseteq Ł$, it follows that $\mathbb{M}$ is of degree 2 over Ł. Let $\mu = e^{2\pi i/w}$ be a generator of the group of roots of unity in $\mathbb{M}$. Clearly, this group contains ζ. If $\mu = \pm\zeta^j$ for some j, it then follows that $\alpha_1 \in Ł$, therefore $\mathbb{K} \subset Ł$, a contradiction. This shows that $\phi(w) > \phi(v)$, therefore $\phi(w) = [\mathbb{M} : \mathbb{Q}] = 2[Ł : \mathbb{Q}] = 2\phi(v)$. Writing $w = \lambda v$ with some integer λ, the only possibilities are:

(*i*) $\lambda = 2$ and v is even;

(*ii*) $\lambda = 3$ and v is coprime to 3;

(*iii*) $\lambda = 4$ and v is odd;

(*iv*) $\lambda = 6$ and v is coprime to 6.

This gives us a certain number of possibilities for (v, w) so a certain number of possibilities for $(\zeta, \eta) = (e^{2\pi u/v}, e^{2\pi u_1/w})$ where $1 \le u \le v,\ 1 \le u_1 \le w$, $\gcd(u, v) = \gcd(u_1, w) = 1$ and

$$\frac{\alpha_1 - \overline{\zeta}}{\alpha_1 - \zeta} = \eta.$$

The above relation gives us

$$\alpha_1 = \frac{\overline{\zeta} - \zeta\eta}{1 - \eta}. \tag{12}$$

We generated all the numbers appearing on the right–hand side of (12) and checked whether the sum of such a number and its reciprocal (namely, β_1), is an integer. We get a certain number of possibilities for $\alpha_1 + \beta_1 = U_{2k}/U_k$, and then we calculate all possible values for a and k. In fact, all examples have $\alpha_1 + \beta_1 = 4$, and $b_1 = -1$, so $\alpha_1 = 2 + \sqrt{3}$, which is the fundamental unit in $\mathbb{Z} = [\sqrt{3}]$. We get that $k = 1$ and we check that for each $v \in \{3, 4, 6\}$, there exists u such that with $\zeta = e^{2\pi u/v}$, we have that $(\alpha - \overline{\zeta})/(\alpha - \zeta)$ is a root of unity. This is instance (*iv*).

Subcase 2.2 $\mathbb{K} \subseteq \mathbb{L}$.

In this case, we have

$$\frac{\alpha_1 - \overline{\zeta}}{\alpha_1 - \zeta} = \pm\zeta^j \tag{13}$$

for some integer $j \in \{1, \ldots, v\}$. If $j = v$, we get $\alpha - \overline{\zeta} = \pm(\alpha - \zeta)$. This leads to $\zeta = \overline{\zeta}$ (when the sign is $+$), which is not allowed since ζ is not real, or $\alpha = (\zeta + \overline{\zeta})/2 = \cos(2\pi u_1/v)$, which is not possible either since $\alpha > 1$. Thus, $j \ne v$. If $j = v - 1$, we get $(\alpha - \overline{\zeta})/(\alpha - \zeta) = \pm\overline{\zeta}$, which leads to $\alpha \in \{\pm 1\}$, which is not allowed either. So, $j \in \{1, \ldots, v - 2\}$. Let $d_1 = \gcd(j, v)$, and write $j_1 = j/d_1,\ v_1 = v/d_1$. Then $\eta := \pm\zeta^j$ has degree $\phi(v_1)$ over $\mathbb{Q}$. The relation

$$\frac{\alpha_1 - \overline{\zeta}}{\alpha_1 - \zeta} = \eta \qquad \text{leads to} \qquad \eta\zeta^2 + (\alpha_1 - \alpha_1\eta)\zeta - 1 = 0,$$

showing that ζ is of degree at most 2 over $\mathbb{Q}(\alpha, \eta)$, a field of degree at most $2\phi(v_1)$ over $\mathbb{Q}$. It thus follows that $\phi(v) \le 4\phi(v_1) = 4\phi(v/d_1) \le 4\phi(v)/\phi(d_1)$, which gives $\phi(d_1) \le 4$, so $d_1 \le 12$.

A similar argument shows that if we put $d_2 = \gcd(j+1, v)$, then $d_2 \leq 6$. Indeed, to see why, let $v_2 = v/d_2$, put $\eta' = \pm\zeta^{j+1}$, and note that our relation is

$$\frac{\alpha_1 - \overline{\zeta}}{\alpha_1 - \zeta} = \zeta^{-1}\eta', \qquad \text{leading to} \qquad \zeta \in \mathbb{Q}(\eta', \alpha).$$

The last field above has degree at most $2\phi(v_2)$. So, we get the inequalities $\phi(v) \leq 2\phi(v_2) \leq 2\phi(v/d_2) \leq 2\phi(v)/\phi(d_2)$, giving $\phi(d_2) \leq 2$, so $d_2 \leq 6$.

We now need one lemma.

Lemma 6. *Let $N \geq 2$ be a positive integer and $x \geq 1$ be any real number. Let $\phi(x; N) = \#\{1 \leq m \leq x : \gcd(m, N) = 1\}$. Then*

$$\phi(x; N) \geq x\phi(N)/N - \tau(N)/2,$$

where $\tau(N)$ is the number of divisors of N.

Proof. Letting $a(x, d) = \#\{1 \leq m \leq x : d \mid m\}$, by the Principle of Inclusion and Exclusion, it follows that

$$\phi(x; N) = \sum_{d|N} \mu(d)a(x; d).$$

Clearly, $a(x; d) = \lfloor x/d \rfloor = x/d + \zeta_{d,x}$, where $\zeta_{d,x} \in (-1, 0)$. Thus,

$$\phi(x; N) = \sum_{d|N} \mu(d)\left(x/d + \zeta_{d,x}\right) = x\sum_{d|N} \mu(d)/d + \sum_{d|N} \mu(d)\zeta_{d,x}.$$

The "main term" above is $\phi(N)/N$. In the error, we have that $\mu(d) = 1$ for $2^{\omega(N)-1}$ divisors of N, where $\omega(N)$ is the number of distinct prime factors of N. For the remaining divisors, $\mu(d)$ is 0 or negative. Hence,

$$\phi(x; N) \geq x\phi(N)/N - 2^{\omega(N)-1} \geq x\phi(N)/N - \tau(N)/2,$$

which is what we wanted. □

Choose $x := (v^{1/2} + 1 + \tau(v)/2)v/\phi(v)$. Assume that

$$x < v. \tag{14}$$

Then the interval $[1, x]$ is contained in $[1, v]$. Lemma 6 shows that there exist positive integers $x_1 < x_2 < \cdots < x_t$ in $[1, x]$ all coprime to v with $t \geq v^{1/2} + 1$. Now look at $jx_1, \ldots, jx_t$. We claim that they are all distinct modulo v. If not, there exist $i_1 \neq i_2$ such that $j(x_{i_1} - x_{i_2}) \equiv 0 \pmod{v}$.

Canceling d_1, we get that $j_1(x_{i_1} - x_{i_2}) \equiv 0 \pmod{v_1}$. Since j_1 is coprime to v_1, we get

$$v_1 \le |x_{i_1} - x_{i_2}|.$$

The left hand-side above is $v/d_1 \ge v/12$, while the right–hand side above is positive and less than $\max\{x_{i_1}, x_{i_2}\} \le x$. Hence, we get

$$v < 12x. \tag{15}$$

Suppose that v is large enough such that (15) does not hold. Then $jx_1, \ldots, jx_t$ are all distinct modulo v. Since $t > v^{1/2} + 1$, there exists $i_1 \ne i_2$ such that $|jx_{i_1} - jx_{i_2}| \le v^{1/2}$. We now apply to relation (13) the two Galois automorphisms of Ł mapping ζ in $\zeta^{x_{i_1}}$ and $\zeta^{x_{i_2}}$, respectively, getting

$$\frac{\alpha_1^{\varepsilon_1} - \overline{\zeta}^{x_{i_1}}}{\alpha_1^{\varepsilon_1} - \zeta^{x_{i_1}}} = \pm\zeta^{jx_{i_1}} \qquad \text{and} \qquad \frac{\alpha_1^{\varepsilon_2} - \overline{\zeta}^{x_{i_2}}}{\alpha_1^{\varepsilon_2} - \zeta^{x_{i_2}}} = \pm\zeta^{jx_{i_2}}.$$

Here, $\varepsilon_{1,2} \in \{\pm 1\}$. Dividing the above relations side by side we get

$$\frac{(\alpha^{\varepsilon_1}\zeta^{x_{i_1}} - 1)(\alpha^{\varepsilon_2} - \zeta^{x_{i_2}})}{(\alpha^{\varepsilon_1} - \zeta^{x_{i_1}})(\alpha^{\varepsilon_2}\zeta^{x_{i_2}} - 1)} = \zeta^{(j+1)(x_{i_1} - x_{i_2})}. \tag{16}$$

We have $(j+1)(x_{i_1} - x_{i_2})$ is not zero modulo v, since that would imply, by an argument used previously and via the fact that $d_2 \le 2$, that $v < 6x$, which is not the case since (15) does not hold. Expanding (16) we get a polynomial equation which is non-trivial since its free term is either α^{ε_2} or α^{ε_1} according to whether $(j+1)(x_{i_1} - x_{i_2})$ is positive or negative. The degree of this polynomial is at most

$$|j(x_{i_1} - x_{i_2})| + |x_{i_1} - x_{i_2}| + x_{i_1} + x_{i_2} < v^{1/2} + 3x.$$

This is a polynomial for ζ with coefficients in $\mathbb{K}$. Thus, this gives a polynomial relation for ζ with coefficients in $\mathbb{Q}$ of degree at most

$$2v^{1/2} + 6x.$$

Assuming

$$2v^{1/2} + 6x < \phi(v), \tag{17}$$

we get a contradiction. Thus, we get that the only candidates for v are the ones for which at least one of the inequalities

$$\begin{array}{rcl} v & < & 12(v^{1/2} + 1 + \tau(v)/2)v/\phi(v) = 2x \\ \phi(v) & \le & 2v^{1/2} + 6(v^{1/2} + 1 + \tau(v)/2)v/\phi(v) = 2v^{1/2} + 6x \end{array}$$

holds. Using the inequalities $\tau(v) \le \sqrt{3v}$ and

$$v/\phi(v) < 1.79 \log\log v + 2.5/\log\log v$$

(see inequality (3.41) in [4]), we get that the last inequalities above are implied by

$$\begin{array}{lcl} v & < & 12((1+\sqrt{3}/2)v^{1/2}+1)(1.79\log\log v + 2.5/\log\log v); \\ v & < & (2v^{1/2} + 6((1+\sqrt{3}/2)v^{1/2}+1)(1.79\log\log v + 2.5/\log\log v)) \\ & & \times(1.79\log\log v + 2.5/\log\log v), \end{array}$$

and they both imply that $v < 116,000$. A quick computation with Mathematica revealed only 1972 candidates, the largest one being $30,030$. We now checked for each v among these candidates and for each $j \in \{1,\ldots,v-2\}$, whether the number γ satisfying

$$\frac{\gamma - \overline{\zeta_1}}{\gamma - \zeta_1} = \pm\zeta_1^j,$$

with $\zeta_1 = e^{2\pi i/v}$ has the property that $\gamma + 1/\gamma$ is a natural number (note that $\gamma = \alpha_1^{\pm 1}$ according to whether the Galois automorphism of Ł mapping $\zeta = e^{2\pi u/v}$ to $\zeta_1 = e^{2\pi i/v}$ fixes α_1 or sends it into its conjugate $\beta_1 = \alpha_1^{-1}$). No new examples were found.

This completes the proof of this lemma. □

The following is a generalization of Lemma 4 from [3].

For a prime number p and a nonzero integer m, we put $\nu_p(m)$ for the exponent of the prime p in the factorization of m. For a finite set of primes $\mathcal{S}$ and a positive integer m, we put

$$m_{\mathcal{S}} = \prod_{p\in\mathcal{S}} p^{\nu_p(m)}$$

for the largest divisor of m whose prime factors are in $\mathcal{S}$. For any prime number p we put f_p for the index of appearance in the Lucas sequence $\{U_n\}_{n\ge 0}$, which is the minimal positive integer k such that $p \mid U_k$.

Lemma 7. *Let $a \ge 1$. If $\mathcal{S}$ is any finite set of primes and m is a positive integer, then*

$$(U_m)_{\mathcal{S}} \le \alpha^2 m\, \mathrm{lcm}[U_{f_p} : p \in \mathcal{S}].$$

Proof. For a prime p, let f_p be its order of appearance in the Lucas sequence $\{U_n\}_{n\ge 0}$, which is the minimal positive integer k such that $p \mid U_k$. It is well-known that

$$\nu_p(U_m) = \begin{cases} 0 & \text{if} \quad m \not\equiv 0 \pmod{f_p}; \\ \nu_p(U_{f_p}) + \nu_p(m/f_p) & \text{if} \quad m \equiv 0 \pmod{f_p}, \qquad p \text{ is odd}; \\ \nu_2(U_2) + \nu_2(m/2) & \text{if} \quad m \equiv 0 \pmod{2}, \quad p = 2,\ a \equiv 0 \pmod{2}; \\ \nu_2(U_3) & \text{if} \quad m \equiv 3 \pmod{6}, \quad p = 2,\ a \equiv 1 \pmod{2}; \\ \nu_2(U_6) + \nu_2(m/2) & \text{if} \quad m \equiv 0 \pmod{6}, \quad p = 2,\ a \equiv 1 \pmod{2}. \end{cases}$$

In particular, the inequality

$$\nu_p(U_m) \le \nu_p(U_{f_p}) + \nu_p(m) + \delta_{p,2}$$

always holds with $\delta_{p,2}$ being 0 if p is odd or $p = 2$ and a is even and $\nu_2((a^2 + 3b)/2)$ if $p = 2$ and a is odd. We get that

$$\begin{aligned} (U_m)_{\mathcal{S}} &\le \left(\prod_{p\in\mathcal{S}} p^{\nu_p(U_{f_p})} \right) \left(\prod_{\substack{p\mid m \\ p>2}} p^{\nu_p(m)} \right) 2^{\nu_2(m)+\nu_2((a^2+3b)/2} \\ &< \alpha^2 m \operatorname{lcm}[U_{f_p} : p \in \mathcal{S}], \end{aligned}$$

which is what we wanted to prove. For the last inequality above, we used the fact that $2^{\nu_2((a^2+3b)/2)} \le (a^2 + 3b)/2 = (\alpha^2 + \beta^2)/2 < \alpha^2$. □

3 Proof of Theorem 1

We replace s by $\operatorname{lcm}[12, s] \mid 12s$, and as such we may assume that $12 \mid s$. In particular, s is even. If $a < 0$, then we change a to $-a > 0$ leaving b unchanged. Then (α, β) changes to $(-\alpha, -\beta)$ and $U_n(-a, b) = (-1)^{n-1}U_n(-a, b)$. Since s is even, $U_{n+k}^s - U_n^s$ remains unchanged while U_m either remains unchanged or changes sign. Hence, we may assume that $a \ge 1$ without changing the divisibility relation (2). Thus, $\alpha > 1 \ge |\beta| = \alpha^{-1}$. We shall show that

$$m \le \max\{9(n + k), 10000(ks)^2\}, \tag{18}$$

which will imply (4). By the Binet formula (5), we get easily that the inequality

$$\alpha^{n-2} \le U_n \le \alpha^n \quad \text{is valid for all} \quad n \ge 1. \tag{19}$$

We also assume that $m \geq 10000k$. Since U_n is periodic modulo U_m with period $4m$ (Lemma 2), we may assume that $n \leq 4m$. We split U_m into various factors.

Step 1. We put $\mathcal{S} := \{p : p \mid s\}$ and bound $D := (U_m)_{\mathcal{S}}$.

By Lemma 7 and the fact that $f_p \leq p + 1$ for all $p \mid s$, we get

$$D \leq \alpha^2 m \prod_{p|s} U_{p+1} < m\alpha^{2+\sum_{p|s}(p+1)} < \alpha^{s+3+\log m/\log \alpha}, \tag{20}$$

where we used the fact that $\sum_{p|s} p + 1 \leq s + 1$, which is easily proved by induction on the number of distinct prime factors of s.

Step 2. *We put* $A := \gcd\left(U_m, (U_{n+k}^6 - U_n^6)(U_{n+k}^2 + U_n^2)\right)$ *and bound* A.

We certainly have

$$A \leq (U_{n+k}^6 - U_n^6)(U_{n+k}^2 + U_n^2) < 2U_{n+k}^8 < \alpha^{2+8(n+k)}. \tag{21}$$

Step 3. *We put* $E = \dfrac{U_m}{\gcd(AD, U_m)}$, *and bound* E.

We shall estimate the number E by using the fact that E is coprime to $2s$. Write

$$U_{n+s}^s - U_n^s = (U_{n+k}^6 - U_n^6)(U_{n+k}^2 + U_n^2) \prod_{\substack{\zeta:\zeta^s=1 \\ \zeta \notin \{\pm 1, \pm i, \pm\omega, \pm\omega^2\}}} (U_{n+k} - \zeta U_n),$$

where $\omega = e^{2\pi i/3}$. Thus, divisibility (2) tells us in particular that

$$U_m \mid AD \prod_{\substack{\zeta:\zeta^s=1 \\ \zeta \notin \{\pm 1, \pm i, \pm\omega, \pm\omega^2\}}}^{*} (U_{n+k} - \zeta U_n),$$

which shows that

$$E \mid \prod_{\substack{\zeta:\zeta^s=1 \\ \zeta \notin \{\pm 1, \pm i, \pm\omega, \pm\omega^2\}}} (U_{n+k} - \zeta U_n). \tag{22}$$

Let $\mathbb{K} = \mathbb{Q}(e^{2\pi i/s}, \alpha)$, which is a number field of degree d equal to $\phi(s)$ or to $2\phi(s)$. Assume that there are ℓ roots of unity ζ participating in the product appearing in the right–hand side of (22) and label them $\zeta_1, \ldots, \zeta_\ell$. Clearly, $\ell = s - 8$. Write

$$\mathcal{E}_i = \gcd(E, U_{n+k} - \zeta_i U_n) \quad \text{for all} \quad i = 1, \ldots, \ell, \tag{23}$$

where $\mathcal{E}_i$ are ideals in $\mathcal{O}_{\mathbb{K}}$. Then relations (22) and (23) tell us that

$$E\mathcal{O}_{\mathbb{K}} \mid \prod_{i=1}^{\ell} \mathcal{E}_i. \tag{24}$$

Our next goal is to bound the norm $N_{\mathbb{K}/\mathbb{Q}}(\mathcal{E}_i)$ of $\mathcal{E}_i$ for $i = 1, \ldots, \ell$. First of all, $U_m \in \mathcal{E}_i$. Thus, with formula (5) and the fact that $\beta = (-b)\alpha^{-1}$, we get

$$\alpha^m \equiv (-b)^m \alpha^{-m} \pmod{\mathcal{E}_i}.$$

Multiplying the above congruence by α^m, we get

$$\alpha^{2m} \equiv (-b)^m \pmod{\mathcal{E}_i}. \tag{25}$$

We next use formulae (5) and (23) to deduce that

$$(\alpha^{n+k} - (-b)^{n+k}\alpha^{-n-k}) - \zeta(\alpha^n - (-b)^n \alpha^{-n}) \equiv 0 \pmod{\mathcal{E}_i}, \quad (\zeta = \zeta_i).$$

Multiplying both sides above by α^n, we get

$$\alpha^{2n}(\alpha^k - \zeta) - (-b)^{n+k}(\alpha^{-k} - (-b)^k \zeta) \equiv 0 \pmod{\mathcal{E}_i}. \tag{26}$$

Let us show that $\alpha^k - \zeta$ and $\mathcal{E}_i$ are coprime. Assume this is not so and let π be some prime ideal of $\mathcal{O}_{\mathbb{K}}$ dividing both $\alpha^k - \zeta$ and $\mathcal{E}_i$. Then we get $\alpha^k \equiv \zeta \pmod{\pi}$ and so $\alpha^{-k} \equiv (-b)^k \zeta \pmod{\pi}$ by (26). Multiplying these two congruences we get $1 \equiv (-b)^k \zeta^2 \pmod{\pi}$. Hence, $\pi \mid 1 - (-b)^k \zeta^2$. If this number is not zero, then, $(-b)^k \zeta^2$ is a root of unity whose order divides $2s$, so, by Lemma 4, we get that $\pi \mid 2s$, which is impossible because $\pi \mid \mathcal{E}_i \mid E$, and E is an integer coprime to $2s$. If the above number is zero, we get that $\zeta^2 = \pm 1$, so $\zeta \in \{\pm 1, \pm i\}$, but these values are excluded at this step. Thus, indeed $\alpha^k - \zeta$ and $\mathcal{E}_i$ are coprime, so $\alpha^k - \zeta$ is invertible modulo $\mathcal{E}_i$. Now congruence (26) shows that

$$\alpha^{2n+k} \equiv (-b)^n \zeta \left(\frac{\alpha^k - (-b)^k \overline{\zeta}}{\alpha^k - \zeta} \right) \pmod{\mathcal{E}_i}. \tag{27}$$

We now apply Lemma 3 to $a = 2m$ and $b = 2n + k \le 8m + k < 9m$ with the choice $X = 9m$ to deduce that there exist integers u, v not both zero with $\max\{|u|,|v|\} \le \sqrt{X}$ such that $|2mu+(2n+k)v| \le 3\sqrt{X}$. We raise congruence (25) to u and congruence (27) to v and multiply the resulting congruences getting

$$\alpha^{2mu+(2n+k)v} = (-b)^{mu+nv}\zeta^v \left(\frac{\alpha^k - (-b)^k\overline{\zeta}}{\alpha^k - \zeta}\right)^v \pmod{\mathcal{E}_i}.$$

We record this as

$$\alpha^A \equiv \eta \left(\frac{\alpha^k - (-b)^k\overline{\zeta}}{\alpha^k - \zeta}\right)^B \pmod{\mathcal{E}_i} \tag{28}$$

for suitable roots of unity η and ζ of order dividing $2s$ with ζ not of order $1,2,3,4$, or 6, where $A = 2mu+(2n+k)v$ and $B = v$. We may assume that $A \ge 0$, for if not, we replace the pair (u,v) by the pair $(-u,-v)$, thus replacing (A,B) by $(-A,-B)$ and η by η^{-1} and leaving ζ unaffected. We may additionally assume that $B \ge 0$, for if not, we replace B by $-B$ and ζ by $(-b)^k\overline{\zeta}$, again a root of unity of order dividing $2s$ but not of order $1,2,3,4$, or 6 and leave A and η unaffected. Thus, $\mathcal{E}_i$ divides the algebraic integer

$$E_i = \alpha^A(\alpha^k - \zeta_i)^B - \eta_i(\alpha^k - (-b)^k\overline{\zeta_i})^B. \tag{29}$$

Let us show that $E_i \ne 0$. If $E_i = 0$, we then get

$$\alpha^A = \eta_i \left(\frac{\alpha - (-b)^k\overline{\zeta_i}}{\alpha - \zeta_i}\right)^B,$$

and after raising both sides of the above equality to the power $2s$, we get, since $\eta_i^{2s} = 1$, that

$$\alpha^{2sA} = \left(\frac{\alpha^k - (-b)^k\overline{\zeta_i}}{\alpha - \zeta_i}\right)^{2Bs}.$$

Lemma 5 gives us a certain number of conditions all of which have ζ_i or a root of unity of order $1,2,3,4$, or 6, which is not our case. Thus, E_i is not equal to zero. We now bound the absolute values of the conjugates of E_i. We find it more convenient to work with the associate of E_i given by

$$G_i = \alpha^{-\lfloor A/2 \rfloor}E_i = \alpha^{A-\lfloor A/2 \rfloor}(\alpha^k - \zeta_i)^B - \alpha^{-\lfloor A/2 \rfloor}\eta_i(\alpha^k - (-b)^k\overline{\zeta_i})^B.$$

Note that

$$A \le |2m+(2n+k)v| \le 3\sqrt{X} = 9\sqrt{m}, \quad \text{and} \quad B = |v| \le \sqrt{X} = 3\sqrt{m}.$$

Let σ be an arbitrary element of $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. We then have that $\sigma(\eta_i) = \eta_i'$, $\sigma(\zeta_i) = \zeta_i'$, where η_i' and ζ_i' are roots of unity of order dividing $2s$. Furthermore, $\sigma(\alpha) \in \{\alpha, \beta\}$. If $\sigma(\alpha) = \alpha$, we then get

$$\begin{aligned} |\sigma(G_i)| &= |\alpha^{A-\lfloor A/2\rfloor}(\alpha^k - \zeta_i')^B - \eta_i'\alpha^{-\lfloor A/2\rfloor}(\alpha - (-b)^k\overline{\zeta_i'})^B| \\ &\le \alpha^{(A+1)/2}(\alpha^k+1)^B + (\alpha^k+1)^B \\ &\le 2\alpha^{(A+1)/2}(\alpha+1)^{Bk} \le \alpha^{2+(9\sqrt{m}+1)/2+6\sqrt{m}k} \\ &\le \alpha^{11\sqrt{m}k}, \end{aligned} \tag{30}$$

while if $\sigma(\alpha) = \beta$, we also get

$$\begin{aligned} |\sigma(G_i)| &= |\beta^{A-\lfloor A/2\rfloor}(\beta^k - \zeta_i')^b - \beta^{-\lfloor A/2\rfloor}\eta_i'(\beta^k - (-b)^k\overline{\zeta_i'})^B| \\ &\le (\alpha^{-k}+1)^B + \alpha^{A/2}(\alpha^{-k}+1)^B \\ &= \alpha^B + \alpha^{A/2+B} \le 2\alpha^{A/2+B} \le \alpha^{2+4.5\sqrt{m}+6\sqrt{m}} \\ &= \alpha^{11\sqrt{m}k}. \end{aligned}$$

In the above, we used the fact that $\alpha^{-k}+1 \le \alpha^{-1}+1 \le \alpha$. In conclusion, inequality (30) holds for all $\sigma \in G$. Thus, if we write $G_i^{(1)}, \ldots, G_i^{(d)}$ for the d conjugates of G_i in $\mathbb{K}$, we then get that

$$|N_{\mathbb{K}/\mathbb{Q}}(\mathcal{E}_i)| \le |N_{\mathbb{K}/\mathbb{Q}}(E_i)| = |N_{\mathbb{K}/\mathbb{Q}}(G_i)| \le \alpha^{11dk\sqrt{m}},$$

where the first inequality above follows because $\mathcal{E}_i$ divides E_i; hence G_i, and $E_i \ne 0$. Multiplying the above inequalities for $i = 1, \ldots, \ell$, we get that

$$\begin{aligned} E^\ell &= N_{\mathbb{K}/\mathbb{Q}}(E) = N_{\mathbb{K}/\mathbb{Q}}(E\mathcal{O}_\mathbb{K}) \le N_{\mathbb{K}/\mathbb{Q}}\left(\prod_{\substack{i=1\\ \mathcal{E}_i\ne 0}}^{\ell} \mathcal{E}_i\right) \\ &\le \prod_{i=1}^{\ell'} N_{\mathbb{K}/\mathbb{Q}}(G_i) \le \alpha^{11d\ell k\sqrt{m}}, \end{aligned}$$

therefore

$$E \le \alpha^{11kd\sqrt{m}} \le \alpha^{22k\phi(s)\sqrt{m}} < \alpha^{8ks\sqrt{m}}. \tag{31}$$

In the above, we used that $d \le 2\phi(s)$, and $\phi(s) \le s/3$, because $12 \mid s$.

Step 4. *The final inequality.*

Inequality (19) together with estimates (20), (21) and (31), give

$$\alpha^{m-2} \le U_m = DAE \le \alpha^{s+3+\log m/\log\alpha+2+8(n+k)+8ks\sqrt{m}}.$$

Thus,

$$m < (s + 7 + 3\log m) + 8(n + k) + 8ks\sqrt{m}.$$

Since $m \geq 10000$, one checks that $s + 7 + 3\log m < 3ks\sqrt{m}$. Hence,

$$m \leq (s + 7 + 3\log m) + 8(n + k) + 8ks\sqrt{m} < 8(n + k) + 11ks\sqrt{m}. \quad (32)$$

If $m \leq 9(n+k)$, we are through. Otherwise, $n+k \leq m/9$, so (32) implies that $m \leq 8m/9 + 11ks\sqrt{m}$, therefore $m < 100ks\sqrt{m}$, giving $m < 10000(ks)^2$, which is what we wanted to prove.

Acknowledgements

This work was done during a visit of T. K., A. P. and P. S. to the School of Mathematics of the Wits University in September 2015. They thank the School for hospitality and support and Kruger National Park for excellent working conditions. F. L. thanks Professor Igor Shparlinski for some useful suggestions. Work of A. P. was partly financed by Proyect DIUV-REG N° 25-2013.

References

[1] Y. 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.

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

[3] T. Komatsu, F. Luca, Y. Tachiya, "On the multiplicative order of F_{n+1}/F_n modulo F_m", *Integers* **12B** (2012/13), Integers Conference 2011 Proc., #A8, 13pp.

[4] J. B. Rosser, L. Schoenfeld, "Approximate formulas for some functions of prime numbers", *Illinois J. Math.* **6** (1962), 64–94.

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