SIAM J. Comput.
Vol. 31, No. 6, pp. 1896–1908

© 2002 Society for Industrial and Applied Mathematics

LOWER BOUNDS FOR LUCAS CHAINS[*]

MARTIN KUTZ[†]

Abstract. Lucas chains are a special type of addition chains satisfying an extra condition: for the representation $a_k = a_j + a_i$ of each element a_k in the chain, the difference $a_j - a_i$ must also be contained in the chain. In analogy to the relation between addition chains and exponentiation, Lucas chains yield computation sequences for Lucas functions, a special kind of linear recurrences.

We show that the great majority of natural numbers n does not have Lucas chains shorter than $(1-\epsilon)\log_\phi n$ for any $\epsilon > 0$, where ϕ is the golden ratio.

Peter L. Montgomery was the first to consider Lucas chains, in the early eighties. He discovered a decomposition theorem for Lucas chains and a lower bound on their length in terms of Fibonacci numbers. His work was not published. Therefore several of Montgomery's original ideas are represented in this paper.

Key words. Lucas chain, addition chain, Lucas function, lower bound, Fibonacci number, golden ratio, smooth number

AMS subject classifications. 11Y55, 11Y16, 11B39, 11N25, 68Q25

PII. S0097539700379255

1. Introduction.

An increasing sequence $1 = a_0 < a_1 < \cdots < a_r = n$ of integers is called an *addition chain* for n if for each index $k \geq 1$ there exist $i \leq j < k$ so that

$$a_k = a_i + a_j. \tag{1}$$

This notion is motivated by the problem of computing x^n from x with few multiplications, so one is primarily interested in chains of small length r for given n. Since their first appearance in [12], addition chains have been intensively studied. See, for example, Schönhage's lower bound in [13] or Bergeron, Berstel, and Brlek's paper [1] on advanced methods for the construction of short addition chains. We refer to Section 4.6.3 of Knuth's classic [5] for a broader survey.

In this paper, we investigate *Lucas chains*, a variant of addition chains introduced by Peter L. Montgomery [9]. Those are chains for which the indices i, j in (1) can be chosen such that either $i = j$ or the difference $a_j - a_i$ is also part of the chain. The term "Lucas chain" is due to the observation that such chains yield computation sequences for Lucas functions, a special kind of linear recurrences.

Montgomery's paper [9], written in 1983, has never been published; for several years no further research was done on Lucas chains. This changed in 1993 when Smith and Lennon introduced the public-key crypto system *LUC* [14], which is based on Lucas functions. Yen and Laih [16] proposed Lucas chains as a means of evaluating the one-way functions of that crypto system; they used the term "Luc chains," though. Then in 1996 in his Ph.D. thesis on crypto systems [2], Bleichenbacher used results from [9] to actually compute short Lucas chains.

[*] Received by the editors October 9, 2000; accepted for publication (in revised form) June 30, 2002; published electronically October 31, 2002. This work was completed while the author was member of the European graduate school "Combinatorics, Geometry, and Computation" supported by the Deutsche Forschungsgemeinschaft, grant GRK 588/1. Most of this work is part of the author's diploma thesis [6].

http://www.siam.org/journals/sicomp/31-6/37925.html

[†] Mathematisches Institut II, Freie Universität Berlin, Arnimallee 3, 14195 Berlin, Germany (kutz@math.fu-berlin.de).

Besides some elaborate techniques for the construction of short Lucas chains, Montgomery [9] proved lower bounds on the length of Lucas chains for given integers. We will show similar results, reusing several of his ideas. From those bounds we will derive the more general statement that the majority of natural numbers n does not have Lucas chains shorter than $(1-\epsilon)\log_\phi n$ for any $\epsilon > 0$, where ϕ is the golden ratio. Two important prerequisites for this bound are a decomposition theorem stating that any Lucas chain can be uniquely factored into a product of so-called *simple* chains, and a lower bound on the length of these chains in terms of Fibonacci numbers.

The results of this paper are from the author's diploma thesis [6], written in ignorance of Montgomery's work. The author is grateful for Montgomery's kind permission to represent several ideas from his original work.

2. From Lucas functions to Lucas chains. Let P and Q be elements from a commutative ring with identity. The *Lucas functions* $V_n(P,Q)$ are defined recursively by [7]:

$$V_0(P,Q) = 2, \quad V_1(P,Q) = P, \quad V_{n+2}(P,Q) = P \cdot V_{n+1}(P,Q) - Q \cdot V_n(P,Q).$$

If α and β are the roots of the polynomial $X^2 - PX + Q$, then

$$P = \alpha + \beta, \quad Q = \alpha\beta, \quad \text{and} \quad V_n(P,Q) = \alpha^n + \beta^n. \tag{2}$$

In the following we will omit the arguments P, Q and simply write V_n.

We ask for a method to compute V_n for some $n \geq 0$ from a given pair P, Q. Looking at the identities

$$\begin{aligned} V_{m+n} &= (\alpha^m + \beta^m)(\alpha^n + \beta^n) - \alpha^n\beta^m - \alpha^m\beta^n \\ &= (\alpha^m + \beta^m)(\alpha^n + \beta^n) - \alpha^m\beta^m(\alpha^{n-m} + \beta^{n-m}) \\ &= V_m \cdot V_n - Q^m \cdot V_{n-m} \qquad (3) \end{aligned}$$

for $0 \leq m \leq n$, we see that we can compute V_{m+n} from V_m, V_n, V_{n-m}, and a certain power of Q. This gives rise to the following definition.

Definition 1. *A* Lucas chain *for an integer $n \geq 1$ is an increasing sequence*

$$1 = a_0 < a_1 < a_2 < \cdots < a_r = n$$

of integers such that for every $k \in \{1, \ldots, r\}$,

$$\boxed{\text{(L)} \quad \begin{array}{l} \textit{there exist indices } i, j \textit{ with } 0 \leq i \leq j < k \\ \textit{such that } a_k = a_j + a_i \textit{ and } a_j - a_i \in \{0, a_0, a_1, \ldots, a_{k-1}\}. \end{array}}$$

We call r the length *of the chain.*

Example 1. The sequence $(1, 2, 3, 5)$ is a Lucas chain for 5 whereas $(1, 2, 4, 5)$ is not—both are addition chains, though. In the latter sequence, 5 can only be represented as $4 + 1$ but $4 - 1 = 3$ is not part of the sequence.

Example 2. $(1, 2, 4, 8, \ldots, 2^l)$ is a Lucas chain of length l for 2^l. For every k, (L) is satisfied with $i = j = k - 1$.

Example 3. Let the *Fibonacci numbers* F_n be recursively defined by

$$F_0 = 0, \quad F_1 = 1, \qquad \text{and} \qquad F_n = F_{n-1} + F_{n-2}, \quad n \geq 2.$$

For any $l \geq 0$ the sequence $\mathcal{F}_l = (F_2, F_3, F_4, F_5, \ldots, F_{l+2})$ is a Lucas chain of length l for F_{l+2}. To show (L), let $j = k - 1$ and $i = k - 2$; then $F_j - F_i = F_{k-3}$. We call $\mathcal{F}_l$ the *lth Fibonacci chain.*

A Lucas chain for n directly yields a computation of V_n. First, we successively compute Q^{a_k} for $k = 1, \dots, r-1$ with $r-1$ multiplications. Second, we repeatedly use (3) to obtain V_{a_k} for $k = 1, \dots, r$, which takes two multiplications in each step. Thus we can compute V_n from P and Q with $3r-1$ multiplications altogether.

3. Applications. As stated in the introduction, Lucas chains turned out to be useful in public-key cryptography. Instead of using powers $X^n \bmod N$ with some large integer N for the one-way function as in the RSA scheme [11], the LUC crypto system [14] uses the Lucas function $V_n \bmod N$ for encryption and decryption. In this application, the parameter Q is always chosen to be 1 so that powers of Q need not be computed and (3) simplifies to $V_{m+n} = V_m \cdot V_n - V_{n-m}$ (see also [16]). Hence in this special case, a Lucas chain of length r for n yields a computation of V_n with exactly r multiplications in $\mathbb{Z}/N\mathbb{Z}$.

The LUC crypto system stimulated research on Lucas chains [2, 16], but the use of Lucas functions for public-key cryptography had been considered before: Müller and Nöbauer [10] proposed the *Dickson polynomials* $g_n(x, a)$, given by

$$g_n(x,a) = \sum_{0 \le j \le n/2} \frac{n}{n-j} \binom{n-j}{j} (-a)^j x^{n-2j} \qquad \text{for} \quad n \ge 1$$

and $g_0(x, a) = 2$ with some a from a commutative ring with identity, as one-way functions. Waring's formula tells us that [8, p. 355]

$$g_n(P, Q) = \alpha^n + \beta^n = V_n(P, Q)$$

with α, β as in (2). Hence, from this point of view, the LUC system uses the Dickson polynomials $g_n(x, 1)$ for encryption. Müller and Nöbauer argued that it might be difficult to efficiently compute Dickson polynomials for large n, but von zur Gathen [15] used the equation $g_{n+2} = xg_{n+1} - ag_n$ and a matrix representation of this recurrence relation to show that g_n can be computed in $\mathcal{O}(\log n)$ ring operations. Lucas chains can thus be seen as a tool to reduce the multiplicative constant in this asymptotic expression.

Montgomery [9] already pointed out another application of Lucas chains: For every $n \in \mathbb{N}$, the *nth Chebyshev polynomial* T_n is defined as the unique polynomial satisfying

$$T_n(\cos z) = \cos(nz).$$

If we let $\alpha = e^{iz}$ and $\beta = e^{-iz}$, we get $\cos z = (\alpha^n + \beta^n)/2$ and $P = 2\cos z$, $Q = 1$ by (2). Writing $x = \cos z$ then yields [8, p. 355]

$$2T_n(x) = 2\cos(nz) = g_n(2x, 1) = V_n(2x, 1).$$

In other words, these polynomials are just a special case of the Dickson polynomials over the complex numbers. Again we see that we can compute $T_n(x)$ from x with r multiplications if we have a Lucas chain of length r for n.

4. Basic structural properties. For technical reasons we extend the usual notion of Lucas chains to what we call "prechains." They do not alter the capabilities of the original chains but simplify our arguments and proofs in this section.

Definition 2. *A strictly monotonically increasing sequence* $\chi = (a_0, a_1, \dots, a_r)$ *of positive integers is called a* Lucas prechain *if property* (L) *holds for every* $k \in$

$\{1,\ldots,r\}$. *We define* $\operatorname{len}(\chi) := r$ *to be the* length *and* $\operatorname{val}(\chi) := a_r/a_0$ *to be the* value *of the prechain. A prechain of length zero is called* trivial.

Obviously, every Lucas chain for some n is a Lucas prechain with value n. Conversely, it is also easy to see that a prechain is nothing but a scaled Lucas chain. Let $\alpha\chi$ denote the sequence $(\alpha a_0,\ldots,\alpha a_r)$, $\alpha \in \mathbb{Q}_+$. Property (L) is obviously invariant under such scalar multiplications; i.e., a sequence χ of integers is a Lucas prechain iff $c\chi$ is, $c \in \mathbb{N}_+$. Also note that the first element of a prechain divides all others. This follows by induction since (L) implies that a_0 divides a_k if it divides a_i and a_j. Thus we see that values of Lucas prechains are always integers, and scalar multiplication with $1/a_0$ makes any prechain into a chain without changing length or value.

Example 4. The sequence $(6, 12, 18, 30, 48)$ is a Lucas prechain of length 4 for 8. Multiplication with $1/6$ yields the chain $(1, 2, 3, 5, 8)$.

4.1. Multiplying chains. It is a well-known fact that two addition chains for a and b can be combined to yield an addition chain for ab [5, Sect. 4.6.3]. As shown in the proof of Theorem 2 of [9], the same method applies to Lucas chains. We restate it here in terms of prechains.

Definition 3. *Let* $\chi_1 = (a_0,\ldots,a_r)$ *and* $\chi_2 = (b_0,\ldots,b_s)$ *be Lucas prechains with* $a_r = b_0$. *Then their* composition $\chi_1 \circ \chi_2$ *is defined as the sequence* $(a_0,\ldots,a_{r-1}, b_0,\ldots,b_s)$.

We see that the composition of two Lucas prechains is also a Lucas prechain because no element is removed from the original sequences. This concept is easily adapted to chains. We simply have to scale the second chain appropriately.

Definition 4. *Let* χ_1 *and* χ_2 *be Lucas chains. Then their* product $\chi_1 * \chi_2$ *is the Lucas chain* $\chi_1 \circ \operatorname{val}(\chi_1)\chi_2$.

Both operations, $\circ$ and $*$, clearly are associative. The following equations are immediate from the definitions:

$$\operatorname{len}(\chi_1 * \chi_2) = \operatorname{len}(\chi_1) + \operatorname{len}(\chi_2), \tag{4}$$

$$\operatorname{val}(\chi_1 * \chi_2) = \operatorname{val}(\chi_1) \cdot \operatorname{val}(\chi_2). \tag{5}$$

In order to obtain a chain for a composite number $n = ab$, we can thus multiply chains χ_1 and χ_2 for a and b, respectively. As with addition chains, we call this technique the *factor method* [5, p. 463].

Example 5. The product chain $(1, 2, 3) * (1, 2, 3, 5, 7) * (1, 2, 4) = (1, 2, 3, 6, 9, 15, 21, 42, 84)$ is a Lucas chain of length $2 + 4 + 2 = 8$ for $3 \cdot 7 \cdot 4 = 84$.

4.2. Decomposing chains. We shall now identify those chains that can be written as products of smaller chains. The following proposition is essentially equivalent to Theorem 5 and Corollary 6 of [9]. But because of its fundamental importance for the understanding of the structure of Lucas chains, we shall prove it here again, in terms of prechains. It states that for Lucas chains, decomposability is a completely local concept.

Proposition 1. *Let* $\chi = (a_0,\ldots,a_r)$ *be a Lucas prechain and let* $0 \le m < r$. *Then the following two statements are equivalent:*

(i) $a_{m+1} = 2a_m$,

(ii) $\chi^{(m)} := (a_m, a_{m+1},\ldots,a_r)$ *is a Lucas prechain.*

Proof. Assume that (i) holds. We show by induction on $k = m+1,\ldots,r$ that a_m divides a_k and that any pair of indices i, j satisfying (L) fulfills

$$m \le i \le j \qquad \text{and} \qquad a_j - a_i \in \{0, a_m,\ldots,a_{k-1}\}.$$

For $k = m + 1$, property (L) is satisfied with $i = j = m$ only. So let $k > m + 1$ and assume that $a_m | a_l$ for $m \leq l < k$. Let i, j as in (L). We have the implications

$$\begin{aligned} k > m + 1 \ &\Rightarrow\ a_k > a_{m+1} = 2a_m \ \Rightarrow\ a_j > a_m \\ &\Rightarrow\ a_j \geq a_{m+1} = 2a_m \ \Rightarrow\ j \geq m + 1, \end{aligned}$$

hence $a_m | a_j$ by induction. Let us now consider the two cases $a_i \geq a_j/2$ and $a_i < a_j/2$. In the first case we get

$$a_i \geq a_j/2 \ \Rightarrow\ a_i \geq a_m \ \Rightarrow\ i \geq m \ \Rightarrow\ a_m | a_i.$$

Otherwise

$$a_i < a_j/2 \ \Rightarrow\ a_j - a_i > a_j/2 \geq a_m \ \Rightarrow\ a_m | (a_j - a_i);$$

combined with $a_m | a_j$ this yields $a_m | a_i$ and thus $i \geq m$. In both cases a_m divides $(a_j + a_i) = a_k$ as was to be shown.

The implication (ii) ⇒ (i) is immediate from (L). □

Such a pair (a_m, a_{m+1}) of consecutive elements with $a_{m+1} = 2a_m$ is called a *doubling step* [5, p. 467] of the prechain χ. Note that the positions of doubling steps in a prechain are obviously invariant under scaling, i.e., (a, b) is a doubling step of χ iff (ca, cb) is a doubling step of $c\chi$. It is now very easy to identify those chains that are not representable as products.

Definition 5. *We call a Lucas prechain* simple *if it contains exactly one doubling step—its first two elements.*

The Fibonacci chains $\mathcal{F}_l$ from Example 3 are simple for every $l \geq 1$. Note that by definition, trivial prechains are not simple.

The term *simple* is due to Bleichenbacher [2, Chap. 5]. He observed that Lucas chains that cannot be written as nontrivial products are simple. For our lower bounds in section 6, we need to make this notion a little more precise.

Proposition 2. *Let $\chi = (a_0, \ldots, a_r)$ be a nontrivial Lucas prechain and let $(a_{r_\mu}, a_{r_\mu+1})$, $1 \leq \mu \leq d$, be all its doubling steps in increasing order, i.e., $1 = a_{r_1} < a_{r_2} < \cdots < a_{r_d}$. Additionally let $r_{d+1} := r$. Then*

$$\chi_\mu := (a_{r_\mu}, a_{r_\mu+1}, \ldots, a_{r_{\mu+1}})$$

is a simple Lucas prechain for every $\mu \in \{1, \ldots, d\}$. We have $\chi = \chi_1 \circ \ldots \circ \chi_d$ and this decomposition into simple prechains is unique.

Proof. By Proposition 1, every χ_μ is a Lucas prechain because they all start with a doubling step. They are also simple because none of them contains more doubling steps. The equation $\chi = \chi_1 \circ \cdots \circ \chi_d$ is immediate from the definition of the χ_μ. For uniqueness, just observe that by Proposition 1 every prechain χ'_μ of a decomposition into simple prechains has to start with a doubling step of χ. To be simple it must not contain any other of χ's doubling steps. And it is also of strictly positive length since trivial prechains are not simple. □

We can directly restate this result for chains. Defining the empty product to be the trivial chain, we get the following theorem, which very much resembles the proof of Theorem 7 in [9].

Theorem 1. *Every Lucas chain χ has a unique decomposition $\chi = \chi_1 * \cdots * \chi_d$ into simple chains. This induces a factorization*

$$\operatorname{val}(\chi) = \prod_{\mu=1}^{d} \operatorname{val}(\chi_\mu)$$

of its value.

Proof. The statement about the simple chain decomposition is just a reformulation of Proposition 2. The product formula for the values directly follows from equation (5). □

Consequently, the structure of a Lucas chain for some $n \in \mathbb{N}_+$ is intimately related to the prime number factorization of n. Theorem 1 will be very important for our lower bounds in section 6.

5. Trivial bounds.

Since Lucas chains resemble computation sequences, we are interested in shortest chains for a given value.

Definition 6. *For every number $n \in \mathbb{N}_+$ we let*

$$t(n) := \min\{\operatorname{len}(\chi) \mid \chi \textit{ is a Lucas chain for } n\},$$
$$t'(n) := \min\{\operatorname{len}(\chi) \mid \chi \textit{ is a simple Lucas chain for } n\}.$$

A Lucas chain χ is called optimal *if* $\operatorname{len}(\chi) = t(\operatorname{val}(\chi))$.

Note that $t'(1) = \infty$ because any simple chain has value ≥ 2; this will be inconsequential since we shall consider $t'(n)$ for $n \geq 2$ only.

We can already state some basic facts about the function t. Application of the factor method directly yields [9, Thm. 2]

$$t(a \cdot b) \leq t(a) + t(b). \tag{6}$$

Just choose optimal chains χ_1 and χ_2 for a and b, respectively, and compare (4) and (5). Denoting $\log_2$ by lg as usual, we also have the trivial lower bound

$$t(n) \geq \lceil \lg n \rceil \tag{7}$$

because by property (L), no element of a Lucas chain can be more than twice as big as any of its predecessors. Therefore the chains in Example 2 are obviously optimal.

5.1. A known upper bound.

Montgomery developed the following *binary method* [9] for the construction of a Lucas chain for any given odd $n \geq 3$.

Let $d_0, d_1, \ldots, d_k$ be the digits in the binary representation of n, starting from the high end. We let $a_0 := d_0 = 1$ and inductively define

$$a_i = 2a_{i-1} + d_i \qquad \text{for} \quad i = 1, \ldots, k.$$

In other words, a_i has the binary representation $d_0 d_1 \ldots d_i$. Then

$$(a_0, a_0 + 1, a_1, a_1 + 1, \ldots, a_{k-1}, a_{k-1} + 1, a_k)$$

is a Lucas chain for n because the elements a_{i+1} and $a_{i+1} + 1$ can always be written as $2a_i$, $a_i + (a_i + 1)$, or $2(a_i + 1)$ so that the respective differences are either 0 or 1. This chain has no more than $2k + 1$ elements. Thus we get the upper bound

$$t(n) \leq 2\lfloor \lg n \rfloor. \tag{8}$$

By application of the factor method to $a = n/2$ and $b = 2$, this bound also carries over to even n.

Example 6. For $n = 37 = 100101_2$, the binary method yields the Lucas chain $(1, 2, 3, 4, 5, 9, 10, 18, 19, 37)$.

6. Lower bounds. It turns out that the trivial bound (7) can be substantially improved upon. Montgomery showed the following [9, Thm. 7].

Theorem 2 (Montgomery). *Let n be a positive integer with s prime divisors (including multiplicities). Then the number of doubling steps in a Lucas chain for n cannot exceed s, and $n \leq 2^{s-1} F_{t(n)-s+3}$.*

This gives us a lower bound on $t(n)$ for any $n \in \mathbb{N}_+$. The aim of this section is to derive a similar bound that depends on the exact prime number factorization of n and not only on the number of prime factors. That result will then enable us to prove the desired lower bound of $t(n) \geq (1-\epsilon)\log_\phi n$ for the vast majority of integers.

6.1. A lower bound for simple chains. By definition, a simple Lucas chain contains exactly one doubling step. Since these are the most efficient steps available, we expect simple chains to grow notably slower than arbitrary Lucas chains can. The following simple but important lemma, which in different form already appeared in [9], captures this intuition.

Lemma 1. *Let χ be a simple Lucas chain. Then its value is bounded by*

$$\operatorname{val}(\chi) \leq F_{\operatorname{len}(\chi)+2}.$$

Proof. Since every Lucas chain is also an addition chain, we may apply Theorem A from [5, p. 467]. Letting $d = 1$ there immediately yields the stated inequality. □

In order to rephrase Lemma 1 in terms of the function t', we reinterpret it in the following way: *The average growth of a simple Lucas chain of length k is no more than a factor of $\sqrt[k]{F_{k+2}}$ per step.*

Definition 7. *For any integer $n \geq 2$, let $k := \min\{l \mid n \leq F_{l+2}\}$ and define*

$$\Phi(n) := \sqrt[k]{F_{k+2}}.$$

Indeed, this is a useful notion. We obtain the following bound.

Proposition 3. *For every $n \geq 2$, we have*

$$t'(n) \geq \frac{\lg n}{\lg \Phi(n)}.$$

Proof. Let k be the unique integer that satisfies $F_{k+1} < n \leq F_{k+2}$. Then by Lemma 1, any simple chain for n has length at least k. Thus

$$t'(n) \geq k \geq \frac{\lg n}{\lg F_{k+2}} k = \frac{\lg n}{\lg \sqrt[k]{F_{k+2}}} = \frac{\lg n}{\lg \Phi(n)}. \qquad \square$$

6.2. From simple chains to arbitrary chains. Theorem 1 now tells us how to obtain a bound for $t(n)$ from Proposition 3. Any chain for n can be factored into simple chains, and the values of these factors are restricted by the possible (partial) factorizations of the integer n. Hence, we can apply Proposition 3 to all those factorizations and get

$$t(n) \geq \min\left\{ \sum_{i=1}^{d} \frac{\lg f_i}{\lg \Phi(f_i)} \;\middle|\; \prod_{i=1}^{d} f_i = n \right\}. \tag{9}$$

We can already use this formula to achieve nontrivial bounds on $t(n)$ for certain values of n.

Example 7. The prime factors of $n = 85$ are 5 and 17. Proposition 3 yields $t'(5) \geq 3$, $t'(17) > 5.5$, and $t'(85) > 8.9$. Since $(1, 2, 3, 5) * (1, 2, 3, 5, 7, 10, 17)$ is a chain of length 9 for 85, we obtain $t(85) = 9$.

So this technique yields useful results, but it may become impractical due to the combinatorial explosion in cases where n has many factors. In the following we shall see how this drawback can be overcome. The key observation is that short simple chains are potentially more efficient than long ones because the shorter the chain the greater the effect of the initial doubling step on the average growth of the chain. In fact, Proposition 3 already captures this behavior in a very satisfying way. We shall see that it is sufficient to apply it only to the prime number factorization of n. In order to prove this formally, we need some basic facts about the function Φ.

6.3. Properties of the function Φ. The Fibonacci numbers are closely related to the golden ratio

$$\phi = \frac{1 + \sqrt{5}}{2},$$

and we have the well-known formula [4, p. 83]

$$F_k = \frac{1}{\sqrt{5}} \left(\phi^k - \hat{\phi}^k \right),$$

where $\hat{\phi} = 1 - \phi = \frac{1}{2}(1 - \sqrt{5})$. Since $\hat{\phi} = -\phi^{-1}$, we can restate this as

$$F_k = \frac{1}{\sqrt{5}} \left(\phi^k - (-\phi)^{-k} \right), \tag{10}$$

which will better suit our needs.

Lemma 2. *For all $k \geq 1$ we have*

$$\sqrt[k+1]{F_{k+3}} < \sqrt[k]{F_{k+2}}.$$

Proof. We first raise both sides of the inequality to the $k(k+1)$st power and apply (10); thus we get

$$\begin{aligned} & \left[\tfrac{1}{\sqrt{5}} \left(\phi^{k+3} - (-\phi)^{-k-3} \right) \right]^k < \left[\tfrac{1}{\sqrt{5}} \left(\phi^{k+2} - (-\phi)^{-k-2} \right) \right]^{k+1} \\ \Leftrightarrow\ & \sqrt{5} \left[\left(1 + (-1)^k \phi^{-2k-6} \right) \phi^{k+3} \right]^k < \left[\left(1 + (-1)^{k+1} \phi^{-2k-4} \right) \phi^{k+2} \right]^{k+1} \\ \Leftrightarrow\ & \sqrt{5}\, \phi^{-2} < \left(1 + (-1)^{k+1} \phi^{-2k-4} \right)^{k+1} \left(1 + (-1)^k \phi^{-2k-6} \right)^{-k}. \end{aligned} \tag{11}$$

Numerical computation of the left-hand side of (11) yields $\sqrt{5}\, \phi^{-2} < 0.86$. If k is odd, the right-hand side is greater than one and hence (11) follows. If k is even, the right-hand side of (11) equals

$$\begin{aligned} & \left(1 - \phi^{-2k-4} \right)^{k+1} \left(1 + \phi^{-2k-6} \right)^{-k} \\ & \quad > \left(1 - \phi^{-2k-4} \right)^{k+1} \left(1 - \phi^{-2k-6} \right)^{k} \\ & \quad > \left(1 - \phi^{-2k-4} \right)^{2k+1} \\ & \quad > 1 - (2k+1)\, \phi^{-2k-4}, \end{aligned}$$

where the last step is by application of the Bernoulli inequality. Now

$$h(x) := 1 - (2x+1)\,\phi^{-2x-4} > \sqrt{5}\,\phi^{-2} \qquad \text{for} \quad x \geq 2$$

since numerical computation for $x = 2$ yields $1 - 5\,\phi^{-8} > 0.89 > \sqrt{5}\,\phi^{-2}$ and

$$h'(x) = \big((2x+1)\ln\phi^2 - 2\big)\phi^{-2x-4} > 0 \qquad \text{for} \quad x \geq 2. \qquad \square$$

Lemma 3. *The sequence* $(\Phi(n))_{n\geq 2}$ *is monotonically decreasing. It converges towards the golden ratio:*

$$\lim_{n\to\infty} \Phi(n) = \phi.$$

Proof. The first statement is a direct consequence of Lemma 2. Equation (10) yields

$$\sqrt[k]{F_{k+2}} = \sqrt[k]{\tfrac{1}{\sqrt{5}}\big(\phi^{k+2} - (-\phi)^{-k-2}\big)} = \phi \cdot \sqrt[k]{\tfrac{\phi^2}{\sqrt{5}}\big(1 \pm \phi^{-2k-4}\big)},$$

and so the second statement follows. □

6.4. The lower bound in closed form. We are now able to prove a lower bound for $t(n)$ that does not suffer from the combinatorial explosion of the rule (9).

Theorem 3. *Let* n *be any positive integer, and let* $n = \prod_1^e p_i$ *be its factorization into prime numbers. Then we have*

$$t(n) \geq \sum_1^e \frac{\lg p_i}{\lg \Phi(p_i)}.$$

Proof. Let χ be an optimal chain for n and let $\chi_1 * \cdots * \chi_d$ be its decomposition into simple chains. We let $n_\mu := \mathrm{val}(\chi_\mu)$ be their corresponding values. Since $n = n_1 \cdots n_d$, there exists a partition $I_1, \ldots, I_d$ of the index set $\{1, \ldots, e\}$ so that

$$n_\mu = \prod_{i \in I_\mu} p_i$$

for every $\mu \in \{1, \ldots, d\}$. Since χ is optimal, every χ_μ must also be optimal. Thus, by (4) and Proposition 3 we have

$$\begin{aligned} t(n) &= \sum_{\mu=1}^d t(n_\mu) = \sum_{\mu=1}^d t'(n_\mu) \\ &\geq \sum_{\mu=1}^d \frac{\lg n_\mu}{\lg \Phi(n_\mu)} = \sum_{\mu=1}^d \sum_{i\in I_\mu} \frac{\lg p_i}{\lg \Phi(n_\mu)} \\ &\geq \sum_{\mu=1}^d \sum_{i\in I_\mu} \frac{\lg p_i}{\lg \Phi(p_i)} = \sum_{i=1}^e \frac{\lg p_i}{\lg \Phi(p_i)}, \end{aligned}$$

where the penultimate step makes use of Lemma 3. □

Theorem 3 is a powerful and also practical tool for proving Lucas chains optimal. Let us again consider the chain from Example 5. The prime number factorization is

$84 = 2^2 \cdot 3 \cdot 7$. We have

$$\begin{aligned} t(84) &\geq 2\,\frac{\lg 2}{\lg \Phi(2)} + \frac{\lg 3}{\lg \Phi(3)} + \frac{\lg 7}{\lg \Phi(7)} \\ &= 2\,\frac{\lg 2}{\lg 2} + \frac{\lg 3}{\lg \sqrt{3}} + \frac{\lg 7}{\lg \sqrt[4]{8}} > 7.7, \end{aligned}$$

and thus $t(84) = 8$.

6.5. Comparison of the bounds. Since we used methods similar to those of Montgomery, the bounds from Theorem 3 are close to those from Theorem 2. For example, the latter also yields $t(84) \geq 8$, as we have computed from the former. But there are also cases in which the former is slightly better than the latter. As an example consider $n = 177$, where we get the lower bounds 11, which is the precise value of $t(177)$, and 10, respectively. The main advantage of Theorem 3, however, is its dependence on the prime factors of n and its implicit relation to the golden ratio through the function Φ. This will enable us to derive the general lower bound in the subsequent section.

7. A general lower bound. By now we have considered only concrete lower bounds for individual values. In this section we are going to show that the great majority of numbers n does not have Lucas chains shorter than $(1-\epsilon)\log_\phi n$ for any given $\epsilon > 0$.

For this, observe that our bound from Theorem 3 is closer to $\log_\phi n$ if n contains many large prime factors. The next definition captures this notion.

Definition 8. *Let n be any positive integer with prime number factorization $n = \prod_1^e p_i$. Let $B \in \mathbb{N}_+$ and $\delta \in (0, 1]$. We call n a (B, δ)-*fat *number if*

$$\prod_{p_i \leq B} p_i < n^\delta,$$

*that is, it contains less than a δ-portion (logarithmically) of factors smaller than B. We call n (B, δ)-*smooth *if it is not (B, δ)-fat.*

The term "smooth number" is generally used for integers that contain no prime factors larger than a certain bound B. Note that this is just the special case $\delta = 1$ in the above definition.

As expected, it turns out that fat numbers cannot have short Lucas chains.

Lemma 4. *Let n be a (B, δ)-fat integer, $B \geq 2$. Then we have*

$$t(n) \geq \frac{1-\delta}{\lg \Phi(B)} \lg n.$$

Proof. Let $\prod_1^e p_i$ be the factorization of n into prime numbers, and let

$$\begin{aligned} S &:= \{i \mid p_i \leq B\}, \\ L &:= \{i \mid p_i > B\} \end{aligned}$$

denote the collection of small and large factors indices, respectively. By Theorem 3 we have

$$\begin{aligned} t(n) &\geq \sum_{i\in S\cup L} \frac{\lg p_i}{\lg \Phi(p_i)} \geq \sum_{i\in L} \frac{\lg p_i}{\lg \Phi(p_i)} \\ &\geq \sum_{i\in L} \frac{\lg p_i}{\lg \Phi(B)} = \frac{1}{\lg \Phi(B)} \lg \prod_{i\in L} p_i \\ &> \frac{\lg n^{1-\delta}}{\lg \Phi(B)} = \frac{1-\delta}{\lg \Phi(B)} \lg n, \end{aligned}$$

where the last line follows from the (B,δ)-fatness of n. Note that we had to exclude $B = 1$ since $\Phi(1)$ is not defined. □

We want to know how many numbers are not of this kind; that is, how frequent are (B,δ)-smooth numbers for given B and δ? While much is known about the frequency of the "ordinary" smooth numbers with $\delta = 1$ (see, for example, [3]), our relaxed notion of smoothness has not yet been investigated. The following lemma gives us satisfactory estimates on the density of (B,δ)-smooth numbers. We let $[N, M] := \{n \in \mathbb{Z} \mid N \leq n \leq M\}$ denote the set of integers between N and M, and let $\pi(x)$ as usual count the numbers of primes less than or equal to x.

LEMMA 5. *For every bound $B \in \mathbb{N}_+$, every $\delta \in (0,1)$, and every $N \in \mathbb{N}_+$, the interval $[N, 2N-1]$ contains fewer than*

$$\left(N^{1-\delta} + 1\right)\binom{\delta \lg N + \lg B + \pi(B)}{\pi(B)}$$

(B,δ)-smooth numbers.

Proof. Let n be any (B,δ)-smooth number from the interval $[N, 2N-1]$, and let $\prod_1^e p_i$ be its factorization into prime numbers. Let $S := \{i \mid p_i \leq B\}$ be the collection of its small factors indices. Then we have

$$\prod_{i\in S} p_i \geq n^\delta \geq N^\delta$$

since n is (B,δ)-smooth. We can successively remove indices from S to obtain a subset $S' \subseteq S$ that satisfies

$$N^\delta \leq f := \prod_{i\in S'} p_i < BN^\delta.$$

Hence, every (B,δ)-smooth number in the interval $[N, 2N-1]$ has such a divisor f. Any such f is of the form

$$f = 2^{\sigma_2} 3^{\sigma_3} 5^{\sigma_5} \ldots p^{\sigma_p},$$

where p is the greatest prime less than or equal to B. Since $f < BN^\delta$, all of the σ's are less than $\lg(BN^\delta)$. Thus, there are fewer than

$$\binom{\lg(BN^\delta) + \pi(B) - 1}{\pi(B) - 1} < \binom{\delta \lg N + \lg B + \pi(B)}{\pi(B)}$$

such f's. Every single $f \geq N^\delta$ divides no more than $N/N^\delta + 1$ numbers in the range $[N, 2N-1]$, and hence the statement of the lemma follows. □

Now we are prepared to prove the announced asymptotic lower bound for Lucas chains.

THEOREM 4. *For any $\epsilon > \rho > 0$ and increasing $N \in \mathbb{N}_+$, there are only $\mathcal{O}(N^{1-\rho})$ numbers $n \in [N, 2N-1]$ satisfying*

$$t(n) \leq (1-\epsilon)\log_\phi n,$$

where the constants hidden in the $\mathcal{O}$ depend on ϵ and ρ.

Proof. Let $\delta := (\epsilon+\rho)/2$ and choose an integer B so that

$$\lg \Phi(B) \leq \frac{\lg \phi}{1-\frac{\epsilon-\rho}{2}};$$

by Lemma 3 such a B exists. Now Lemma 4 yields

$$t(n) > \frac{1-\delta}{\lg \Phi(B)} \lg n \geq (1-\delta)\Big(1-\frac{\epsilon-\rho}{2}\Big)\log_\phi n > (1-\epsilon)\log_\phi n$$

for any (B,δ)-fat integer n. Thus, only (B,δ)-smooth numbers can have shorter chains, but by Lemma 5 there are no more than

$$\big(N^{1-\delta}+1\big)\binom{\delta \lg N + \lg B + \pi(B)}{\pi(B)} \in \mathcal{O}\big(N^{1-\rho}\big)$$

of these in any interval $[N, 2N-1]$. □

8. Final remarks. Since $\log_\phi n \approx 1.44 \lg n$, Theorem 4 is a significant improvement on the trivial bound (7). But we may ask how close this comes to the optimum. Examples 5 and 7 show that there are cases in which our bounds are extremely sharp. Yet, the majority of numbers could still need chains much longer than Theorem 4 indicates.

We strongly believe that this is not the case. Comparison of the concrete bounds from Theorem 3 with heuristic computations of short chains for the first million natural numbers suggests that our bound is very sharp. It turned out that for all $n \leq 10^6$ we have

$$t(n) \leq \left\lceil \sum_1^e \frac{\lg p_i}{\lg \Phi(p_i)} \right\rceil + 2,$$

where $n = \prod_1^e p_i$ is the prime number factorization of n.

It seems that Theorem 4 already captures the behavior of the function t in a most fundamental way.

CONJECTURE 1. *The length function t satisfies*

$$\limsup \frac{t(n)}{\lg n} = \frac{1}{\lg \phi}.$$

In fact, Montgomery already asked in Problem 2 of [9] whether this upper bound holds. And in a private communication Donald E. Knuth conjectured the slightly stronger bound of $t(n) \leq \log_\phi n + \mathcal{O}(1)$. Nevertheless, I do not expect Conjecture 1 to be shown in the near future. Though the heuristics have produced good results, it seems to be very hard to actually prove any significantly better upper bound than (8). By now we are not even able to show $t(n) \leq \alpha \lg n$ for any $\alpha < 2$.

Acknowledgments. I thank my editor Joachim von zur Gathen for pointing me to Montgomery's paper and for many constructive hints. And I am very grateful for Peter L. Montgomery's permission to represent his results. I also want to thank Donald E. Knuth, who supplied me with a list of precise values of $t(n)$, for his encouragement. Above all, I am indebted to my teacher Arnold Schönhage for his friendly support and valuable advice.

REFERENCES

[1] F. Bergeron, J. Berstel, and S. Brlek, *Efficient computation of addition chains*, J. Théor. Nombres Bordeaux, 6 (1994), pp. 21–38.

[2] D. Bleichenbacher, *Efficiency and Security of Cryptosystems Based on Number Theory*, Ph.D. thesis, Swiss Federal Institute of Technology, Zürich, 1996.

[3] A. Hildebrand, *On the number of positive integers $\leq x$ and free of prime factors $> y$*, J. Number Theory, 22 (1986), pp. 298–307.

[4] D. E. Knuth, *The Art of Computer Programming*, Vol. 1, 3rd ed., Addison–Wesley, Reading, MA, 1997.

[5] D. E. Knuth, *The Art of Computer Programming*, Vol. 2, 3rd ed., Addison–Wesley, Reading, MA, 1998.

[6] M. Kutz, *Grundlegende Betrachtungen zu einer Variante von Additionsketten*, Diploma thesis, Rheinische Friedrich-Wilhelms-Universität Bonn, Germany, 2000 (in German).

[7] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math., 31 (1930), pp. 419–448.

[8] R. Lidl and H. Niederreiter, *Finite Fields*, Addison–Wesley, Reading, MA, 1983.

[9] P. L. Montgomery, *Evaluating Recurrences of Form $X_{m+n} = f(X_m, X_n, X_{m-n})$ via Lucas Chains*, manuscript, 1992. Available via ftp from ftp://ftp.cwi.nl/pub/pmontgom/Lucas.ps.gz.

[10] W. B. Müller and W. Nöbauer, *Some remarks on public-key cryptosystems*, Studia Sci. Math. Hungar., 16 (1981), pp. 71–76.

[11] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Comm. ACM, 21 (1978), pp. 120–126.

[12] A. Scholz, *Aufgabe* 253, in Jahresbericht der Deutschen Mathematikervereinigung, Vol. 47, Teil II, B. G. Teubner, Leipzig and Berlin, 1937, pp. 41–42 (in German).

[13] A. Schönhage, *A lower bound for the length of addition chains*, Theoret. Comput. Sci., 1 (1975), pp. 1–12.

[14] P. J. Smith and M. J. J. Lennon, *LUC: A new public key system*, in Proceedings of the 9th IFIP International Symposium on Computer Security, E. G. Dougall, ed., Elsevier, New York, 1993, pp. 97–110.

[15] J. von zur Gathen, *Tests and Algorithms for Permutation Polynomials*, Tech. report, Department of Computer Science, The Australian National University, Canberra, 1989.

[16] S.-M. Yen and C.-S. Laih, *Fast algorithms for LUC digital signature computation*, IEE Proceedings - Computers and Digital Techniques, 142 (1995), pp. 165–169.