Monatshefte für Mathematik
https://doi.org/10.1007/s00605-019-01354-x

A primality test for $4Kp^n - 1$ numbers

J. M. Grau[1] · A. M. Oller-Marcén[2] · D. Sadornil[3]

Received: 13 September 2018 / Accepted: 15 November 2019

Abstract
We present a Lucasian type primality test, not explicitly based on Lucas sequences, for numbers written in the form $N = 4Kp^n - 1$. This test is a generalization of the classical Lucas–Lehmer test for Mersenne numbers using as underlying group $\mathcal{G}_N := \{z \in (\mathbb{Z}/N\mathbb{Z})[i] : z\overline{z} \equiv 1 \pmod{N}\}$.

Keywords Proth numbers · Primality test · Lucas sequences · Lucasian primality test

Mathematics Subject Classification 11A51 · 11Y11 · 11Y40

1 Introduction

The Lucas–Lehmer test for Mersenne numbers given in Theorem 1 is the primality test most often used to locate large primes. This search has been successful in locating many of the largest primes known to date [7].

Communicated by Ilse Fischer.

Daniel Sadornil is partially supported by the Spanish Government under projects MTM2014-55421-P and MTM2017-83271-R.

✉ A. M. Oller-Marcén
oller@unizar.es

J. M. Grau
grau@uniovi.es

D. Sadornil
daniel.sadornil@unican.es

[1] Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo, s/n, 33007 Oviedo, Spain

[2] Centro Universitario de la Defensa, Ctra. de Huesca, s/n, 50090 Zaragoza, Spain

[3] Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Avda de los Castros s/n, 39005 Santander, Spain

Published online: 25 November 2019

Theorem 1 *Let $M_p = 2^p - 1$ be the Mersenne number with p an odd prime and let be the following sequence $S_0 = 4$, $S_n = S_{n-1}^2 - 2 \bmod M_p$.*

$$M_p \text{ is prime if and only if } S_{p-2} \equiv 0 \pmod{M_p}$$

Many authors, including Lucas [13] and Lehmer [11], have developed so-called Lucasian type primality tests; i.e., primality criteria for numbers written in a specific form and based on the use of a recursive sequence.

For example, for numbers written in the form $N = k2^n - 1$ with $2^n > k$, Riesel test [14] states that N is prime if and only if $S_{n-2} \equiv 0 \pmod N$, with $S_i = S_{i-1}^2 - 2$ and a particular S_0 which depends on n and k (if $k = 3$ and $n \equiv 0$ or $3 \pmod 4$, then $S_0 = 5778$; if $k \equiv 1$ or $5 \pmod 6$ and $3 \nmid n$, then we take $S_0 = (2+\sqrt{3})^k + (2-\sqrt{3})^k$).

For numbers written in the form $N = k2^n - 1$, we can also cite the works by Stechkin [19], Rödseth [15], Berrizbeitia and Berry [2], Sun [21] or Deng and Huang [6]. If we consider numbers written in the form $N = k3^n - 1$, Williams and Zarnke [24], Bosma [3] or Berrizbeitia and Berry [1] have proposed Lucasian type primality tests. There are also some other generalizations for numbers written in the form $N = kp^n - 1$ with $p = 5, 7$ and even general p prime [5,17,20,22].

For all the aforementioned Lucasian type primality tests for numbers written in the form $N = kp^n - 1$, the initial value S_0 in the sequence depends on N and, more specifically, on particular properties of k and n. In general, there is no S_0 valid for all N in the considered family.

It is natural to ponder if it is really important to have a necessary and sufficient primality condition. An alternative would be to avoid the necessity in order to obtain a laxer sufficient condition independent of k and n, assuming a small risk of having to repeat the test in the unlikely case that it could not confirm or discard primality. This idea was already successfully explored in [8] for numbers written in the form $N = Kp^n + 1$, with the following result:

Proposition 1 *Let $N = Kp^n + 1$ where p is a prime number. Let us consider the sequence $S_0 = 2^K$ and $S_i = S_{i-1}^p$ for all $i \geq 1$. If for some $j > \frac{1}{2}(\log_p(K) + n)$ it holds that $\gcd(S_{j-1} - 1, N) = 1$ and $S_j \equiv 1 \pmod N$, then N is prime.*

In this work, we present a similar result regarding numbers written in the form $N = K2^n - 1$ and, more generally, in the form $N = 4Kp^n - 1$. The setting for this work is the group $\mathcal{G}_N := \{z \in (\mathbb{Z}/N\mathbb{Z})[i] : z\overline{z} \equiv 1 \pmod N\}$, whose properties were analyzed in [9]. Other authors have addressed primality tests for particular types of numbers (including the ones we deal with in this work) that include the explicit use of Lucas sequences [16]. Our treatment is quite similar in the background, but we adopt a novel and original presentation.

2 A generalization of Miller–Rabin primality test

Given a positive integer N, we consider the group

$$\mathcal{G}_N := \{a + bi \in (\mathbb{Z}/N\mathbb{Z})[i] : a^2 + b^2 \equiv 1 \pmod N\}.$$

Note that $\mathcal{G}_N$ is the unit circle modulo N over the Gaussian integers and is a very special case of the so called *Pell Conics* [12]. In [9] some number-theoretical concepts and properties related to these groups were introduced and studied. In particular, if $p \equiv 3 \pmod 4$ is a prime; i.e., if p remains prime in the ring of Gaussian integers, then $|\mathcal{G}_p| = p + 1$ and the following result holds [9, Proposition 3.1]

Proposition 2 *Let $p \equiv 3 \pmod 4$ be a prime number and let z be a Gaussian integer such that p is coprime with $z\overline{z}$. Then, $(z/\overline{z})^{p+1} \equiv 1 \pmod p$.*

This proposition can be seen as a compositeness test for integers. Given a positive integer $N \equiv 3 \pmod 4$, if we find a Gaussian integer z with $\gcd(N, z\overline{z}) = 1$ and such that $(z/\overline{z})^{N+1} \not\equiv 1 \pmod N$ then N is a composite number. Nevertheless, like in the classical setting, the converse is not always true. This fact motivates the following definition.

Definition 1 A composite integer $N \equiv 3 \pmod 4$ is called a *Gaussian Fermat pseudoprime (GFP) with respect to the base $z \in \mathbb{Z}[i]$* if $\gcd(N, z\overline{z}) = 1$ and $(z/\overline{z})^{N+1} \equiv 1 \pmod N$.

As we have shown in [9], there is no number $N = 4k + 3 < 10^{18}$ such that N is simultaneously a Fermat pseudoprime with respect to the base 2 and a GFP with respect to the base $z = 1 + 2i$.

Miller–Rabin probabilistic primality test applies to integers written in the form $N = K2^n + 1$. It is based on Fermat's little theorem and on the fact that, if p is prime, the only solutions to $x^2 \equiv 1 \pmod p$ are $x \equiv \pm 1$. In our Gaussian setting, if we use Proposition 2 instead of Fermat's little theorem, this idea can be easily extended to integers written in the form $N = K2^n - 1$. In fact, the next theorem easily follows (it is interesting to compare it with [4, Theorem 3.5.1.]).

Theorem 2 *Let $N = K2^n - 1$ be a prime number with $n > 1$ and K odd. If z is a Gaussian integer such that $\gcd(N, z\overline{z}) = 1$, then one of the following holds:*

(i) $(z/\overline{z})^K \equiv 1 \pmod N$.
(ii) *There exists $0 \le j < n$ such that $(z/\overline{z})^{K2^j} \equiv -1 \pmod N$.*

In the same way, we can further extend this result to integers written in the form $N = 4Kp^n - 1$ in order to obtain a result similar to [8, Theorem 3.2]

Theorem 3 *Let $N = 4Kp^n - 1$ be a prime with p an odd prime number and $n \ge 1$. If $z \in \mathbb{Z}[i]$ is a Gaussian integer such that $\gcd(N, z\overline{z}) = 1$, then one of the following holds:*

(i) $(z/\overline{z})^{4K} \equiv 1 \pmod N$.
(ii) *There exists $0 \le j < n$ such that $\Phi_p((z/\overline{z})^{4Kp^j}) \equiv 0 \pmod N$.*

These results can be seen as probabilistic primality tests and they lead to the following definition which generalizes, in this Gaussian setting, Definition 3.3 from [8].

Definition 2 Given a prime p, $n \geq 1$ and K odd, the number $N = 4Kp^n - 1$ ($N = K2^n - 1$, $n \geq 2$, in the case $p = 2$) is a *p-Gaussian strong probable prime to base z* if it satisfies conditions (i) or (ii) of Theorem 3 (of Theorem 2, in the case $p = 2$) above. If, in addition, it is a composite number, then it is a *p-Gaussian strong pseudoprime to base z*.

As in the classical setting, every p-Gaussian strong pseudoprime to base z is also a Gaussian Fermat pseudoprime with respect to the same base z. For instance, up to 10^6, there are eighteen 2-Gaussian strong pseudoprimes to base $1 + 2i$ while there are seventy five Gaussian Fermat pseudoprimes. On the other hand, in comparison with its classical counterpart, this notion is less restrictive. For instance, up to 10^6, there are only 3 (resp. 9, 6, 6) strong pseudoprimes of the form $K2^n - 1$, $n \geq 2$, with respect to the base 2 (resp. 3, 5 or 7).

3 Primality test for numbers written in the form $4Kp^n - 1$

In what follows we will use the notation from the previous section. Given an integer written in the form $N = 4Kp^n - 1$ and $w \in \mathcal{G}_N$, Definition 2 states that N is a p-Gaussian strong probable prime to base w if either the finite sequence

$$w^{4K}, w^{4Kp}, w^{4Kp^2}, \ldots, w^{4Kp^n}$$

is constantly 1 modulo N or its last element different from 1 is a root of the cyclotomic polynomial Φ_p modulo N. Now, we establish a condition over the index in which this holds in order to certify the primality of N.

Proposition 3 *Let $N = 4Kp^n - 1$ be an integer with p an odd prime and let w be a Gaussian integer such that $w \in \mathcal{G}_N$. Assume that there exists $1 \leq j \leq n$ such that:*

(i) $\Phi_p(w^{4Kp^{j-1}}) \equiv 0 \pmod{N}$,
(ii) $2j \geq \log_p(4K) + n$.

Then, N is prime.

Proof Put $X = w^{4K}$, then $\Phi_p(X^{p^{j-1}}) \equiv 0 \pmod{N}$. Suppose N is composite and let q be a prime divisor of N with $q \leq \sqrt{N}$. Then $\Phi_p(X^{p^{j-1}}) \equiv 0 \pmod{q}$ and $X^{p^j} \equiv 1 \pmod{q}$. Thus, the order of X in $\mathcal{G}_q$ is a divisor of p^j, but if $X^{p^s} \equiv 1 \pmod{q}$ with $s < j$ it would imply that $p = \Phi_p(1) \equiv \Phi_p(X^{p^s}) \equiv \Phi_p(X^{p^{j-1}}) \equiv 0 \pmod{q}$ which is clearly a contradiction. Consequently, since $X \in \mathcal{G}_q$, it follows that p^j divides $|\mathcal{G}_q| = q \pm 1$ (depending on whether $q \equiv \mp 1 \pmod 4$, see [9, Proposition 2.1]). Since p, q are odd primes, it is not possible that $p^j = q$ or $p^j = q + 1$. Hence, it must be $p^j < q \leq \sqrt{N}$ from which it follows that $p^{2j} < N = 4Kp^n - 1$. But, in this case, $2j < \log_p(4K) + n$. This is a contradiction with the size of j. □

Remark 1 Note that condition $2j \geq \log_p(4K) + n$ holds only if $4K \leq p^n$. Hence, the previous result can certify primality only if $4K \leq p^n$. Also, since we know that

$\Phi_p(x)(x-1) = x^p - 1$, condition (i) in the previous proposition can be replaced by $w^{4Kp^j} \equiv 1 \pmod N$ and $\gcd(w^{4Kp^{j-1}} - 1, N) = 1$.

In the case $p = 2$, Proposition 3 must be slightly modified since $\Phi_2(X) = X + 1$ but the proof is similar.

Proposition 4 *Let $N = K2^n - 1 \geq 6$ ($n > 1$ and K odd) be an integer and let w be a Gaussian integer such that $w \in \mathcal{G}_N$. Assume that there exists $1 \leq j \leq n$ such that:*

(i) $w^{K2^{j-1}} \equiv -1 \pmod N$,
(ii) $2j \geq \log_2(K) + n + 1$.

Then, N is prime.

Remark 2 In this case, Proposition 4 can be used to certify primality only if $K \leq 2^{n-1}$.

Propositions 3 and 4 can be restated in a more algorithmic fashion. The case $p = 2$ (Corollary 2) provides a Gaussian analogue of the classical Lucas–Lehmer–Riesel test.

Corollary 1 *Let $N = 4Kp^n - 1$ with p an odd prime and $n \geq 1$ and let K be an odd integer with $4K \leq p^n$. Also, $w \in \mathcal{G}_N$ and consider the recursive sequence defined by: $S_0 = w^{4K}$ and $S_i = S_{i-1}^p \pmod N$ for every $i \geq 1$. If for some j with $\frac{1}{2}(\log_p(4K) + n) \leq j \leq n$ it holds that $\gcd(S_{j-1} - 1, N) = 1$ and $S_j \equiv 1 \pmod N$, then N is prime.*

Corollary 2 *Let $N = K2^n - 1$ with $n \geq 2$, and let K be an odd integer with $K \leq 2^{n-1}$. Also, let $w \in \mathcal{G}_N$ and consider the recursive sequence defined by: $S_0 = w^K$ and $S_i = S_{i-1}^2 \pmod N$ for every $i \geq 1$. If for some j with $\frac{1}{2}(\log_2(K) + n - 1) \leq j < n$ it holds that $S_j \equiv -1 \pmod N$, then N is prime.*

4 Algorithm and computational complexity

Using Corollary 1, we can design an algorithm to test the primality of numbers written in the form $N = 4Kp^n - 1$ which requires just one modular exponentiation over the Gaussian integers (for numbers $N = K2^n - 1$ we must consider Corollary 2 and modify some indices). A pseudo code for this algorithm would be as follows.

1: INPUT: K, $p, n, z \in \mathbb{Z}[i]$. Let $N := 4Kp^n - 1$.
2: **if** $\gcd(|z|, N) = 1$ **then** Let $w = \frac{z^2}{|z|} \pmod N$; $S_0 := w^{4K}$.
3: **else return** N is composite.
4: **end if**
5: **if** $S_0 \equiv 1 \pmod N$ **then**
6: **return** N is a p-Gaussian strong probable prime to base w.
7: **end if**
8: **for** $i = 1, 2, 3, \ldots, n$ **do**
9: $S_i := S_{i-1}^p \pmod N$
10: **if** $S_i \equiv 1 \pmod N$ and $\gcd(S_{i-1} - 1, N) = 1$ **then GoTo** 17.

11: **else**
12: **if** $S_i \equiv 1 \pmod N$ and $\gcd(S_{i-1} - 1, N) \neq 1$ **then**
13: **return** N is composite
14: **end if**
15: **end if**
16: **end for return** N is composite
17: **if** $2i < \log_p 4K + n$ **then**
18: **return** N is a p-Gaussian strong probable prime to base w
19: **else return** N is PRIME.
20: **end if**

Remark 3 Given a Gaussian integer w, in order to compute w^k, we must compute A_k and B_k such that $w^k = A_k + B_k i$. If $w = a + bi$, it is easy to see that $2A_k = v_k(2a, a^2 + b^2)$ and $B_k = bu_k(2a, a^2 + b^2)$, where u_k and v_k are the Lucas functions defined in [16, p. 516]. Computing remote terms of Lucas sequences is discussed in [23, Section 4.4]. However, all these computations can be performed in a natural way in this Gaussian setting without the explicit use of Lucas sequences.

Now, the complexity of this algorithm is given in the following result.

Proposition 5 *For $N = 4Kp^n - 1$ with fixed K and p, the computational complexity of the algorithm above is $\widetilde{\mathcal{O}}(\log^2 N)$.*

Proof Only the for loop in lines 8 to 16 cause complexity, the rest is obviously irrelevant. Note that w is a Gaussian integer and a modular exponentiation can be performed using the Schoenhage–Strassen algorithm [18] with complexity $\widetilde{\mathcal{O}}(\log N)$. In fact, we could even use a dedicated algorithm, like the LSEG proposed by Koval [10] for Gaussian integer exponentiation. In line 9, we must do at most n modular exponentiations with the same complexity. Since $n = \log_p(\frac{N-1}{4K})$, the complexity for this task is $\widetilde{\mathcal{O}}(\log^2(N))$. Finally, in line 12, we test whether $\gcd(S_i - 1, N) = 1$. Since this has computational complexity $\mathcal{O}(\log(N))$ the result follows. □

With the notation of the previous algorithm, let us consider an integer N written in the form $4Kp^n - 1$ with $4K < p^n$. Also, given $w \in \mathcal{G}_N$, let us define $S_J := w^{4Kp^J}$ with $J := \left\lfloor \frac{\log_p(4K)+n}{2} \right\rfloor$. It is easy to see that if $S_J \not\equiv 1 \pmod N$, then the algorithm always certifies the primality or compositeness of N.

We will now see that, for moderately big values of n, the probability that the algorithm does not certify the primality of a prime $N = 4Kp^n - 1$ without choosing more that one base is extremely small and that it decreases with p. To do so, we first need the following lemma.

Lemma 1 *let $N = 4Kp^n - 1$ be a prime number. The number of p^s-th powers modulo N in $\mathcal{G}_N$ is $4Kp^{n-s}$.*

Proof It is enough to recall [9, Proposition 2.1] that, if N is prime, $\mathcal{G}_N$ is the cyclic group C_{N+1} because $N \equiv 3 \pmod 4$. □

Using this result, we can prove the following proposition.

Proposition 6 *Let N be a prime number written in the form $4Kp^n - 1$ with $4K < p^n$. Given a random base $w \in \mathcal{G}_N$, the probability that the algorithm returns "p-Gaussian strong probable prime" is:*

$$\frac{4Kp^{\left\lfloor \frac{\log_p(4K)+n}{2} \right\rfloor} - 1}{4Kp^n - 1}.$$

Proof The algorithm returns "N is p-Gaussian strong probable prime" when $J := \left\lfloor \frac{\log_p(4K)+n}{2} \right\rfloor$ satisfies that $w^{4Kp^J} \equiv 1 \pmod{N}$. That is, when the order of $w \in \mathcal{G}_N$ divides $4Kp^J$. Since $\mathcal{G}_N$ is cyclic, it is equivalent to w being a residual power of order p^{n-J} modulo N. But, by the previous lemma, this happens with probability:

$$\frac{4Kp^J - 1}{|\mathcal{G}_N| - 1} = \frac{4Kp^{\left\lfloor \frac{\log_p(4K)+n}{2} \right\rfloor} - 1}{4Kp^n - 1}.$$

□

Note that, if $N = 4Kp^n - 1$ is prime and K is "much smaller" that p^n, then a random choice of w will most likely determine the primality of N. In particular, so it happens when K is fixed and n increases (which is usually the case when searching for primes of this form) and Proposition 6 above implies that, for big values of n, the probability that a prime of the form $N = 4Kp^n - 1$ is certified as p-strong probable prime is about $p^{-n/2}$. However, if $p^{n-1} \leq K < p^n$ and N is prime, then the test will give "p-strong probable prime" with probability approximately equal to $1/p$ which is not really good. For numbers of the form $N = K2^n - 1$ with $n \geq 2$ and $K \leq 2^{n-1}$ an odd number, these results can be easily adapted just modifying the value of J.

5 Conclusions and future work

The importance of our work relies on the fact that we certify primality of $4Kp^n - 1$ numbers using a non-explicit Lucasian method. The required computations have a cost equivalent to that of a modular exponentiation, w^{N+1}, carried out by n (and, sometimes, much less than n) modular exponentiations of order p. Unlike other methods, ours do not require to choose an adequate base, since it is independent from both the prime p and the integer K. Also, while other methods usually require several tries in the choice of the Lucas sequence, the failure probability of our test with a random choice of the base w is extremely small for moderately big values of n. For instance, if $K = 1$, $p = 7$ and $n > 50$ Proposition 6 implies that this probability is smaller than 10^{-21}.

So, even if we cannot state that our results certify the primality of any integer for which the known primality results fail, we can state that any prime written in the form $N = 4Kp^n - 1$ with moderately big n will be certified as such with extremely high probability. On the other hand, there are composite numbers (apparently very few of them) that the algorithm certifies as "p-Gaussian strong probable prime". This is the case, for instance, of $223154201663 =$

$4 \cdot 16 \cdot 3^{20} - 1$ 19601671586459972505009745912142 3 $= 4 \cdot 1156 \cdot 3^{60} - 1$ 11767419407284731086 3 $= 4 \cdot 196 \cdot 3^{36} - 1$. It is noteworthy that these three examples are obtained as the product of twin primes which are Gaussian Carmichael numbers [9]; i.e., numbers N satisfying that $(w/\overline{w})^{N+1} \equiv 1 \pmod{N}$ for all w Gaussian integer such that N is coprime to $w\overline{w}$.

As future development related to the ideas that we have presented in this work and to those that were used in [8] for numbers written in the form $Kp^n + 1$, we may mention the study of algorithms aimed at certifying the primality of numbers of the form $n! \pm 1$, $\sharp n \pm 1$, $2p^n q^m \pm 1$ (and, in general, of numbers such that either $N + 1$ or $N - 1$ are easily factored) requiring only one modular exponentiation of a randomly chosen integer or Gaussian base.

Acknowledgements The authors wish to thank the anonymous referees for their many insightful comments and suggestions that helped to improve the paper.

References

1. Berrizbeitia, P., Berry, T.G.: Cubic reciprocity and generalised Lucas–Lehmer tests for primality of $A \cdot 3^n \pm 1$. Proc. Am. Math. Soc. **127**(7), 1923–1925 (1999)
2. Berrizbeitia, P., Berry, T.G.: Biquadratic reciprocity and a Lucasian primality test. Math. Comput. **73**(247), 1559–1564 (2004)
3. Bosma, W.: Cubic reciprocity and explicit primality tests for $h \cdot 3^k \pm 1$. In: van der Poorten, A., Stein, A. (eds.) High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams, volume 41 of Fields Inst. Commun., pp. 77–89. American Mathematical Society, Providence, RI (2004)
4. Crandall, R., Pomerance, C.: Prime Numbers: A Computational Perspective, 2nd edn. Springer, New York (2005)
5. Deng, Y., Lv, C.: Primality test for numbers of the form $Ap^n + w_n$. J. Discret. Algorithms **33**, 81–92 (2015)
6. Deng, Y., Huang, D.: Explicit primality criteria for $h \cdot 2^n \pm 1$. Journal de Theorie des Nombres de Bordeaux **28**(1), 55–74 (2016)
7. GIMPS, GreatInternet Mersenne Prime Search. Founded by G. Woltman. https://www.mersenne.org. Accessed 1 Nov 2019
8. Grau, J.M., Oller-Marcén, A.M., Sadornil, D.: A primality test for $Kp^n + 1$ numbers. Math. Comput. **84**(291), 505–512 (2015)
9. Grau, J.M., Oller-Marcén, A.M., Sadornil, D.: Fermat test with Gaussian base and Gaussian pseudoprimes. Czechoslov. Math. J. **65**(140), 969–982 (2015)
10. Koval, A.: Algorithm for Gaussian integer exponentiation. In: Latifi, S. (ed.) Information Technology: New Generations. Advances in Intelligent Systems and Computing, vol. 448, pp. 1075–1085. Springer, Berlin (2016)
11. Lehmer, D.H.: An extended theory of Lucas' functions. Ann. Math. Second Ser. **31**(3), 419–448 (1930)
12. Lemmermeyer, F.: Conics—a poor man's elliptic curves. arXiv:math/0311306v1, preprint at http://www.fen.bilkent.edu.tr/franz/publ/conics.pdf
13. Lucas, E.: Théorie des fonctions numériques simplement périodiques. Am. J. Math. Pure Appl. **1**(184–239), 289–321 (1878)
14. Riesel, H.: Lucasian criteria for the primality of $N = h \cdot 2^n - 1$. Math. Comput. **23**(108), 869–875 (1969)
15. Rödseth, O.J.: A note on primality tests for $N = h \cdot 2^n - 1$. BIT **34**(3), 451–454 (1994)
16. Roettger, E.L., Williams, H.C., Guy, R.K.: Some primality tests that eluded Lucas. Des. Codes Cryptogr. **77**, 515–539 (2015)
17. Sadovnik, E.V.: Testing numbers of the form $N = 2kp^m - 1$ for primality. Discret. Math. Appl. **16**(2), 99–108 (2006)

18. Schönhage, A., Strassen, V.: Schnelle multiplikation grosser zahlen. Computing (Arch. Elektron. Rechnen) **7**, 281–292 (1971)
19. Stechkin, S.B.: Lucas's criterion for the primality of numbers of the form $N = h2^n - 1$. Math. Notes Acad. Sci. USSR **10**(3), 578–584 (1971)
20. Stein, A., Williams, H.C.: Explicit primality criteria for $(p - 1)p^n - 1$. Math. Comput. **69**(232), 1721–1734 (2000)
21. Sun, Z.-H.: Primality tests for numbers of the form $K \cdot 2^m \pm 1$. Fibonacci Q. **44**(2), 121–130 (2006)
22. Williams, H.C.: The primality of certain integers of the form $2Ar^n - 1$. Acta Arith. **39**(1), 7–17 (1981)
23. Williams, H.C.: Édouard Lucas and Primality Testing. Wiley, New York (1998)
24. Williams, H.C., Zarnke, C.R.: Some prime numbers of the forms $2A3^n + 1$ and $2A3^n - 1$. Math. Comput. **26**, 995–998 (1972)