MATHEMATICS OF COMPUTATION
Volume 66, Number 218, April 1997, Pages 869–881
S 0025-5718(97)00836-3

THE RABIN-MONIER THEOREM FOR LUCAS PSEUDOPRIMES

F. ARNAULT

ABSTRACT. We give bounds on the number of pairs (P, Q) with $0 \leq P, Q < n$ such that a composite number n is a strong Lucas pseudoprime with respect to the parameters (P, Q).

1. INTRODUCTION

Pseudoprimes, strong pseudoprimes. It is well known that if n is a prime number, then it satisfies one of the following relations, where $n - 1 = 2^k q$ with q odd.

$$\text{(1)}\quad \begin{aligned} &b^q \equiv 1 \text{ modulo } n \\ &\text{or} \\ &\text{there exists an integer } i \text{ such that } 0 \leq i < k \text{ and } b^{2^i q} \equiv -1 \text{ modulo } n. \end{aligned}$$

This property is often used as a primality "test", called the Rabin-Miller test, which consists in checking if the property (1) holds, for several bases b. If (1) does not hold for some b, then n is certainly composite. If (1) is found to be true when trying several bases (usually 10 or 20), then n is likely to be prime. Composite numbers which satisfy the condition (1) are called strong pseudoprimes with respect to the base b. For short spsp(b).

By recent results, it is possible to build composite numbers which satisfy (1) for several chosen bases b (see [1], [2], [5]). So, when one knows the bases used by a given implementation of the Rabin-Miller test, one can find composite numbers which this test finds to be prime. However, it is possible to give upper bounds for the probability that this test will give an incorrect answer. The main result in this direction is the Rabin-Monier theorem.

1.1. Theorem (Rabin-Monier). *Let n be a composite integer distinct from 9. The number of bases b such that $0 < b < n$, which are relatively prime to n and for which n is a* spsp(b) *is bounded by $\varphi(n)/4$, where φ is the Euler function.*

Lucas pseudoprimes. Let P and Q be integers and $D = P^2 - 4Q$. For n integer, we denote by $\varepsilon(n)$ the Jacobi symbol (D/n). The Lucas sequences associated with the parameters P, Q are defined by

$$\begin{cases} U_0 = 0, & U_1 = 1, \\ V_0 = 2, & V_1 = P, \end{cases} \quad \text{and, for } k \geq 0, \quad \begin{cases} U_{k+2} = PU_{k+1} - QU_k, \\ V_{k+2} = PV_{k+1} - QV_k. \end{cases}$$

Received by the editor August 30, 1994 and, in revised form, February 28, 1995 and November 6, 1995.

1991 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A51, 11R11.

Key words and phrases. Primality testing, Lucas pseudoprimes.

We have the following result, which can be compared with the criterion (1):

1.2. Theorem. *Let p be a prime number not dividing $2QD$. Put $p - \varepsilon(p) = 2^k q$ with q odd. One of the following conditions is satisfied:*

$$p|U_q$$

or

$$\text{there exists } i \text{ such that } 0 \leq i < k \text{ and } p|V_{2^i q}.$$

A composite number n relatively prime to $2QD$ and satisfying

$$n|U_q \quad \text{or} \quad \text{there exists } i \text{ such that } 0 \leq i < k \text{ and } p|V_{2^i q}, \tag{2}$$

where we have put $n - \varepsilon(n) = 2^k q$ with q odd, is called a strong Lucas pseudoprime with respect to the parameters P and Q. For short we write n is an slpsp(P, Q).

As above, we can derive a "test" from this property: the strong Lucas pseudoprime test [4]. In this test, we check whether property (2) holds, for several pairs (P, Q).

The main result. The main purpose of this paper is to prove the following theorem, which is the analog of Theorem 1.1 but for strong Lucas pseudoprimes.

1.3. Theorem. *Let D be an integer and n a composite number relatively prime to $2D$ and distinct from 9. For all integer D, the size*

$$\mathrm{SL}(D,n) = \# \left\{ (P,Q) \left| \begin{matrix} 0 \leq P, Q < n, & P^2 - 4Q \equiv D \textit{ modulo } n, \\ \gcd(Q,n) = 1, & n \textit{ is } \mathrm{slpsp}(P,Q) \end{matrix} \right. \right\} \tag{3}$$

is less than or equal to $\frac{4}{15}n$ except if n is the product

$$n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$$

of twin primes with q_1 odd and such that the Legendre symbols satisfy $(D/2^{k_1}q_1 - 1) = -1$, $(D/2^{k_1}q_1 + 1) = 1$. Also, the following inequality is always true:

$$\mathrm{SL}(D,n) \leq n/2.$$

The Monier formula and its analog. A result close to Theorem 1.1 was first shown by Rabin [9]. But Monier [7] gave the following formula and used it to prove Theorem 1.1.

1.4. Theorem (Monier). *Let $p_1^{r_1} \cdots p_s^{r_s}$ be the prime decomposition of an odd integer $n > 0$. Put*

$$\begin{cases} n - 1 = 2^k q, \\ p_i - 1 = 2^{k_i} q_i \quad \textit{for } 0 \leq i \leq s, \end{cases} \quad \textit{with } q, q_i \textit{ odd,}$$

ordering the p_i's such that $k_1 \leq \cdots \leq k_s$. The number of bases b such that n is an spsp(b) *is expressed by the following formula*

$$B(n) = \left(1 + \sum_{j=0}^{k_1 - 1} 2^{js} \right) \prod_{i=1}^{s} \gcd(q, q_i).$$

Similarly, we will first prove, in Section 4, an analogous formula for the Lucas test.

1.5. Theorem. *Let D be an integer and let $p_1^{r_1}\cdots p_s^{r_s}$ be the prime decomposition of an integer $n>2$ relatively prime to $2D$. Put*

$$\begin{cases} n-\varepsilon(n)=2^k q, \\ p_i-\varepsilon(p_i)=2^{k_i}q_i \quad \text{for } 1\le i\le s, \end{cases} \qquad \text{with } q, q_i \text{ odd},$$

ordering the p_i's such that $k_1\le\cdots\le k_s$. The number of pairs (P,Q) with $0\le P,Q<n$, $\gcd(Q,n)=1$, $P^2-4Q\equiv D$ modulo n and such that n is an $\operatorname{slpsp}(P,Q)$ *is expressed by the following formula*

$$\operatorname{SL}(D,n)=\prod_{i=1}^{s}(\gcd(q,q_i)-1)+\sum_{j=0}^{k_1-1}2^{js}\prod_{i=1}^{s}\gcd(q,q_i).$$

2. Some lemmas

We start with three lemmas. The first two will be used to prove Theorem 1.5, and the last to prove Theorem 1.3.

Roots in a cyclic group.

2.1. Lemma. *Let G be a cyclic group and q an integer.* (a) *There are exactly* $\gcd(q,|G|)$ *qth-roots of* 1 *in G.* (b) *An element y of G is a qth-power if and only if*

$$y^{|G|/\gcd(q,|G|)}=1.$$

In this case, y has exactly $\gcd(q,|G|)$ *qth-roots in G.*

Proof. Put $d=\gcd(q,|G|)$. The proof of (a) is easy if we see, using Bezout relations, that for $x\in G$,

$$x^q=1\Leftrightarrow x^d=1.$$

Also, the qth-powers in G are the dth-powers. But, y is a dth-power if and only if $y^{|G|/d}=1$. To count the qth-roots of y whenever such a root exists, we remark that we can obtain the others from it by multiplying it by a qth-root of 1. □

Congruences in some rings.

2.2. Lemma. *Let $\mathcal{O}$ be a ring extension of $\mathbb{Z}$ and $\alpha,\beta\in\mathcal{O}$. Let also $\mathfrak{p}$ be a prime ideal in $\mathcal{O}$, $r\ge 1$ be an integer, and $k\in\mathfrak{p}\cap\mathbb{Z}$. One has the implication*

$$\alpha\equiv\beta \text{ modulo } \mathfrak{p}\Rightarrow \alpha^{k^{r-1}}\equiv\beta^{k^{r-1}} \text{ modulo } \mathfrak{p}^r.$$

Proof. If $\alpha-\beta\in\mathfrak{p}$, then

$$\begin{aligned}\alpha^k-\beta^k&=(\alpha-\beta)(\alpha^{k-1}+\alpha^{k-2}\beta+\cdots+\beta^{k-1})\\ &\equiv(\alpha-\beta)(\alpha^{k-1}+\alpha^{k-1}+\cdots+\alpha^{k-1}) \text{ modulo } \mathfrak{p}\\ &=(\alpha-\beta)k\alpha^{k-1}\in\mathfrak{p}^2.\end{aligned}$$

This shows the assertion when $r=2$. An easy induction concludes the proof. □

The φ_D function. Let D be an integer and let $\varepsilon(n)$ denote the Jacobi symbol (D/n). For convenience, we introduce the following number-theoretic function, studied in [3] and defined only on integers relatively prime to $2D$:

$$\begin{cases} \varphi_D(p^r) = p^{r-1}(p - \varepsilon(p)) & \text{for any prime } p \nmid 2D, \text{ and } r \in \mathbb{N}^*, \\ \varphi_D(n_1 n_2) = \varphi_D(n_1)\varphi_D(n_2) & \text{for } n_1 \text{ and } n_2 \text{ relatively prime.} \end{cases}$$

2.3. Lemma. *Let D be an integer. For $n > 0$ relatively prime to $2D$, we have*

$$\varphi_D(n) \leq \left(\frac{4}{3}\right)^s n$$

where s is the number of distinct prime factors of n. Also, we have the particular cases:

$$\begin{aligned} s = 2 &\Rightarrow \varphi_D(n) \leq \frac{8}{5} n, \\ s = 3 &\Rightarrow \varphi_D(n) \leq \frac{64}{35} n, \\ s \geq 4 &\Rightarrow \varphi_D(n) \leq \frac{768}{385} \left(\frac{14}{13}\right)^{s-4} n. \end{aligned}$$

Proof. For the first part of the result, it is sufficient to handle the case where $n = p^r$ is an odd prime power such that $p \nmid D$. Then we have

$$\frac{\varphi_D(p^r)}{p^r} = \frac{p^{r-1}(p - \varepsilon(p))}{p^r} = 1 - \varepsilon(p)/p \leq 1 + 1/p \leq 4/3$$

and the result follows. The proof of the second part is similar, using the knowledge that $p_i \geq 5$ for all but perhaps one subscript $i, p_i \geq 7$ for all but perhaps two subscripts $i, p_i \geq 11$ for all but perhaps three subscripts, and $p_i \geq 13$ for all but perhaps four subscripts. □

3. Connection with quadratic integers

Let P, Q be integers such that $D = P^2 - 4Q \neq 0$ and consider the Lucas sequences (U_n) and (V_n) associated with P, Q. It is easy to see that we have the relations

$$(4) \qquad U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta}, \quad V_k = \alpha^k + \beta^k, \quad \text{for all } k \in \mathbb{N},$$

where α, β are the two roots of the polynomial $X^2 - PX + Q$. Also, if n is an integer relatively prime to $2QD$, we can put $\tau = \alpha\beta^{-1}$ modulo $n\mathcal{O}$. Then we have the following equivalences, for $k \in \mathbb{N}$,

$$\begin{aligned} n | U_k &\Leftrightarrow \tau^k \equiv 1 \text{ modulo } n, \\ n | V_k &\Leftrightarrow \tau^k \equiv -1 \text{ modulo } n. \end{aligned}$$

Hence, if n is composite and relatively prime to $2QD$, it is an slpsp(P, Q) if and only if

$$\tau^q \equiv 1 \quad \text{modulo } n$$

or

$$\text{there exists } i \text{ such that } 0 \leq i < k \text{ and } \tau^{2^i q} \equiv -1 \text{ modulo } n,$$

where $n - \varepsilon(n) = 2^k q$ with q odd.

Norm 1 elements. Let $\mathcal{O}$ be the ring of integers of a quadratic field $\mathbb{Q}(\sqrt{D})$. The norm in $\mathbb{Q}(\sqrt{D})$ is the map N defined by $N(u+v\sqrt{D}) = u^2 - Dv^2 \in \mathbb{Q}$ $(u, v \in \mathbb{Q})$. For z in $\mathcal{O}$, the norm $N(z)$ is in $\mathbb{Z}$. For a rational integer n, the ring $\mathcal{O}/n$ is a free $(\mathbb{Z}/n\mathbb{Z})$-algebra of rank 2. We consider, in this algebra, the multiplicative group of norm 1 elements, which we denote by $(\mathcal{O}/n)^\wedge$. In other words, $(\mathcal{O}/n)^\wedge$ is the image of the set

$$\{x \in \mathcal{O} | N(x) \equiv 1 \text{ modulo } n\}$$

by the canonical map $\mathcal{O} \to \mathcal{O}/n$.

The proof of Theorem 1.5 will be similar to Monier's proof, but will use the following result on the structure of the group $(\mathcal{O}/n)^\wedge$, which is proved in [3].

3.1. Theorem. *Let $p \nmid 2D$ be a prime number and $r \geq 1$ an integer. The group $(\mathcal{O}/p^r)^\wedge$ is* ***cyclic*** *of order $p^{r-1}(p - (D/p))$.* □

The link between the parameters P, Q and the norm 1 elements τ is described by the following result:

3.2. Proposition. *Let D be an integer, but not a perfect square and $\mathcal{O}$ be the ring of integers in $\mathbb{Q}(\sqrt{D})$. Let n be an integer relatively prime to $2D$. Then, for all integers P, there exists an integer Q, uniquely determined modulo n, such that $P^2 - 4Q \equiv D$ modulo n. Moreover, the set of integers P such that*

$$\begin{cases} 0 \leq P < n, \\ \gcd(P^2 - D, n) = 1 \ (i.e. \ \gcd(Q, n) = 1), \end{cases}$$

is in a one-to-one correspondence with the elements τ in $(\mathcal{O}/n)^\wedge$ such that $\tau - 1$ is a unit in $\mathcal{O}/n$. This correspondence is expressed by the following formulas

$$\begin{cases} \tau \equiv (P + \sqrt{D})(P - \sqrt{D})^{-1} \\ P \equiv \sqrt{D}(\tau + 1)(\tau - 1)^{-1} \end{cases} \quad \textit{modulo } n\mathcal{O}. \tag{5}$$

Proof. The first claim is easy, as n is odd. Then, we observe that τ^{-1} and τ are conjugate in $\mathcal{O}/n$. So putting $u + \sqrt{D}v = \sqrt{D}(\tau + 1)(\tau - 1)^{-1}$, we have

$$\begin{aligned} u - v\sqrt{D} &= \overline{\sqrt{D}(\tau + 1)(\tau - 1)^{-1}} \\ &\equiv -\sqrt{D}(\tau^{-1} + 1)(\tau^{-1} - 1)^{-1} \text{ modulo } n \\ &= -\sqrt{D}(1 + \tau)(1 - \tau)^{-1} \\ &= \sqrt{D}(\tau + 1)(\tau - 1)^{-1} = u + v\sqrt{D}. \end{aligned}$$

As n is odd, we obtain $v \equiv 0$ modulo n. So the second equation in (5) is satisfied by a rational integer. Then we leave to the reader the task of showing that the two relations (5) are equivalent to each other. □

Remark on the square discriminant case. If D is a non-zero perfect square it is well known that the strong Lucas test reduces to the Rabin-Miller test. It is interesting to clarify this fact. If n is an integer relatively prime to $2D$, we can put $T = \alpha\beta^{-1}$ modulo n (this time, α, β are rational integers). From (4) we have the following equivalences, for $k \in \mathbb{N}$:

$$n | U_k \Leftrightarrow T^k \equiv 1 \text{ modulo } n, \qquad n | V_k \Leftrightarrow T^k \equiv -1 \text{ modulo } n.$$

So n is an slpsp(P, Q) if and only if it is an spsp(T).

Moreover, the proof of Proposition 3.2 could very easily be adapted to show that there exists a one-to-one correspondence between the sets

$$\left\{P \,\middle|\, \begin{array}{l} 0 \le P < n \\ \gcd(P^2 - D, n) = 1 \end{array}\right\} \quad \text{and} \quad \left\{T \,\middle|\, \begin{array}{l} 0 \le T < n \\ \gcd(T, n) = \gcd(T-1, n) = 1 \end{array}\right\}.$$

Hence, the proof of Theorem 1.4 given by Monier could easily be adapted to prove Theorem 1.5 in this special case where D is a perfect square.

4. Proof of Theorem 1.5

The difference between consecutive perfect squares d^2 and $(d+1)^2$ tends to $+\infty$ as d tends to $+\infty$. So the integers $D+kn$ with $k \in \mathbb{Z}$ cannot all be perfect squares. Because $\mathrm{SL}(D, n)$ is equal to $\mathrm{SL}(D+kn, n)$ for all integer k, we can assume in the proof that D is not a perfect square.

We denote by $\mathcal{O}$ the ring of integers of the field $\mathbb{Q}(\sqrt{D})$. Proposition 3.2 shows that we have to count the number of elements in the sets

$$X(n) = \{\tau \in (\mathcal{O}/n)^\wedge | 1-\tau \in (\mathcal{O}/n)^\times, \tau^q = 1\},$$

$$Y_j(n) = \{\tau \in (\mathcal{O}/n)^\wedge | 1-\tau \in (\mathcal{O}/n)^\times, \tau^{2^j q} = -1\}, \quad \text{for } 0 \le j \le k-1,$$

because their sum is $\mathrm{SL}(D, n)$. Using the Chinese Remainder Theorem, we reduce the problem to counting the sets $X(p_i^{r_i})$ and $Y_j(p_i^{r_i})$.

Count of $X(p_i^{r_i})$.

- We first count $X(p_i^{r_i})$. By Theorem 3.1, the number of qth-roots of 1 in the group $(\mathcal{O}/p_i^{r_i})^\wedge$ is

$$\begin{aligned} d &= \gcd(q, p_i^{r_i-1}(p_i - \varepsilon(p_i))) \\ &= \gcd(q, p_i - \varepsilon(p_i)) \quad \text{since } q \text{ is relatively prime to } n, \\ &= \gcd(q, q_i) \quad \text{since } q \text{ is odd.} \end{aligned}$$

From these roots, we must throw away those such that $1-\tau$ is not invertible modulo p_i. We show that the only such τ is the trivial root 1. Indeed, note that

$$\left\{\begin{array}{l} \tau^{n-\varepsilon(n)} \equiv 1 \\ \tau^{p_i^{r_i-1}(p_i-\varepsilon(p_i))} \equiv 1 \end{array}\right. \Rightarrow \tau^d \equiv 1 \Rightarrow \tau^{p_i-\varepsilon(p_i)} \equiv 1 \quad \text{modulo } p_i^{r_i}\mathcal{O}.$$

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ containing $\mathfrak{p}_i\mathcal{O}$. For $k \ge 1$ integer, we have

$$\begin{aligned} \tau \equiv 1 \text{ modulo } \mathfrak{p}^k &\Rightarrow \tau^{p_i} \equiv 1 \text{ modulo } \mathfrak{p}^{k+1} \quad \text{by Lemma 2.2,} \\ &\Rightarrow 1 \equiv \tau^{p_i-\varepsilon(p_i)} \equiv \tau^{-\varepsilon(p_i)} \quad \text{modulo } \mathfrak{p}^{k+1} \\ &\Rightarrow \tau \equiv 1 \text{ modulo } \mathfrak{p}^{k+1}. \end{aligned}$$

So, by induction, $1-\tau$ is not a unit modulo $\mathfrak{p}^{r_i}$. If p_i splits in $\mathcal{O}$, this implies $\tau \equiv 1$ modulo $\bar{\mathfrak{p}}^{r_i}$ (as $\bar{\tau} = \tau^{-1}$). In both cases (inertial or split), we obtain $\tau \equiv 1$ modulo $p_i^{r_i}$. Hence, the number of elements in $X(p_i^{r_i})$ is

$$d - 1 = \gcd(q, q_i) - 1.$$

Hence,

$$\#X(n) = \prod_{i=1}^{s} (\gcd(q, q_i) - 1).$$

Count of $Y_j(p_i^{r_i})$.

- We now count $Y_j(p_i^{r_i})$. Here, the invertibility condition for $1-\tau$ modulo p_i does not throw away any solution. Indeed, as p_i is odd we cannot have, for $\mathfrak{p}$ a prime ideal containing $p_i\mathcal{O}$,

$$1 = 1^{2^j q} \equiv \tau^{2^j q} \equiv -1 \quad \text{modulo } \mathfrak{p}.$$

By Lemma 2.1, we have

$$\#Y_j(p_i^{r_i}) = \begin{cases} 0 & \text{if } j \geq k_i, \\ \gcd(2^j q, \varphi_D(p_i^{r_i})) = 2^j \gcd(q, q_i) & \text{if } j < k_i. \end{cases}$$

Lastly, the equality

$$\mathrm{SL}(D,n) = \#X(n) + \sum_{j=0}^{k-1} \#Y_j(n)$$

completes the proof because, as $n \equiv \varepsilon(n)$ modulo 2^{k_1} (as $p_i \equiv \varepsilon(p_i)$ modulo 2^{k_1} for all i), we have $k_1 \leq k$. □

5. First consequences

Following the usual proof [7] of the Rabin-Monier theorem, we would easily obtain

5.1. Corollary. *If n is an odd composite integer, then*

$$\mathrm{SL}(D,n) \leq \varphi_D(n)/4.$$

But, as the function $\varphi_D(n)$ is not bounded by n (see [3] for more details), this result is not of the same interest as Theorem 1.3.

In fact, using Proposition 3.2, one can show, if $p_1^{r_1}\cdots p_s^{r_s}$ is the prime decomposition of n, that the size

$$\#\left\{(P,Q) \;\middle|\; \begin{array}{c} 0 \leq P, Q < n, \quad P^2 - 4Q \equiv D \text{ modulo } n, \\ \gcd(Q,n) = 1 \end{array}\right\} \text{ is } \prod_{i=1}^{s} p_i^{r_i - 1}(p_i - \varepsilon(p_i) - 1).$$

This size is less than n and is equal to it infinitely many times. So it seems quite natural to try to bound $\mathrm{SL}(D,n)$ by kn for some constant k.

5.2. Lemma. *Let $p_1^{r_1}\cdots p_s^{r_s}$ be the prime decomposition of an integer n relatively prime to $2D$. With the notations k, q, k_i, q_i of Theorem 1.5, we have the inequalities*

$$\frac{\mathrm{SL}(D,n)}{\varphi_D(n)} \leq \begin{cases} \frac{1}{2^{s-1}} \prod_{i=1}^{s} \frac{\gcd(q,q_i)}{q_i}, \\ \frac{1}{2^{s-1}} \prod_{i=1}^{s} \frac{1}{p_i^{r_i-1}}, \\ 1/2^{s-1+\delta_2+\cdots+\delta_s} \quad \textit{where } \delta_i = k_i - k_1. \end{cases}$$

Proof. We follow the proof of the very similar statement by Monier [7]. We have

$$\varphi_D(n) = 2^{k_1+\cdots+k_s} \cdot \prod_{i=1}^{s} q_i \cdot \prod_{i=1}^{s} p_i^{r_i-1}$$

so, by Theorem 1.5,

$$\frac{\mathrm{SL}(D,n)}{\varphi_D(n)} \leq \frac{1 + \sum_{j=0}^{k_1-1} 2^{js}}{2^{k_1+\cdots+k_s}} \prod_{i=1}^{s} \frac{\gcd(q,q_i)}{q_i} \prod_{i=1}^{s} \frac{1}{p_i^{r_i-1}}. \tag{6}$$

But the left-hand factor of (6) is bounded by

$$\begin{aligned}\frac{1+\sum_{j=0}^{k_1-1} 2^{js}}{2^{sk_1}} &= \frac{1+(2^{sk_1}-1)/(2^s-1)}{2^{sk_1}}\\ &= \left(1+\frac{2^{sk_1}}{2^s-1}-\frac{1}{2^s-1}\right)/2^{sk_1}\\ &= \left[\left(1-\frac{1}{2^s-1}\right)/2^{sk_1}\right]+\frac{1}{2^s-1}.\end{aligned}$$

The last formula shows that this is a decreasing function of k_1. So we can bound it by its value at $k_1 = 1$:

$$\frac{1+\sum_{j=0}^{k_1-1} 2^{js}}{2^{sk_1}} \le \frac{1}{2^{s-1}}. \tag{7}$$

The first two inequalities follow from this. The last also follows from (7), using the equality

$$\frac{1+\sum_{j=0}^{k_1-1} 2^{js}}{2^{k_1+\cdots+k_s}} = \frac{1+\sum_{j=0}^{k_1-1} 2^{js}}{2^{sk_1}} \frac{1}{2^{\delta_2+\cdots+\delta_s}}. \quad \square$$

6. Proof of Theorem 1.3

As in Theorem 1.5, we use the following notation: Let $p_1^{r_1}\cdots p_s^{r_s}$ be the prime decomposition of n and put

$$\begin{cases} n-\varepsilon(n) = 2^k q, & \\ & \text{with } q, q_i \text{ odd.}\\ p_i-\varepsilon(p_i) = 2^{k_i}q_i \quad \text{for } 1\le i\le s, & \end{cases}$$

The case $s = 1$. First, consider the case $s = 1$. The second inequality of Lemma 5.2 shows that

$$\mathrm{SL}(D,n) \le \frac{1}{p_1^{r_1-1}}\varphi_D(n).$$

If $p_1 \ge 5$ we obtain, as $r_1 \ge 2$,

$$\mathrm{SL}(D,n) \le \varphi_D(n)/5.$$

In this case, Lemma 2.3 implies $\mathrm{SL}(D,n) \le (4/3)n/5 = (4/15)n$. If $p_1 = 3$, a similar argument holds, because we assume $n \ne 9$.

The case $s = 2$. Now, the case $s = 2$. By the second part of Lemma 2.3, it is sufficient to show that we have

$$\mathrm{SL}(D,n) \le \frac{1}{6}\varphi_D(n). \tag{8}$$

- But, Lemma 5.2 gives

$$\frac{\mathrm{SL}(D,n)}{\varphi_D(n)} \le \begin{cases} 1/6 & \text{if } r_i \ge 2 \text{ for at least some } i,\\ 1/8 & \text{if } \delta_2 = k_2-k_1 \ge 2,\end{cases}$$

which is sufficient to prove the assertion in both cases.

- So we can assume that $r_1 = r_2 = 1$ ($n = p_1p_2$) and $\delta_2 = k_2 - k_1 = 0$ or 1. First, we consider the subcase where $q_1 \neq q_2$. Then the first inequality of Lemma 5.2 shows that

$$\frac{\mathrm{SL}(D,n)}{\varphi_D(n)} \leq \frac{1}{2}\frac{\gcd(q,q_1)}{q_1}\frac{\gcd(q,q_2)}{q_2}.$$

Here, we point out that at least one of the ratios $\gcd(q,q_i)/q_i$ is bounded by $1/3$. Otherwise, they would both be 1 and then both q_1 and q_2 would divide q. Also

$$\begin{aligned} 2^kq &= p_1p_2 - \varepsilon(p_1p_2) \\ &= (2^{k_1}q_1 + \varepsilon(p_1))(2^{k_1+\delta_2}q_2 + \varepsilon(p_2)) - \varepsilon(p_1p_2) \\ &= 2^{2k_1+\delta_2}q_1q_2 \pm 2^{k_1}(q_1 \pm 2^{\delta_2}q_2). \end{aligned}$$

We would then have $q_1|q_2$ and $q_2|q_1$, contradicting the hypothesis $q_1 \neq q_2$. Hence, if $q_1 \neq q_2$, then

$$\frac{\mathrm{SL}(D,n)}{\varphi_D(n)} \leq 1/6$$

and equation (8) is satisfied.

- So we can suppose that $r_1 = r_2 = 1$ ($n = p_1p_2$), $\delta_2 = k_2 - k_1$ equals 0 or 1, and that $q_1 = q_2$. If $\delta_2 = 1$, the integer n is

$$\begin{aligned} n &= (2^{k_1}q_1 \pm 1)(2^{k_1+1}q_1 \pm 1) \quad \text{with } q_1 \text{ odd} \\ &\geq (2^{k_1}q_1 - 1)(2^{k_1+1}q_1 - 1) \\ &= 2(2^{k_1}q_1)^2 - 3(2^{k_1}q_1) + 1. \end{aligned}$$

Hence, $8(2^{k_1}q_1)^2 - 12(2^{k_1}q_1) + 4 \leq 4n$. We have also

$$2^kq = n - \varepsilon(n) = 2(2^{k_1}q_1)^2 + (2\varepsilon(p_1) + \varepsilon(p_2))(2^{k_1}q_1)$$

and so, q_1 divides q. Here, Theorem 1.5 gives

$$\begin{aligned} \mathrm{SL}(D,n) &= (q_1 - 1)^2 + (1 + 4 + \cdots + 4^{k_1-1})q_1^2 \\ &= (q_1 - 1)^2 + \frac{4^{k_1} - 1}{3}q_1^2 \qquad (9) \\ &\leq \frac{4^{k_1} + 2}{3}q_1^2. \end{aligned}$$

Hence, $15\,\mathrm{SL}(D,n) \leq 5(2^{k_1}q_1)^2 + 10q_1^2$. We distinguish the subcase $k_1 = 1$ from the one where $k_1 \geq 2$. If $k_1 \geq 2$ we have $10q_1^2 < (2^2q_1)^2 \leq (2^{k_1}q_1)^2$. Hence,

$$\begin{aligned} 4n - 15\,\mathrm{SL}(D,n) &\geq 3(2^{k_1}q_1)^2 - 10q_1^2 - 12(2^{k_1}q_1) + 4 \\ &> 2(2^{k_1}q_1)^2 - 12(2^{k_1}q_1) + 4 \\ &= 2((2^{k_1}q_1)^2 - 6(2^{k_1}q_1) + 2). \end{aligned}$$

The roots of this polynomial are less than 6. So it is positive as soon as $2^{k_1}q_1 \geq 6$. As $k_1 \geq 2$, the only possibility in this case is $2^{k_1}q_1 = 4$, which implies $k_1 = 2$ and $q_1 = 1$ so that $p_1 = 3$ or 5, and $p_2 = 2^{k_1+1}q_1 \pm 1 = 7$ or 9, so that $n = 21$ or 35, and $\mathrm{SL}(D,n) = 5$.

In the other subcase ($k_1 = 1$), $\delta_2 = 1$ and hence $k_2 = 2$ and therefore

$$\begin{cases} n \geq (2q_1 - 1)(4q_1 - 1) & \text{with } q_1 \text{ odd,} \\ \mathrm{SL}(D,n) = 2q_1^2 - 2q_1 + 1 & \text{from (9).} \end{cases}$$

Hence,

$$\begin{aligned} 4n - 15\,\mathrm{SL}(D,n) &\geq 2q_1^2 + 6q_1 - 11 \\ &> 0 \text{ if } q_1 \neq 1. \end{aligned}$$

The remaining case is $q_1 = 1$. Since $k_1 = 1$ and $\delta_2 = 1$ so that $k_2 = 2$, this implies $n = 15$ and $\mathrm{SL}(D,n) = 1$. At this point, the result has been proved when $\delta_2 = 1$.

• Lastly, we consider the exceptional case $n = p_1p_2$, $\delta_2 = 0$ so that $k_1 = k_2$, and $q_1 = q_2$. Then we have

$$n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1) = 4^{k_1}q_1^2 - 1 \quad \text{with } \varepsilon(n) = -1,$$

$$\mathrm{SL}(D,n) = (q_1 - 1)^2 + \frac{4^{k_1} - 1}{3}q_1^2 \quad \text{as in (9).}$$

Hence,

$$\begin{aligned} 3(n - 2\,\mathrm{SL}(D,n)) &= 4^{k_1}q_1^2 - 4q_1^2 + 12q_1 - 9 \\ &\geq 12q_1 - 9 > 0. \end{aligned}$$

Therefore, $\mathrm{SL}(D,n) < n/2$.

The case $s = 3$. Now, the case $s = 3$. By the second part of Lemma 2.3, it is sufficient to show that the inequality

$$\mathrm{SL}(D,n) \leq \frac{7}{48}\varphi_D(n) \tag{10}$$

holds.

• Lemma 5.2 implies the result under the following conditions:

$$\frac{\mathrm{SL}(D,n)}{\varphi_D(n)} \leq \begin{cases} 1/12 & \text{if } r_i \geq 2 \text{ for at least one } i, \\ 1/8 & \text{if the } k_i\text{'s are not all equal,} \\ 1/12 & \text{if one of the } q_i\text{'s does not divide } q, \end{cases}$$

because the inequality (10) is then satisfied.

• In the remaining case, we have

$$n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1}q_2 + \varepsilon_2)(2^{k_1}q_3 + \varepsilon_3)$$

with q_1, q_2 and q_3 odd and dividing $n - \varepsilon(n) = 2^{k_1}q$. The formula of Theorem 1.5 can be written

$$\begin{aligned} \mathrm{SL}(D,n) &= (q_1 - 1)(q_2 - 1)(q_3 - 1) + (1 + 8 + \cdots + 8^{k_1 - 1})q_1q_2q_3 \\ &= (q_1 - 1)(q_2 - 1)(q_3 - 1) + \frac{8^{k_1} - 1}{7}q_1q_2q_3. \end{aligned}$$

But, $\varphi_D(n) = 8^{k_1}q_1q_2q_3$ so, the inequality (10) can be written

$$(q_1 - 1)(q_2 - 1)(q_3 - 1) + \frac{8^{k_1} - 1}{7}q_1q_2q_3 \leq \frac{7}{48}8^{k_1}q_1q_2q_3$$

or more simply,

$$(q_1 - 1)(q_2 - 1)(q_3 - 1) \leq \left(\frac{8^{k_1}}{336} + \frac{1}{7}\right)q_1q_2q_3.$$

This is satisfied as soon as

$$\left(\frac{8^{k_1}}{336}+\frac{1}{7}\right)\geq 1$$

and in particular as soon as $k_1 \geq 3$. So we can assume that k_1 equals 1 or 2.

- We handle first the case $k_1 = 2$, that is

$$n = (4q_1+\varepsilon_1)(4q_2+\varepsilon_2)(4q_3+\varepsilon_3)$$

with q_1, q_2, q_3 odd and dividing $n - \varepsilon(n) = 4q$. Suppose that $q_1 = q_2 = 1$, so that $\varepsilon_1 = -\varepsilon_2$ and $\{p_1, p_2\} = \{3, 5\}$. Then $\varepsilon(n) = -\varepsilon_3$ and

$$4q = n - \varepsilon(n) = 15(4q_3+\varepsilon_3)+\varepsilon_3 = 60q_3 + 16\varepsilon_3.$$

As $q_3|q$, this implies $q_3|16$, so $q_3 = 1$, which is impossible because the prime p_1, p_2, p_3 are distinct.

Hence, we can assume that $q_2 \geq 3$ and $q_3 \geq 3$ since the ordering of the primes is arbitrary here. Then since

$$\begin{aligned} n &\geq (4q_1-1)(4q_2-1)(4q_3-1) \\ &= 64q_1q_2q_3 - 16(q_1q_2+q_1q_3+q_2q_3)+4(q_1+q_2+q_3)-1 \end{aligned}$$

and since

$$\mathrm{SL}(D,n) = 10q_1q_2q_3 - (q_1q_2+q_1q_3+q_2q_3)+(q_1+q_2+q_3)-1$$

we can see that

$$\begin{aligned} 4n - 15\,\mathrm{SL}(D,n) &\geq 106q_1q_2q_3 - 49(q_1q_2+q_1q_3+q_2q_3)+(q_1+q_2+q_3)+11 \\ &= 106(q_1-1)(q_2-3)(q_3-3) \\ &\quad + 269(q_1-1)(q_2-3)+269(q_1-1)(q_3-3)+57(q_2-3)(q_3-3) \\ &\quad + 661(q_1-1)+123(q_2-3)+123(q_3-3)+237 \\ &> 0. \end{aligned}$$

- Now, we consider the case where $k_1 = 1$, that is

$$n = (2q_1+\varepsilon_1)(2q_2+\varepsilon_2)(2q_3+\varepsilon_3)$$

with q_1, q_2, q_3 odd and dividing $n-\varepsilon(n) = 2q$. First, assume that $q_1 = 1$, so $p_1 = 3$. Then $p_2, p_3 \geq 5$ so $q_2, q_3 \geq 3$ and

$$n = 3(2q_2+\varepsilon_2)(2q_3+\varepsilon_3) \geq 3(2q_2-1)(3q_3-1), \quad \mathrm{SL}(D,n) = q_2q_3.$$

Hence,

$$\begin{aligned} 4n - 15\,\mathrm{SL}(D,n) &\geq 12(2q_2-1)(2q_3-1) - 15q_2q_3 = 33q_2q_3 - 24q_2 - 24q_3 + 12 \\ &= 33(q_2-3)(q_3-3)+75(q_2-3)+75(q_3-3)+165 > 0. \end{aligned}$$

So we can assume that all q_i's are greater than 1. But $q_i = 3$ only if $p_i = 5$ or 7. If $q_1 = q_2 = 3$, then $\{p_1, p_2\} = \{5, 7\}$ and $q_3 \geq 5$. In this case $n = 5 \cdot 7(2q_3+\varepsilon_3)$ and $\mathrm{SL}(D,n) = 4(q_3-1)+9q_3$. Hence

$$\begin{aligned} 4n - 15\,\mathrm{SL}(D,n) &\geq 4\cdot 5\cdot 7(2q_3-1) - 60(q_3-1) - 135q_3 \\ &= 85q_3 - 80 = 85(q_3-5)+345 > 0. \end{aligned}$$

So we can assume that $q_1 \geq 3$ and $q_2, q_3 \geq 5$. But $q_i = 5$ only if $p_i = 11$. So we can assume that $q_2 \geq 5$ and $q_3 \geq 7$. We have

$$\begin{aligned} n &\geq (2q_1 - 1)(2q_2 - 1)(2q_3 - 1) \\ &= 8q_1q_2q_3 - 4(q_1q_2 + q_1q_3 + q_2q_3) + 2(q_1 + q_2 + q_3) - 1, \end{aligned}$$

$$\mathrm{SL}(D, n) = (q_1 - 1)(q_2 - 1)(q_3 - 1) + q_1q_2q_3.$$

From this we easily deduce (if we are lucky to have good computing tools at hand) that

$$\begin{aligned} 4n - 15\,\mathrm{SL}(D, n) &\geq 2q_1q_2q_3 - (q_1q_2 + q_1q_3 + q_2q_3) - 7(q_1 + q_2 + q_3) + 11 \\ &= 2(q_1 - 3)(q_2 - 5)(q_3 - 7) \\ &\quad + 13(q_1 - 3)(q_2 - 5) + 9(q_1 - 3)(q_3 - 7) + 5(q_2 - 5)(q_3 - 7) \\ &\quad + 51(q_1 - 3) + 25(q_2 - 5) + 15(q_3 - 7) + 45. \end{aligned}$$

This proves that $4n - 15\,\mathrm{SL}(D, n) > 0$ because we have assumed $q_1 \geq 3$, $q_2 \geq 5$, $q_3 \geq 7$.

The case $s \geq 4$. Lastly, the case where $s \geq 4$. Lemma 5.2 shows that

$$\mathrm{SL}(D, n) \leq \varphi_D(n)/2^{s-1} = \frac{1}{2^{s-4}}\varphi_D(n)/8.$$

Using the inequality 2.3, we obtain

$$\mathrm{SL}(D, n) \leq \frac{96}{385}\left(\frac{7}{13}\right)^{s-4} n \leq \frac{96}{385}n \leq \frac{4}{15}n.$$

This finally (!) concludes the proof. □

7. Worst cases and better bounds

Twin primes. We have noted that the only numbers n such that $\mathrm{SL}(D, n) > \frac{4}{15}n$ are products

$$n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$$

of twin primes with q_1 odd and $\varepsilon(2^{k_1}q_1 - 1) = -1$, $\varepsilon(2^{k_1}q_1 + 1) = 1$. The proof of Theorem 1.3 shows that in fact, we then have

$$n/3 \leq \mathrm{SL}(D, n) \leq n/2. \tag{11}$$

If there are infinitely many twin primes $p_1 < p_2$ satisfying the conditions $(D/p_1) = -1$ and $(D/p_2) = 1$, then there are infinitely many n such that relations (11) hold. If p_1, p_2 are such twin primes satisfying the additional condition $k_1 = 1$ (that is $p_1 \equiv 1$ modulo 4), then for $n = p_1p_2$, we have

$$\frac{\mathrm{SL}(D, n)}{n} = \frac{(q_1 - 1)^2 + \frac{4^{k_1 - 1}}{3}q_1^2}{4^{k_1}q_1^2 - 1} = \frac{(q_1 - 1)^2 + q_1^2}{4q_1^2 - 1} = \frac{2q_1^2 - 2q_1 + 1}{4q_1^2 - 1}.$$

This shows that $\mathrm{SL}(D, n)/n$ tends to $1/2$ as q_1 tends to $+\infty$. So, under the assumption that there are infinitely many such twin primes, we can find numbers n such that $\mathrm{SL}(D, n)/n$ is as close as we want to $1/2$. However, note that such numbers are easy to spot, so they do not really represent a nuisance for primality testing.

Example. Let $D = 2$ and $n = 1\ 000\ 037 \cdot 1\ 000\ 039 = 1\ 000\ 076\ 001\ 443$. Then $\mathrm{SL}(D, n) = 500\ 037\ 000\ 685$ and $1/2 - \mathrm{SL}(D, n)/n < 10^{-6}$.

The bound $4/15$. Among numbers n such that $\mathrm{SL}(D,n)$ does to exceed $\frac{4}{15}n$, consider those such that

$$n = p_1p_2p_3 \equiv 1 \text{ modulo } 4, \quad \varepsilon(p_i) = -1, \text{ and } p_i + 1 | n+1 \quad \text{for } i = 1,2,3$$

(these numbers were already encountered in [10]). We have, in this case,

$$\mathrm{SL}(D,n) = (q_1 - 1)(q_2 - 1)(q_3 - 1) + q_1q_2q_3$$

which can be greater than $n/4$, and very close to $4/15n$. For example, consider the following

Example. Let $D = 7$ and $n = 20705$, so that

$$p_1 = 5, \quad p_2 = 41, \quad p_3 = 101,$$
$$\varepsilon(p_1) = \varepsilon(p_2) = \varepsilon(p_3) = \varepsilon(n) = -1,$$
$$p_1 + 1 = 2q_1 = 2 \cdot 3, \quad p_2 + 1 = 2q_2 = 2(3 \cdot 7), \quad p_3 + 1 = 2q_3 = 2(3 \cdot 17),$$
$$n + 1 = 2q = 2(3 \cdot 7 \cdot 17 \cdot 29),$$
$$\mathrm{SL}(7, 20705) = 5213.$$

Better bounds. There exist several ways to improve the Lucas test in order to make it more secure. One good idea yet found in [4] and [8] is to combine a Rabin-Miller test and a "true" (i.e. with $(D/n) = -1$) Lucas test. Such a combination seems much more secure than one might expect considering each test separately. But no precise result is known about this fact.

Another approach is found in [6] where a strong test derived from the strong Lucas test is defined. It is shown that there the probability of error in each iteration of this new test is less than $1/8$.

References

1. F. Arnault, *Rabin-Miller primality test: Composite numbers which pass it*, Math. Comp. **64** (1995), 355–361. MR **95c:**11152
2. ———, *Constructing Carmichael numbers which are strong pseudoprimes to several bases*, J. Symbolic Comput. **20** (1995), 151–161. CMP 96:08
3. F. Arnault and G. Robin, *Sur une fonction associée aux entiers quadratiques*, Preprint.
4. R. Baillie and S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35** (1980), 1391–1417. MR **81j:**10005
5. G. Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), 915–926. MR **94d:**11004
6. Z. Mo and J. P. Jones, *A new probabilistic primality test using Lucas sequences*, Preprint.
7. L. Monier, *Evaluation and comparison of two efficient primality testing algorithms*, Theoret. Comput. Sci. **11** (1980), 97–108. MR **82a:**68078
8. C. Pomerance, J. L. Selfridge, and S. S. Wagstraff, *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026. MR **82g:**10030

→ M. O. Rabin, *Probabilistic algorithms for testing primality*, J. Number Theory **12** (1980), 128–138. MR **81f:**10003

10. H. C. Williams, *On numbers analogous to the Carmichael numbers*, Canad. Math. Bull. **20** (1977), 133–143. MR **56:**5414

Université de Limoges, Faculté des Sciences, URA 1586, Laboratoire d'Arithmétique de Calcul formel et d'Optimisation, 123, av Albert Thomas, 87060 Limoges Cedex, France

E-mail address: arnault@unilim.fr