Developments on primality tests based on linear recurrent sequences of degree two

Rendiconti Sem. Mat. Univ. Pol. Torino
Vol. 80, 2022 (2022), 17 – 27

S. Dutto

DEVELOPMENTS ON PRIMALITY TESTS BASED ON LINEAR RECURRENT SEQUENCES OF DEGREE TWO

Abstract. Some probabilistic primality tests, like the strong Lucas test that is part of the widely used Baillie-PSW test, are defined through linear recurrent sequences. When adopting linear recurrent sequences of degree two, the simple version of the Lucas test as well as tests based on the Pell hyperbola can be generalized obtaining new powerful primality tests. This paper describes a deeper analysis of these two generalized tests in order to find the best parameters by number of pseudoprimes, i.e., the instances of the tests with less composite integers that are declared primes. The Selfridge method for choosing the parameters of the Lucas test can be adapted to the generalized tests and, when adopting the parameters among those with best statistical results, the resulting tests have no pseudoprimes up to 2^{44}.

1. Introduction

The problem of deciding whether an integer is prime is very important from a theoretical point of view, but also for applications like public-key cryptography, for example in the RSA cryptosystem, which security relies on the integer factorization problem [22].

Primality (or compositeness) tests are implemented exploiting theoretical properties and can be classified depending on the reliability of their results:

- *deterministic* tests give a sure result but have high computational costs. Between them, the *AKS test* [1] is the only unconditional deterministic algorithm able to determine in polynomial time the primality of an integer n. Its complexity is $\tilde{O}(\log^6 n)$ as proved in [12], but it has very slow practical applications;
- *probabilistic* tests, which are the focus of this paper, have provable bounds on the probability of false positive results, moreover they are the most used because of the good trade off between reliability and performance.

The most used probabilistic tests are the Rabin-Miller test and the Baillie-PSW test. They both include the *strong Fermat test*, which declares an odd integer n probable prime for a base $a \in \mathbb{Z}$ if $\gcd(n,a) = 1$, $n-1 = 2^r s$ with s odd and

$$a^s \equiv 1 \pmod{n} \quad \text{or} \quad a^{2^k s} \equiv -1 \pmod{n} \quad \text{for some } 0 \leq k < r.$$

A composite n that satisfies this condition is called *strong pseudoprime to base a* and it is proven in [19] that a composite n is a strong pseudoprime to at most one quarter of all bases $a \in \mathbb{Z}$.

This property is the fundamental idea behind the *Rabin-Miller test* [15, 19], which tests the integer n by applying the strong Fermat test for k different bases and declares n probably prime with a probability at most 4^{-k}.

The *Baillie-PSW test* [3,18], instead, combines the strong Fermat test with base $a = 2$ and the strong Lucas test. The latter exploits two *Lucas sequences* [9] that, given the parameters $P, Q \in \mathbb{Z}$, are defined as

$$(1) \qquad \begin{cases} U_0 = 0, \quad U_1 = 1, \\ U_k = PU_{k-1} - QU_{k-2}, \quad \text{if } k > 1, \end{cases} \qquad \begin{cases} V_0 = 2, \quad V_1 = P, \\ V_k = PV_{k-1} - QV_{k-2}, \quad \text{if } k > 1. \end{cases}$$

Given $D = P^2 - 4Q$ and $j = \left(\frac{D}{n}\right)$ the Jacobi symbol of D over n, the *strong Lucas test* declares an odd integer n probable prime for the parameters $P, Q \in \mathbb{Z}$ if $j \neq 0$, $\gcd(n, Q) = 1$, $n - j = 2^r s$ with s odd and

$$U_s \equiv 0 \pmod{n} \quad \text{or} \quad V_{2^k s} \equiv 0 \pmod{n} \quad \text{for some } 0 \leq k < r.$$

The parameters $P, Q \in \mathbb{Z}$ are usually selected depending on n through the Selfridge method [3] such that:

- D is taken as the first element in $\{5, -7, 9, -11, \ldots\}$ such that $j = \left(\frac{D}{n}\right) = -1$;
- $P = 1$, $Q = \frac{1-D}{4}$.

It is conjectured that there are infinitely many BailliePSW pseudoprimes [16], i.e., composite n that are declared primes by both the strong Fermat test with base $a = 2$ and the strong Lucas test with parameters selected with the Selfridge method. However, no one has found a BailliePSW pseudoprime yet [6].

The strong Lucas test has a simpler version called *Lucas test*, which considers only the sequence $(U_k)_{k \geq 0}$ and declares an odd integer n probable prime for the parameters $P, Q \in \mathbb{Z}$ with $D = P^2 - 4Q$ if $j = \left(\frac{D}{n}\right) \neq 0$, $\gcd(n, Q) = 1$ and

$$U_{n-j} \equiv 0 \pmod{n}.$$

A composite n that passes this test is called *Lucas pseudoprime with parameters P, Q*.

Lucas pseudoprimes have been widely studied [7, 10, 17, 20, 21], as well as the idea of primality tests using more general linear recurrence sequences [11, 13].

In particular, in [8] the Lucas test is related with a test based on the points of a *Pell hyperbola*. This is a curve depending on a parameter $D \in \mathbb{Z}$ and is defined through the Pell equation [4] as $\mathscr{C}_D = \{(x, y) \in \mathbb{Z}_n^2 \,|\, x^2 - Dy^2 \equiv 1 \pmod{n}\}$. If n is prime, this set with the *Brahmagupta product*

$$(2) \qquad (x_1, y_1) \otimes (x_2, y_2) = (x_1 x_2 + D y_1 y_2, x_1 y_2 + y_1 x_2) \pmod{n},$$

is a cyclic group of order $n - j$ with $j = \left(\frac{D}{n}\right) \neq 0$ [14].

The group structure allows to define the *Pell test* [8], which declares an odd integer n probable prime for the parameters $D \in \mathbb{Z}$ and $(\tilde{x}, \tilde{y}) \in \mathscr{C}_D$ with $j = \left(\frac{D}{n}\right) \neq 0$ if

$$y_{n-j} \equiv 0 \pmod{n}, \quad \text{where } \left(x_{n-j}, y_{n-j}\right) = (\tilde{x}, \tilde{y})^{\otimes (n-j)}.$$

A composite n that passes this test is called *Pell pseudoprime with parameters D,* $(\tilde{x},\tilde{y})$.

In particular, an integer that passes the Pell test with parameters $D \in \mathbb{Z}$ and $(\tilde{x},\tilde{y}) \in \mathscr{C}_D$ passes also the Lucas test with parameters $P = 2\tilde{x}, Q = 1$. On the other hand, if n passes the Lucas test with parameters $P \in \mathbb{Z}, Q = 1$, then n passes the Pell test with parameters $D = P^2 - 4, (\tilde{x},\tilde{y}) = (P/2, 1/2) \in \mathscr{C}_D$.

In [5], generalizations of the Lucas and Pell tests through linear recurrent sequences of degree two have been introduced, and this work describes a deeper analysis of these primality tests. In Section 2, the setting and the main result from [5] is recalled, while Sections 3 and 4 focus on new results about the choice of parameters for the generalized Pell test and the generalized Lucas test, respectively. Finally, Section 5 shows some new results on these tests when their parameters are fixed and when adaptations of the Selfridge method for choosing the parameters are adopted.

2. Linear recurrent sequences for primality tests

The Pell test can be improved by considering both the coordinates of the obtained point. The result is the *strong Pell test* [5], which declares an odd integer n probable prime for the parameters $D \in \mathbb{Z}$ and $(\tilde{x},\tilde{y}) \in \mathscr{C}_D$ with $j = \left(\frac{D}{n}\right) \neq 0$ if

$$\left(x_{n-j}, y_{n-j}\right) = (\tilde{x},\tilde{y})^{\otimes(n-j)} = (1,0) \in \mathscr{C}_D.$$

A composite n that passes this test is called strong *Pell pseudoprime with parameters D,* $(\tilde{x},\tilde{y})$. The check in this test can be written in a matrix form as

$$\begin{pmatrix} x_{n-j} \\ y_{n-j} \end{pmatrix} = \begin{pmatrix} \tilde{x} & D\tilde{y} \\ \tilde{y} & \tilde{x} \end{pmatrix}^{n-j} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \pmod{n}. \tag{3}$$

This structure can be generalized by considering that any matrix $M \in \mathbb{Z}^{2\times 2}$ generates the linear recurrent sequences

$$\begin{pmatrix} \tilde{V}_k \\ \tilde{U}_k \end{pmatrix} = M^k \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \text{for } k \geq 0,$$

and the following result holds [5].

LEMMA 1. *Let D be the discriminant of the characteristic polynomial of the matrix $M \in \mathbb{Z}^{2\times 2}$. If p is prime and* $\det(M) \not\equiv 0 \pmod{p}$*, then*

1. $(\tilde{V}_{p-1}, \tilde{U}_{p-1}) \equiv (1,0) \pmod{p}$*, when* $\sqrt{D} \in \mathbb{Z}_p^{\times}$*;*
2. $(\tilde{V}_{p+1}, \tilde{U}_{p+1}) \equiv \left(\det(M), 0\right) \pmod{p}$*, when* $\sqrt{D} \notin \mathbb{Z}_p^{\times}$.

Therefore, given the sequences $(\tilde{U}_k)_{k\geq 0}, (\tilde{V}_k)_{k\geq 0}$ generated by $M \in \mathbb{Z}^{2\times 2}$ with $\gcd(n, \det(M)) = 1$ and D discriminant of the characteristic polynomial, new primality

tests can be defined by declaring an odd integer n probable prime if $j = \left(\frac{D}{n}\right) \neq 0$ and

$$(\tilde{V}_{n-j}, \tilde{U}_{n-j}) \equiv \begin{cases} (1,0) \pmod{n}, & \text{if } j = 1, \\ (\det(M), 0) \pmod{n}, & \text{if } j = -1. \end{cases}$$

The strong Pell test is an example of this construction, but also the Lucas test can be improved by considering the sequence $(U_k)_{k\geq 0}$ as generated by

$$\begin{pmatrix} U_{k+1} \\ U_k \end{pmatrix} = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}^k \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \text{for } k \geq 0. \tag{4}$$

This gives a second condition that defines the *double Lucas test* [5], which declares an odd integer n prime for the parameters $P, Q \in \mathbb{Z}$ with $D = P^2 - 4Q$ if $j = \left(\frac{D}{n}\right) \neq 0$, $\gcd(n, Q) = 1$ and

$$(U_{n+1-j}, U_{n-j}) \equiv \begin{cases} (1,0) \pmod{n}, & \text{if } j = 1, \\ (Q,0) \pmod{n}, & \text{if } j = -1. \end{cases}$$

As for the Lucas and Pell tests, there is an equivalence between double Lucas and strong Pell tests. In particular, if $P \in \mathbb{Z}$ and $Q = 1$, then the matrix in Eq. (4) is similar to one of the type in Eq. (3) through $\left(\begin{smallmatrix} 1 & P \\ 0 & 2 \end{smallmatrix}\right)$ and the resulting strong Pell test has parameters $D = P^2 - 4, (\tilde{x}, \tilde{y}) = (P/2, 1/2) \in \mathscr{C}_D$. The vice versa is also true since the matrix in Eq. (3) is similar to one of the type in Eq. (4) through $\left(\begin{smallmatrix} 1 & -\tilde{x} \\ 0 & \tilde{y} \end{smallmatrix}\right)$, and the parameters of the resulting double Lucas test are $P = 2\tilde{x}, Q = 1$.

3. Generalized Pell test

In order to obtain a relation between strong Pell tests and double Lucas tests with any Q, it is possible to consider the generalized Pell conic

$$\mathscr{C}_{D,Q} = \{(x,y) \in \mathbb{Z}_n^2 \,|\, x^2 - Dy^2 \equiv Q \pmod{n}\}.$$

Despite the product $\otimes$ introduced in Eq. (2) is no more well defined over $\mathscr{C}_{D,Q}$, taking a point $(\tilde{x}, \tilde{y}) \in \mathscr{C}_{D,Q}$ defines the linear recurrent sequences

$$\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} \tilde{x} & D\tilde{y} \\ \tilde{y} & \tilde{x} \end{pmatrix}^k \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \text{for } k \geq 0,$$

where the determinant of the matrix is $\tilde{x}^2 - D\tilde{y}^2 \equiv Q \pmod{n}$. Using Lemma 1 with $(\tilde{x}_k)_{k\geq 0}, (\tilde{y}_k)_{k\geq 0}$ returns the *generalized Pell test* [5], which declares an odd integer n probable prime for the parameters $D \in \mathbb{Z}$, $(\tilde{x}, \tilde{y}) \in \mathscr{C}_{D,Q}$ if $j = \left(\frac{D}{n}\right) \neq 0$, $\gcd(n, Q) = 1$ and

$$(x_{n-j}, y_{n-j}) \equiv \begin{cases} (1,0) \pmod{n}, & \text{if } j = 1, \\ (Q,0) \pmod{n}, & \text{if } j = -1. \end{cases}$$

A composite n that passes this test is called *generalized Pell pseudoprime with parameters D,* $(\tilde{x},\tilde{y})$.

In particular, if n passes the double Lucas test with parameters $P,Q \in \mathbb{Z}$ then n passes the generalized Pell test with parameters $D = P^2 - 4Q$ and $(\tilde{x},\tilde{y}) = (P/2, 1/2)$. On the other hand, if n passes the generalized Pell test with parameters $D \in \mathbb{Z}$ and $(\tilde{x},\tilde{y}) \in \mathscr{C}_{D,Q}$, then n passes the double Lucas test with parameters $P = 2\tilde{x}$, $Q = \tilde{x}^2 - D\tilde{y}^2$.

PROPOSITION 1. *The generalized Pell test is independent of the sign of the parameters* $\tilde{x},\tilde{y} \in \mathbb{Z}$.

Proof. Exponentiation with respect to the product $\otimes$ can be obtained by considering the isomorphism between $\mathscr{C}_{D,Q}$ and $\mathbb{Z}_n[t]/(t^2 - D)$ given by $(\tilde{x},\tilde{y}) \cong \tilde{x} + t\tilde{y}$, so that

$$(x_k, y_k) = (\tilde{x},\tilde{y})^{\otimes k} \cong (\tilde{x} + t\tilde{y})^k = A_k(D,\tilde{x},\tilde{y}) + tB_k(D,\tilde{x},\tilde{y}), \quad \text{for } k \geq 0,$$

where

$$x_k = A_k(D,\tilde{x},\tilde{y}) = \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i} D^i \tilde{x}^{k-2i} \tilde{y}^{2i},$$
$$y_k = B_k(D,\tilde{x},\tilde{y}) = \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i+1} D^i \tilde{x}^{k-2i-1} \tilde{y}^{2i+1}.$$

Since even integers can be easily declared composite, in the generalized Pell test the exponent is generally $n - j$ with $j = \left(\frac{D}{n}\right) = \pm 1$ and n odd, so that changing the sign of $\tilde{x}$ or $\tilde{y}$ results in obtaining

$$\begin{cases} A_{n-j}(D,\pm\tilde{x},\mp\tilde{y}) = A_{n-j}(D,\tilde{x},\tilde{y}), \\ B_{n-j}(D,\pm\tilde{x},\mp\tilde{y}) = -B_{n-j}(D,\tilde{x},\tilde{y}), \end{cases}$$

Thus, in the generalized Pell test, the check on x_{n-j} is the same in both cases, while $y_{n-j} = B_{n\pm1}(D,\tilde{x},\tilde{y}) \equiv 0 \pmod{n}$ if and only if $-B_{n\pm1}(D,\tilde{x},\tilde{y}) \equiv 0 \pmod{n}$. In conclusion, an integer n that passes the generalized Pell test for the parameters D and $(\tilde{x},\tilde{y})$ still passes it if the sign of $\tilde{x}$ or $\tilde{y}$ (or both) is changed, and vice versa. □

PROPOSITION 2. *The generalized Pell test is independent of the values of the parameters* $D,\tilde{y} \in \mathbb{Z} \setminus \{0\}$ *as long as* $D\tilde{y}^2$ *remains unchanged.*

Proof. The formulation in the previous proof can be written for any $k \geq 0$ as

$$x_k = A_k(D,\tilde{x},\tilde{y}) = \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i} \tilde{x}^{k-2i} (D\tilde{y}^2)^i,$$
$$y_k = B_k(D,\tilde{x},\tilde{y}) = \sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i+1} \tilde{x}^{k-2i-1} (D\tilde{y}^2)^i \tilde{y}.$$

Thus, if the parameters $D,\tilde{y}\in\mathbb{Z}$ and $D',\tilde{y}'\in\mathbb{Z}$ have $D\tilde{y}^2=D'\tilde{y}'^2$, then $j=\left(\frac{D}{n}\right)=\left(\frac{D'}{n}\right)$ and in the generalized Pell test the check on x_{n-j} uses $A_k(D,\tilde{x},\tilde{y})=A_k(D',\tilde{x},\tilde{y}')$, so that it is the same in both cases.

The check on y_{n-j} uses $B_k(D,\tilde{x},\tilde{y})=\tilde{y}B_k(D\tilde{y}^2,\tilde{x},1)$, with $\tilde{y}\neq 0$, so that it becomes $B_{n-j}(D,\tilde{x},\tilde{y})\equiv 0 \pmod{n}$ if and only if $B_{n-j}(D\tilde{y}^2,\tilde{x},1)\equiv 0 \pmod{n}$. An analogous results can be obtained with $D',\tilde{y}'\in\mathbb{Z}$, i.e., $B_k(D',\tilde{x},\tilde{y}')=\tilde{y}'B_k(D'\tilde{y}'^2,\tilde{x},1)$, with $\tilde{y}'\neq 0$, so that $B_{n-j}(D',\tilde{x},\tilde{y}')\equiv 0 \pmod{n}$ if and only if $B_{n-j}(D'\tilde{y}'^2,\tilde{x},1)\equiv 0 \pmod{n}$, and the thesis is confirmed because $D\tilde{y}^2=D'\tilde{y}'^2$ and $j=\left(\frac{D}{n}\right)=\left(\frac{D'}{n}\right)$. □

4. Generalized Lucas test

Lemma 1 allows also to generalize the double Lucas test. In particular, considering the parameters $P,Q,R\in\mathbb{Z}$, the linear recurrent sequences

$$\begin{pmatrix}\tilde{V}_k\\ \tilde{U}_k\end{pmatrix}=\begin{pmatrix}P & -Q\\ R & 0\end{pmatrix}^k\begin{pmatrix}1\\ 0\end{pmatrix},\quad \text{for } k\geq 0, \tag{5}$$

define the *generalized Lucas test* [5], which declares an odd integer n probable prime for the parameters $P,Q,R\in\mathbb{Z}$ with $D=P^2-4QR$ if $j=\left(\frac{D}{n}\right)\neq 0$, $\gcd(n,QR)=1$ and

$$(\tilde{V}_{n-j},\tilde{U}_{n-j})\equiv\begin{cases}(1,0) \pmod{n}, & \text{if } j=1,\\ (QR,0) \pmod{n}, & \text{if } j=-1.\end{cases}$$

A composite n that passes this test is called *generalized Lucas pseudoprime with parameters P, Q, R*.

PROPOSITION 3. *The generalized Lucas test is independent of the sign of the parameter $P\in\mathbb{Z}$.*

Proof. The linear recurrent sequences defined in Eq. (5) are a generalization of Lucas sequences introduced in Eq. (1), and can be described as

$$\begin{cases}\tilde{U}_0=0,\quad \tilde{U}_1=R,\\ \tilde{U}_k=P\tilde{U}_{k-1}-QR\tilde{U}_{k-2},\quad \text{if } k>1,\end{cases}\qquad\begin{cases}\tilde{V}_0=1,\quad \tilde{V}_1=P,\\ \tilde{V}_k=P\tilde{V}_{k-1}-QR\tilde{V}_{k-2},\quad \text{if } k>1,\end{cases} \tag{6}$$

If the sign of the parameter $P\in\mathbb{Z}_n$ is changed, then the obtained sequences are

$$\begin{cases}\tilde{U}'_0=0,\quad \tilde{U}'_1=R,\\ \tilde{U}'_k=-P\tilde{U}'_{k-1}-QR\tilde{U}'_{k-2},\quad \text{if } k>1,\end{cases}\qquad\begin{cases}\tilde{V}'_0=1,\quad \tilde{V}'_1=-P,\\ \tilde{V}'_k=-P\tilde{V}'_{k-1}-QR\tilde{V}'_{k-2},\quad \text{if } k>1,\end{cases}$$

and for any $k\geq 0$

$$\tilde{U}'_k=\begin{cases}-\tilde{U}_k & \text{if } k \text{ is even},\\ \tilde{U}_k & \text{if } k \text{ is odd},\end{cases}\qquad\tilde{V}'_k=\begin{cases}\tilde{V}_k & \text{if } k \text{ is even},\\ -\tilde{V}_k & \text{if } k \text{ is odd}.\end{cases}$$

This can be verified by induction on the index k:

- when $k = 0$ or $k = 1$ the thesis is confirmed;
- if $k > 1$ is even, then assuming the thesis true for $k-1$ and $k-2$ results in

$$\begin{cases} \tilde{U}'_k = -P\tilde{U}'_{k-1} - QR\tilde{U}'_{k-2} = -P\tilde{U}_{k-1} + QR\tilde{U}_{k-2} = -\tilde{U}_k, \\ \tilde{V}'_k = -P\tilde{V}'_{k-1} - QR\tilde{V}'_{k-2} = P\tilde{V}_{k-1} - QR\tilde{V}_{k-2} = \tilde{V}_k; \end{cases}$$

- if $k > 1$ is odd, then assuming the thesis true for $k-1$ and $k-2$ results in

$$\begin{cases} \tilde{U}'_k = -P\tilde{U}'_{k-1} - QR\tilde{U}'_{k-2} = P\tilde{U}_{k-1} - QR\tilde{U}_{k-2} = \tilde{U}_k, \\ \tilde{V}'_k = -P\tilde{V}'_{k-1} - QR\tilde{V}'_{k-2} = -P\tilde{V}_{k-1} + QR\tilde{V}_{k-2} = -\tilde{V}_k. \end{cases}$$

In the generalized Lucas test, $k = n \pm 1$ with n odd, so that the interesting case is k even. Thus, when changing the sign of P, the check on $\tilde{V}_k$ remains unchanged, while $\tilde{U}_{n\pm1} \equiv 0 \pmod{n}$ is satisfied iff $-\tilde{U}_{n\pm1} \equiv 0 \pmod{n}$. □

This result is true for all tests based on Lucas sequences, so that when studying these tests with fixed parameters for testing different integers, it is sufficient to focus only on the instances with $P \geq 0$.

PROPOSITION 4. *The generalized Lucas test is independent of the choice of $Q, R \in \mathbb{Z}$, as long as the value of QR remains unchanged.*

Proof. The generalized Lucas sequences with parameters $P, Q, R \in \mathbb{Z}$ can be compared with the classic Lucas sequences with parameters $P, Q' = QR$. By induction on the index $k > 0$ it is possible to prove that $\tilde{U}_k = RU_k$ and $\tilde{V}_k = V_k$:

- if $k = 0$, then $\tilde{U}_0 = RU_0 = 0$ and $\tilde{V}_0 = V_0 = 1$;
- if $k = 1$, then $\tilde{U}_1 = RU_1 = R$ and $\tilde{V}_1 = V_1 = P$;
- if $k > 1$, then assuming the thesis true for $k-1$ and $k-2$ results in having

$$\begin{aligned} \tilde{U}_k &= P\tilde{U}_{k-1} - QR\tilde{U}_{k-2} = PRU_{k-1} - QR^2U_{k-2} \\ &= R(PU_{k-1} - Q'U_{k-2}) = RU_k, \end{aligned}$$

  as well as

$$\begin{aligned} \tilde{V}_k &= P\tilde{V}_{k-1} - QR\tilde{V}_{k-2} = PV_{k-1} - QRV_{k-2} \\ &= PV_{k-1} - Q'V_{k-2} = V_k. \end{aligned}$$

Thus, the generalized tests with parameters $P, Q, R \in \mathbb{Z}$ is equivalent to the double Lucas test with parameters $P, Q' = QR$.

Given two generalized Lucas tests with parameters $P, Q, R \in \mathbb{Z}$ and $P, Q', R' \in \mathbb{Z}$, respectively, if $QR = Q'R'$, then they are both equivalent to the same double Lucas test and the thesis is verified. □

D	$\tilde{x}$	0			1			2			3			μ_D
	$\tilde{y}$	1	2	3	1	2	3	1	2	3	1	2	3	
5		108	144	126	17	11	14	178	11	14	19	7	17	56
-7		102	104	137	11	3	21	3	7	10	9	5	6	35
-11		92	156	157	4	6	12	4	7	8	2	8	7	39
13		106	120	132	7	2	8	4	8	10	6	4	4	34
-15		81	118	156	8	15	10	5	24	10	7	9	15	38
17		108	187	109	12	8	5	6	12	5	8	5	6	39
$\mu_{(\tilde{x},\tilde{y})}$		100	138	136	10	8	12	33	12	10	9	6	9	

Table 2.1: Number of generalized Pell pseudoprimes up to 2^{20} for different parameters $D,(\tilde{x},\tilde{y})$ and their arithmetic means $\mu_D,\mu_{(\tilde{x},\tilde{y})}$ with fixed D or $(\tilde{x},\tilde{y})$, respectively.

Despite this equivalence makes the generalized Lucas test less important, adapting the Selfridge method gives very interesting results. As for the other tests based on Lucas sequences, the idea is to test the integer n with parameters that have discriminant D such that $\left(\frac{D}{n}\right)=-1$, so that the test is not equivalent to a strong Fermat test [3]. Therefore, the following algorithm for choosing the parameters is introduced:

1. fix $P,R>0$;
2. take the minimum $D\in\left\{P^2-4RQ\,|\,Q\in\mathbb{Z}\setminus\{0\}\right\}$ such that $\left(\frac{D}{n}\right)=-1$;
3. evaluate $Q=\frac{P^2-D}{4R}$.

In the following section, an analysis on the resulting number of pseudoprimes is performed, in order to find the best values for the parameters of the introduced tests.

5. Numerical experiments

Table 2.1 collects the number of pseudoprimes up to $2^{20}=1.048.576$ for the generalized Pell test with different choices of the parameters:

- D is taken among the first six non-square values used in the Selfridge method (the average number of D to be tried is less than 2 [3]), which are the interesting cases because of the relation between generalized Pell test and double Lucas test;
- $(\tilde{x},\tilde{y})$ has coordinates between 0 and 3, since negative values behave as positive ones because of Proposition 1. Points with coordinate $\tilde{y}=0$ can be excluded because Proposition 2 assures that they are equivalent to cases with $D=0$.

The collected data strongly depend on the values of the parameters. However, their arithmetic means for fixed D or $(\tilde{x},\tilde{y})$, shown in the last column and row, respectively, allow to understand which values can be considered more reliable, for example in an adaptation of the Selfridge method introduced in Section 1.

In particular, if the parameters for the generalized Pell test are chosen as:

Q	P	0			1			2			3			μ_Q
	R	1	2	3	1	2	3	1	2	3	1	2	3	
1		-	118	128	-	2	6	-	118	9	165	251	128	103
-1		-	118	128	60	223	4	121	18	250	74	4	5	91
2		118	251	140	2	20	4	118	223	4	251	13	7	96
-2		118	251	140	223	8	60	18	17	6	4	409	9	105
3		128	140	250	6	4	6	9	4	25	128	7	250	80
-3		128	140	250	4	60	11	250	6	9	5	9	9	73
$\mu_{P,R}$		123	170	173	59	53	15	103	64	51	105	116	68	

Table 2.2: Number of generalized Lucas pseudoprimes up to 2^{20} for different parameters P,Q,R and their arithmetic means $\mu_Q,\mu_{P,R}$ with fixed Q or P,R, respectively.

- D first element in $\{5,-7,9,-11,\ldots\}$ such that $j=\left(\frac{D}{n}\right)=-1$;
- $(\tilde{x},\tilde{y})=(3,2)$, the case with lowest arithmetic mean in Table 2.1;

then, when testing all the integers up to $2^{44}=17.592.186.044.416$, only primes were declared primes, i.e., no generalized Pell pseudoprime was found.

Analogously, Table 2.2 shows the number of pseudoprimes up to 2^{20} for the generalized Lucas test with different choices of the parameters, namely for the integers $0\le P\le 3, 1\le R\le 3$ and the first six Q obtained by the Selfridge method. Negative values of P can be excluded thanks to Proposition 3, while Proposition 4 assures that, if Q is taken among positive and negative integers, then it is possible to consider only positive values of R. Since cases with same value of QR are equivalent, they return the same number of pseudoprimes, but they are collected in order to study the behavior of the test with fixed P,R for the adaptation of the Selfridge method.

Some trivial cases are excluded because they generate sequences for which Eq. (5) is satisfied by most of the odd integers, namely:

- $P=0$, $Q=R=1$, related to the matrix $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$ that has period 4;
- $P=0$, $Q=-1$, $R=1$, related to the matrix $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ that has period 2;
- $P=Q=R=1$, related to the matrix $\left(\begin{smallmatrix}1 & -1\\ 1 & 0\end{smallmatrix}\right)$ that has period 6.

The case with $P=2$, $Q=R=1$ is also excluded since its discriminant D is zero. When $R=1$ the test is simply the double Lucas tests, but these cases are included for the sake of completeness, as well as the cases with $P=0$ in which $\tilde{U}_{2k}=0\ \forall k\ge 0$, i.e., in the test only the check on $\tilde{V}_{n-j}=(-QR)^{\frac{n-j}{2}}$ is significant.

The collected quantities strongly depend on the chosen parameters. Table 2.2 contains also the arithmetic means of the values for fixed Q in the last column and for fixed P,R in the last row, which allow to understand what are the most reliable choices.

When adapting the Selfridge method to the generalized Lucas test, the best choices for the fixed parameters and the consequent set of possible values of D are, in order of best statistical results:

1. $P = 1$, $R = 3$ and $D \in \{-11, 13, -23, 25, \ldots\}$;
2. $P = 2$, $R = 3$ and $D \in \{-8, 16, -20, 28, \ldots\}$;
3. $P = 1$, $R = 2$ and $D \in \{-7, 9, -15, 17, \ldots\}$;
4. $P = 1$, $R = 1$ and $D \in \{5, -7, 9, -11, \ldots\}$ that gives the double Lucas test with the Selfridge method, with 5777 as first pseudoprime.

In all these cases, D is taken as the minimum with $\left(\frac{D}{n}\right) = -1$ and $Q = \frac{P^2 - D}{4R}$.

In particular, when testing the integers up to 2^{44} with the parameters obtained through method 1, only primes were declared primes, i.e., no generalized Lucas pseudoprime with parameters $P = 1$, $R = 3$ and Q from the Selfridge method was found.

References

[1] AGRAWAL M. AND KAYAL N. AND SAXENA N., *PRIMES is in P*, Ann. of Math. **160** 2 (2004), 781–793.

[2] ALFORD W.R. AND GRANVILLE A. AND POMERANCE C., *There are infinitely many Carmichael numbers*, Ann. of Math. **140** (1994), 703–722.

[3] BAILLIE R. AND WAGSTAFF S.S., *Lucas pseudoprimes*, Math. Comp. **35** 152 (1980), 1391–1417.

[4] BARBEAU E.J., *Pells Equation*, Springer-Verlag, New York-Berlin 2003.

[5] BAZZANELLA D. AND DI SCALA A.J. AND DUTTO S. AND MURRU N., *Primality tests, linear recurrent sequences and the Pell equation*, Ramanujan J. **57** (2022), 755–768.

[6] CHEN Z., GREENE J., *Some comments on Baillie-PSW pseudoprimes*, Fibonacci Quart. **41** 4 (2003), 334–344.

[7] DI PORTO A. AND FILIPPONI P., *A probabilistic primality test based on the properties of certain generalized Lucas numbers*, Advances in Cryptology – EUROCRYPT 88 (1988), 211–223.

[8] DI SCALA A.J. AND MURRU N. AND SANNA C., *Lucas pseudoprimes and the Pell conic*, arXiv:2001.00353 (2020).

[9] DICKSON L.E., *History of the Theory of Numbers, Vol. 1: Divisibility and Primality*, Dover Publications, New York 2005 (1919).

[10] GORDON D.M. AND POMERANCE C., *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** 196 (1991), 825–838.

[11] GRANTHAM J., *There are infinitely many Perrin pseudoprimes*, J. Number Theory **130** 5 (2010), 1117–1128.

[12] LENSTRA, H.W.JR. AND POMERANCE, C., *Primality testing with Gaussian periods*, J. Eur. Math. Soc. **21** 4 (2019), 1229–1269.

[13] LUCA F. AND SHPARLINSKI I.E., *Pseudoprimes in certain linear recurrences*, Albanian J. Math. **1** 3 (2007), 125–131.

[14] MENEZES A.J. AND VANSTONE S.A., *A note on cyclic groups, finite fields, and the discrete logarithm problem*, Appl. Algebra Eng. Commun. Comput. **3** (1992), 67–74.

[15] MILLER G.L., *Riemann's Hypothesis and Tests for Primality*, J. Comput. Syst. Sci. **13** 3 (1976), 300–317.

[16] POMERANCE C., *Are There Counterexamples to the Baillie-PSW Primality Test?*, unpublished (1984).

[17] POMERANCE C., *Primality testing: variations on a theme of Lucas*, Congr. Numer. **201** (2010), 301–312.

[18] POMERANCE C. AND SELFRIDGE J.L. AND WAGSTAFF S.S., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** 151 (1980), 1003–1026.

[19] RABIN M.O., *Probabilistic algorithm for testing primality*, J. Number Theory **12** 1 (1980), 128–138.

[20] SOMER L., *Lucas pseudoprimes of special types*, Fibonacci Quart. **47** 3 (2009), 198–206.

[21] SUWA N., *Some remarks on Lucas pseudoprimes*, Math. J. Okayama Univ. **54** (2012), 1–32.

[22] YAN S.Y., *Primality testing and integer factorization in public-key cryptography*, Springer-Verlag, New York-Berlin 2004.

AMS Subject Classification: 11Y11, 11B39

Simone DUTTO,
DISMA, Politecnico di Torino
Corso Duca degli Abruzzi 24, 10129 Turin, Italy
e-mail: simone.dutto@polito.it

Lavoro pervenuto in redazione il 07.03.2022.