Primality tests, linear recurrent sequences and the Pell equation

Danilo Bazzanella*, Antonio Di Scala*, Simone Dutto*, Nadir Murru**
* Politecnico of Turin, Corso Duca degli Abruzzi 24, Torino, 10129, ITALY
** University of Turin, Via Carlo Alberto 10, Torino, 10123, ITALY, Corresponding Author

Abstract

We study new primality tests based on linear recurrent sequences of degree two exploiting a matrix approach. The classical Lucas test arises as a particular case and we see how it can be easily improved. Moreover, this approach shows clearly how the Lucas pseudoprimes are connected to the Pell equation and the Brahamagupta product. We also introduce two new specific primality tests, which we will call generalized Lucas test and generalized Pell test. We perform some numerical computations on the new primality tests and we do not find any pseudoprime up to 2^{38}. Moreover, we combined the generalized Lucas test with the Fermat test up to 2^{64} and we did not find any composite number that passes the test. We get the same result using the generalized Pell test.

Keywords: linear recurrent sequence; Lucas pseudoprime; Pell equation; Pell pseudoprime; primality test.
2010 Mathematics Subject Classification: Primary: 11Y11; Secondary: 11B39.

1 Introduction

The problem of deciding whether an integer number is prime has very important applications, like in cryptography [22], and it is very important also from a theoretical point of view. One of the most classical primality test is based on the Little Fermat's Theorem, i.e., the Fermat test. It is known that there are infinitely many composite numbers that pass the test to every base [2]. However, it is possible to define a stronger test considering that for $p = 2^r s + 1$ prime, s odd, then

$$a^s \equiv 1 \pmod p \quad \text{or} \quad a^{2^k s} \equiv -1 \pmod p$$

for any $a \in \mathbb{Z}_p^*$ and some $0 \leq k < r$. An odd composite number satisfying this condition is a *strong pseudoprime* to base a and it is known that there are no strong pseudoprimes to all bases. See [17] for a classical study on these pseudoprimes. The famous Rabin–Miller test is based on these concepts and the unconditional version is just a probabilistic algorithm [18]. The only unconditional deterministic algorithm able to determine in polynomial time the primality of an integer number is the AKS primality test [1]. However, in practical applications, the AKS primality test is not used, because it is too slow despite the theoretical results. In fact, the most used primality test (together to the probabilistic version of Rabin–Miller) is the Baillie–PSW primality test that combines the above test with the Lucas test [3]; an overlap between strong and Lucas pseudoprimes has not been found so far. However, it is conjectured that there are infinitely many Baillie–PSW pseudoprimes and Pomerance gave an idea for constructing them [15]. Some calculations about the search of Baillie–PSW pseudoprimes can be also found in [6]. The Lucas test is based on some properties of the Lucas sequence. Given two integers P and Q the Lucas sequence is defined by

$$\begin{cases} U_0 = 0, U_1 = 1 \\ U_k = PU_{k-1} + QU_{k-2} \end{cases}$$

for any $k \geq 2$ and for any $k \geq 0$ we have

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta},$$

where α, β are the roots of the characteristic polynomial. The Lucas test is based on the fact that when p is prime, p does not divide D, we have

$$U_{p-1} \equiv 0 \pmod{p} \quad \text{or} \quad U_{p+1} \equiv 0 \pmod{p}$$

when $\left(\dfrac{D}{p}\right) = 1$ or $\left(\dfrac{D}{p}\right) = -1$ (Jacobi symbols), respectively, for $D = P^2 - 4Q$. Thus, the Lucas pseudoprimes, with parameters P and Q, are the odd composite integers n such that

$$U_{n-(D/n)} \equiv 0 \pmod{n}. \tag{1}$$

The Lucas pseudoprimes have been widely studied, see, e.g., [7, 9, 16, 20, 21]. Some authors also studied primilaty tests using more general linear recurrence sequences [10, 13]. Thus, the study of Lucas pseudoprimes and new primality tests appears to be still interesting.

In [8], the authors highlighted how the Lucas test can be introduced in an equivalent way by means of the Brahmagupta product and the Pell equation. We recall here some facts. The Pell equation is one of the most famous and studied Diophantine equation, it is

$$x^2 - Dy^2 = 1$$

for D non–square integer. It is well–known that given two solutions (x_1, y_1) and (x_2, y_2) of the Pell equation, then the Brahmagupta product

$$(x_1, y_1) \otimes (x_2, y_2) = (x_1x_2 + Dy_1y_2, x_1y_2 + x_2y_1)$$

yields to another solution of the Pell equation. For a complete survey, we refer the reader to [4]. Given a ring $\mathcal{R}$, we can consider the Pell conic

$$\mathcal{C} = \{(x, y) \in \mathcal{R} \times \mathcal{R} : x^2 - Dy^2 = 1\}$$

and $(\mathcal{C}, \otimes)$ is a group with identity $(1, 0)$. Moreover, when $\mathcal{R} = \mathbb{Z}_p$, the order of $\mathcal{C}$ depends on D to be or not a quadratic residue. In particular, we have $|\mathcal{C}| = p - 1$ if D is a quadratic residue in $\mathbb{Z}_p$ and $|\mathcal{C}| = p + 1$ if not, see, e.g., [14]. This property allows to construct a primality test. In [8], the authors defined the *Pell pseudoprimes*, as the odd composite integers n such that

$$y_n \equiv 0 \pmod{n}$$

with $(x_n, y_n) = (\tilde{x}, \tilde{y})^{\otimes n-(D/n)}$, where D and $(\tilde{x}, \tilde{y}) \in \mathcal{C}$ are the parameters of the test, for $\mathcal{R} = \mathbb{Z}_n$. With this definition, we have an equivalence between the Lucas and Pell test described in the following theorem.

Theorem 1. *On the one hand, if n is a Lucas pseudoprime with parameters $P > 0$ and $Q = 1$, then n is a Pell pseudoprime with parameter $\tilde{x} \equiv P/2 \pmod{n}$, $\tilde{y} \equiv 1/2 \bmod n$, and $D = P^2 - 4$. On the other hand, if n is a Pell pseudoprime with parameter $\tilde{x}$, $\tilde{y}$, and D, then n is a Lucas pseudoprime with parameters $P = 2\tilde{x}$, and $Q = 1$ [8].*

Considering the order of the Pell conic over finite fields $\mathbb{Z}_p$, we can clearly define a stronger test. Hence, we define the *strong Pell pseudoprimes* as the odd composite integers n such that

$$(\tilde{x}, \tilde{y})^{\otimes n-(D/n)} \equiv (1, 0) \pmod{n},$$

where D and $(\tilde{x}, \tilde{y}) \in \mathcal{C}$ are the parameters of the test, for $\mathcal{R} = \mathbb{Z}_n$.

Remark 1. *In [12], the author highlighted the properties of the Pell conic for constructing a primality test, but only focused on a Pell conic of the kind $x^2 - Dy^2 = 4$, as well as in [11], where the author focused on $x^2 + 3y^2 = 4$ for testing numbers of the form $3^n h \pm 1$. Moreover, we would like to point out that sometimes the term Pell pseudoprimes is used for the Lucas pseudoprimes with parameters $P = 2$ and $Q = -1$, since for these parameters the sequence U_n is known as the Pell sequence (A000129 in OEIS [19]). We have also found a different definition of Pell pseudoprimes that are the odd composite integers n such that*

$$U_n \equiv \left(\frac{2}{n}\right) \pmod{n}$$

for $P = 2$ and $Q = -1$ (A099011 in OEIS).

In this paper, firstly, in section 2, we show how many primality tests based on linear recurrent sequences of order 2 can be introduced from a matrix point of view. The Lucas test and the Pell test, as well as their connection, arise as particular cases. Moreover, in this way, we are able to introduce a generalized Pell test based on the quotient ring $\mathcal{R}[t]/(t^2-D)$, for $D \in \mathcal{R}$, which also has an analogue via Lucas sequence as we will see. Then, in section 3, we perform numerical experiments and comparison between some primality tests with a special focus on the generalized Pell test. In particular, we will show a method for the choice of the parameters, inspired to the Selfridge method, that produces very promising results. Indeed, we did not found any composite numbers that pass the generalized Pell test, with such method for the choice of parameters, up to 2^{38}.

2 Pseudoprimes with matrices

Given a matrix $M \in \mathbb{Z}^{2\times 2}$, we can consider the linear recurrence sequences $(\widetilde{U}_k)_{k\geq 0}$ and $(\widetilde{V}_k)_{k\geq 0}$ defined by

$$\begin{pmatrix}\widetilde{V}_k\\ \widetilde{U}_k\end{pmatrix} := M^k \begin{pmatrix}1\\0\end{pmatrix}.$$

The following lemma provides a primality test based on these sequences, the Lucas and strong Pell tests arise for particular choices of M. Hence, this lemma will allow to highlight many primality tests based on linear recurrence sequences of order 2 and the connection between the Lucas test and the Pell conic.

Lemma 1. *Let Δ be the discriminant of the characteristic polynomial of $M \in \mathbb{Z}^{2\times 2}$, if p is prime and $\det M \not\equiv 0 \pmod p$, then*

1. *$\widetilde{U}_{p-1} \equiv 0 \pmod p$ and $\widetilde{V}_{p-1} \equiv 1 \pmod p$, when $\sqrt{\Delta} \in \mathbb{Z}_p^*$;*
2. *$\widetilde{U}_{p+1} \equiv 0 \pmod p$ and $\widetilde{V}_{p+1} \equiv \det M \pmod p$, when $\sqrt{\Delta} \notin \mathbb{Z}_p^*$.*

Proof. Let α, β be the roots of the characteristic polynomial of M, we have that M is similar to the diagonal matrix

$$\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix}.$$

Thus, when $\sqrt{\Delta} \in \mathbb{Z}_p^*$, we also have $\alpha, \beta \in \mathbb{Z}_p^*$ and M^{p-1} is the identity matrix modulo p by the Little Fermat's Theorem, then

$$\begin{pmatrix}\tilde{V}_{p-1}\\ \tilde{U}_{p-1}\end{pmatrix} = M^{p-1}\begin{pmatrix}1\\0\end{pmatrix} \equiv \begin{pmatrix}1\\0\end{pmatrix} \pmod p.$$

When $\sqrt{\Delta} \notin \mathbb{Z}_p^*$, by the Frobenius morphism we have $\alpha^p = \beta$, $\beta^p = \alpha$ and

$$\begin{pmatrix}\tilde{V}_{p+1}\\ \tilde{U}_{p+1}\end{pmatrix} = M^p \cdot M \begin{pmatrix}1\\0\end{pmatrix} \equiv \det M \begin{pmatrix}1\\0\end{pmatrix} \pmod p$$

□

In the following we see that the Lucas and Pell tests arise as particular cases of the previous Lemma.

Lemma 2. *Given*

$$L = \begin{pmatrix}P & -Q\\ 1 & 0\end{pmatrix}, \quad C = \begin{pmatrix}\widetilde{x} & D\widetilde{y}\\ \widetilde{y} & \widetilde{x}\end{pmatrix},$$

we have

$$L^k\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}U_{k+1}\\ U_k\end{pmatrix}, \quad C^k\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}x_k\\ y_k\end{pmatrix}$$

where $(U_k)_{k\geq 0}$ is the Lucas sequence with characteristic polynomial $t^2 - Pt + Q$, $(\widetilde{x}, \widetilde{y}) \in \mathcal{C}$ (for any ring $\mathcal{R}$), and $(x_k, y_k) = (\widetilde{x}, \widetilde{y})^{\otimes k}$, for any $k \geq 0$.

Proof. Let us denote with L^k_{ij} the entry (i,j) of the matrix L^k. It is well–known that the entries of L^k are linear recurrence sequences that recur with the characteristic polynomial of L, i.e., $t^2 - Pt + Q$. Observing that $L^0_{11} = 1$, $L^1_{11} = P$ and $L^0_{21} = 0$, $L^1_{21} = 1$, we have

$$L^k \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} U_{k+1} \\ U_k \end{pmatrix}$$

for any $k \geq 0$.

Given $(\widetilde{x}, \widetilde{y}) \in \mathcal{C}$, the sequences $(x_k)_{k \geq 0}$ and $(y_k)_{k \geq 0}$ defined by $(x_k, y_k) = (\widetilde{x}, \widetilde{y})^{\otimes k}$ can be also evaluated by

$$(\widetilde{x} + \sqrt{D}\widetilde{y})^k = x_k + \sqrt{D} y_k$$

from which it is straightforward to obtain

$$\begin{cases} x_{k+1} = \widetilde{x} x_k + D\widetilde{y} y_k \\ y_{k+1} = \widetilde{y} x_k + \widetilde{x} y_k \end{cases},$$

i.e.,

$$\begin{pmatrix} \widetilde{x} & D\widetilde{y} \\ \widetilde{y} & \widetilde{x} \end{pmatrix} \begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} x_{k+1} \\ y_{k+1} \end{pmatrix}.$$

Observing that (x_0, y_0) is the identity of $(\mathcal{C}, \otimes)$, i.e., $(1, 0)$, we have

$$C^k \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_k \\ y_k \end{pmatrix}$$

for any $k \geq 0$. □

Now, we can see that the strong Pell test is connected with a stronger version of the Lucas test, which we will call *double Lucas test*. Indeed, by Lemma 1 and Lemma 2, if p is prime, then

$$U_{p-1} \equiv 0 \pmod{p}, \quad U_p \equiv 1 \pmod{p}$$

or

$$U_{p+1} \equiv 0 \pmod{p}, \quad U_{p+2} \equiv Q \pmod{p}$$

for $\sqrt{P^2 - 4Q} \in \mathbb{Z}_p^*$ or $\sqrt{P^2 - 4Q} \notin \mathbb{Z}_p^*$, respectively. We call double Lucas pseudoprimes the odd composite numbers that satisfy the above conditions.

Since $\det C = 1$ and $\det L = Q$, the matrices C and L are similar only if $Q = 1$. In this case, we can consider the matrix

$$R_1 = \begin{pmatrix} 1 & P \\ 0 & 2 \end{pmatrix},$$

and we have

$$R_1^{-1} L R_1 = \begin{pmatrix} P/2 & P^2/2 - 2 \\ 1/2 & P/2 \end{pmatrix},$$

choosing $\widetilde{x} = P/2$, $\widetilde{y} = 1/2$, $D = P^2 - 4$, we get $R_1^{-1} L R_1 = C$. In other words, if n is a double Lucas pseudoprime, for parameters P and $Q = 1$, then n is a strong Pell pseudoprime, for parameters $\widetilde{x} = P/2$, $\widetilde{y} = 1/2$, $D = P^2 - 4$. Let us note that 2 must be invertible in $\mathbb{Z}_n$.

On the other hand, given

$$R_2 = \begin{pmatrix} 1 & -\widetilde{x} \\ 0 & \widetilde{y} \end{pmatrix}$$

we have

$$R_2^{-1} C R_2 = \begin{pmatrix} 2\widetilde{x} & -\widetilde{x}^2 + D\widetilde{y}^2 \\ 1 & 0 \end{pmatrix},$$

which is L for $P = 2x_1$ and $Q = 1$. This means that if n is a strong Pell pseudoprime, for parameters $\widetilde{x}, \widetilde{y}, D$, then n is a double Lucas pseudoprime, for parameters $P = 2x_1$ and $Q = 1$. Note that in this case D is not necessarily equal to $P^2 - 4$ (the discriminant of the characteristic polynomial of the Lucas sequence), this happens only for $\widetilde{y} = \pm 1/2$. However, since $D = (\widetilde{x}^2 - 1)/\widetilde{y}^2$ and $P^2 - 4 = 4(\widetilde{x}^2 - 1)$, D is a quadratic residue in $\mathbb{Z}_n$ if and only if $P^2 - 4$ is. We summarize this in the following proposition.

Proposition 1. *If n is a double Lucas pseudoprime for the parameters P and $Q = 1$, then n is a strong Pell pseudoprime for the parameters $\widetilde{x} = P/2$, $\widetilde{y} = 1/2$, $D = P^2 - 4$.*
If n is a strong Pell pseudoprime for the parameters $\widetilde{x}$, $\widetilde{y}$ and D, then n is a double Lucas pseudoprime for the parameters $P = 2\widetilde{x}$ and $Q = 1$.

Let us note that, fixed the parameters P and $Q = 1$ for the Lucas test (for checking, e.g., the primality of all the integers in a certain range), there is not a corresponding strong Pell test with fixed parameters D, $\widetilde{x}$ and $\widetilde{y}$ as integer numbers. Indeed, given any P and $Q = 1$, we have seen that $\widetilde{x} = P/2$, $\widetilde{y} = 1/2$, $D = P^2 - 4$ are the corresponding parameters of the strong Pell test, but these values depend on the integer n we are testing (remember that in this context $1/2$ is the inverse of 2 in $\mathbb{Z}_n$).

Moreover, in general, we are not able to fix the integer parameters $D, \widetilde{x}, \widetilde{y}$ in the strong Pell test for checking the primality of all the integers in a given range, because it is necessary that $\widetilde{x}^2 - D\widetilde{y}^2 \equiv 1 \pmod{n}$ and this can not be true for any integer n. For overcoming these issues, the use of a parametrization of the conic $\mathcal{C}$ can be helpful. In [5], the authors provided the following map

$$\Phi : \begin{cases} \mathcal{R} \cup \{\alpha\} \to \mathcal{C} \\ a \mapsto \left(\dfrac{a^2 + D}{a^2 - D}, \dfrac{2a}{a^2 - D} \right), \quad a \neq \alpha \\ \alpha \mapsto (1, 0) \end{cases}$$

where $\alpha \notin \mathcal{R}$ is the point at the infinity of such a parametrization of $\mathcal{C}$. When $\mathcal{R}$ is a field and $t^2 - D$ is irreducible in $\mathcal{R}$, the map is always defined, otherwise there are values of a such that $\Phi(a)$ can not be evaluated. In this way, we can consider the strong Pell test with fixed parameters D and a, in the sense that $\widetilde{x} = (a^2 + D)/(a^2 - D)$ and $\widetilde{y} = 2a/(a^2 - D)$.

Example 1. *Given $P = 4$ and $Q = 1$, the Lucas pseudoprimes up to 5000 are*

$$65, 209, 629, 679, 901, 989, 1241, 1769, 1961, 1991, 2509, 2701, 2911, 3007, 3439, 3869,$$

whereas the double Lucas pseudoprimes are

$$209, 901, 989, 2701, 2911, 3007, 3439.$$

When P is even, we are always able to find an equivalent strong Pell test, providing all the same pseudoprimes of the double Lucas test. Indeed, it is sufficient to choice D and a such that $(a^2 + D)/(a^2 - D)$ is the integer number $P/2$. For instance in this case, taking $D = 3$ and $a = 3$, we have $\widetilde{x} = 2$ and $\widetilde{y} = 1$.

Remark 2. *A double Lucas test with parameters P and $Q = 1$ is equivalent to the strong Pell test with parameters $D = P^2 - 4$ and $a = P + 2$. Indeed, in this case, exploiting the parametrization Φ, we get $\widetilde{x} = P/2$ and $\widetilde{y} = 1/2$. Note that using this method, the strong Pell test equivalent to the double Lucas test considered in Example 1 has parameters $D = 12$ and $a = 6$. This means that there are strong Pell tests with different parameters which are equivalent to each others.*

We conclude observing that the double Lucas test for any value of P and Q can be described in terms of the Barahmagupta product. The Pell equation can be introduced over a general ring $\mathcal{R}$ considering the quotient ring $\mathcal{A} = \mathcal{R}[t]/(t^2 - D)$, for $D \in \mathcal{R}$. The product of two elements $x_1 + y_1 t, x_2 + y_2 t \in \mathcal{A}$, i.e., $(x_1, y_1), (x_2, y_2) \in \mathcal{A}$, coincide with the Brahmagupta product and the elements of norm 1 define $\mathcal{C}$. If we take $(x_1, y_1) \in \mathcal{A}$ with norm Q, considering $(x_n, y_n) := (x_1, y_1)^{\otimes n}$, we still have

$$C^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

and we can still use the matrices R_1 and R_2 for passing from L to C and viceversa, without any restriction on the choice of Q. Hence the double Lucas test is connected with the Brahmagupta product also for $Q \neq 1$. Hence, we define the *generalized Pell pseudoprimes*, for the parameters $D, \tilde{x}, \tilde{y}$, as the odd composite integers n such that

$$\begin{cases} (\tilde{x}, \tilde{y})^{\otimes n+1} \equiv (Q, 0) \pmod{n}, & \text{if } \dfrac{D}{n} = \text{-1} \\ (\tilde{x}, \tilde{y})^{\otimes n-1} \equiv (1, 0) \pmod{n}, & \text{if } \dfrac{D}{n} = 1 \end{cases} . \qquad (2)$$

P	Q	L Pseudo	DL Pseudo	P	Q	L Pseudo	DL Pseudo
1	-3	72	2	3	-3	45	2
1	-2	64	64	3	-2	94	0
1	-1	50	16	3	-1	59	23
1	2	53	0	3	1	91	50
1	3	50	1	3	2	78	78
1	4	86	3	3	4	113	3
2	-4	50	3	4	-3	80	3
2	-3	75	75	4	-2	79	2
2	-2	54	3	4	-1	119	49
2	-1	81	39	4	1	100	54
2	3	73	1	4	2	81	6
2	5	127	7	4	3	75	75

Table 1: Number of Lucas pseudoprimes (L Pseudo) and double Lucas pseudoprimes (DL Pseudo) for different values of the parameters P and Q up to 10^5.

3 Numerical experiments

In this section, we show the behaviour of some primality tests in terms of number of pseudoprimes that pass them. In particular, we first focus on the classical Lucas test and we show how the use of the double Lucas test decreases a lot of the number of composite integers that are stated primes. Then, we see how the use of matrices introduced in the previous section allow the definition of many new primality tests and we study them for some different values of the parameters. Similarly, we also study the strong Pell test. In these experiments, we will see that the performances of the above tests are very sensitive with respect to the values of the parameters. For this reason in subsection 3.2 we study these tests setting the parameters by using methods à la Selfridge. In facts, the Selfridge method was introduced for finding good values of the parameters of the Lucas and strong Lucas tests, see [3] and observe that in OEIS the sequences of Lucas pseudoprimes (A217120) and strong Lucas pseduoprimes (A217255) are defined by using the parameters P and Q with the Selfridge method.

3.1 Tests with fixed parameters

The Lucas test depends on two parameters P and Q that determine the Lucas sequence $(U_k)_{k\geq 0}$ used in equation (1) for testing the primality of an integer number. Similarly, the double Lucas test depends on the same two parameters P and Q, since the double Lucas pseudoprimes are the odd composite integers n satisfying

$$\begin{cases} U_{n-1} \equiv 0 \pmod{n} \quad \text{and} \quad U_n \equiv 1 \pmod{n}, \quad \text{if } \left(\dfrac{D}{n}\right) = 1 \\ U_{n+1} \equiv 0 \pmod{n} \quad \text{and} \quad U_{n+2} \equiv Q \pmod{n}, \quad \text{if } \left(\dfrac{D}{n}\right) = \text{-1} \end{cases}.$$

In Figure 1, we compare the number of Lucas pseudoprimes and the number of double Lucas pseudoprimes up to 10^5 for different values of P and Q, avoiding trivial choices ot the parameters like, e.g., $P = 1$, $Q = 1$ or $P = 2$, $Q = -1$. We only consider positive values for P because the Lucas and double Lucas tests are not sensitive with respect to the sign of the parameter P. The data used in Figure 1 are also summarized in Table 1. For instance, we can observe that for $P = 1$ and $Q = -3$ there are only 2 double Lucas pseudoprimes up to 10^5, against the 72 Lucas pseudoprimes. However, we also have to observe that in some cases, the double Lucas test does not provide great improvements in this sense, for example for $P = 3$ and $Q = 1$ we found 50 double Lucas pseudoprimes and 91 Lucas pseudoprimes; for $P = 3$ and $Q = 2$ we found the same number of pseudoprimes. Moreover, we can see that there are sensible differences in the performances depending on the values of the parameters P and Q. In fact, for example, for $P = 1$ and $Q = 2$ there are not double Lucas pseudoprimes up to 10^5 (the first double Lucas pseudoprime is 100127 in this case), whereas we have 78 double Lucas pseudoprimes for $P = 3$ and $Q = 2$.

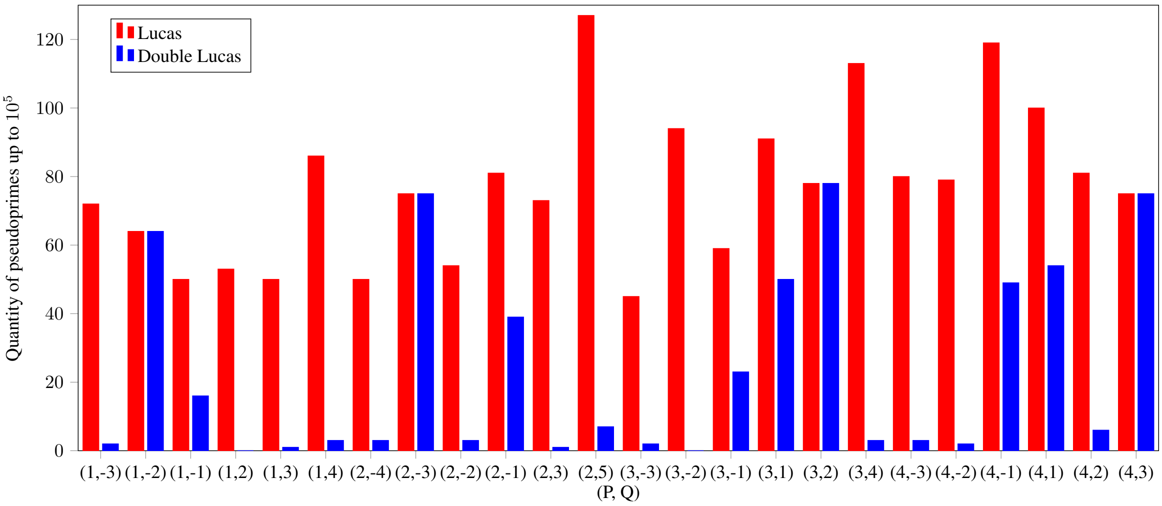

Figure 1: Comparison between the number of Lucas and double Lucas pseudoprimes (on the y–axis) up to 10^5 for different values of (P, Q) (on the x–axis)

Thanks to Lemma 1, we are able to define primality tests based on linear recurrent sequences of degree two, different from the Lucas sequences. Specifically, if we take the matrix

$$\begin{pmatrix} P & -Q \\ R & 0 \end{pmatrix}$$

and consider the sequences $(\tilde{U}_k)_{k\geq 0}$ and $(\tilde{V}_k)_{k\geq 0}$ defined by $M^k \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \tilde{V}_k \\ \tilde{U}_k \end{pmatrix}$, we deal with linear recurrent sequences with characteristic polynomial $t^2 - Pt + QR$ and initial conditions $\tilde{U}_0 = 0, \tilde{U}_1 = R$ and $\tilde{V}_0 = 1, \tilde{V}_1 = P$. Note that $(\tilde{V}_k)_{k\geq 0}$ is the same sequence used in the double Lucas test, whereas $(\tilde{U}_k)_{k\geq 0}$ is different due to the initial conditions. In this case the pseudoprimes, which we will call generalized Lucas pseudoprimes, are the odd composite integers satisfying

$$\begin{cases} \tilde{U}_{n-1} \equiv 0 \pmod{n} \quad \text{and} \quad \tilde{U}_n \equiv 1 \pmod{n}, \quad \text{if } \left(\dfrac{D}{n}\right) = 1 \\ \tilde{U}_{n+1} \equiv 0 \pmod{n} \quad \text{and} \quad \tilde{U}_{n+2} \equiv QR \pmod{n}, \quad \text{if } \left(\dfrac{D}{n}\right) = \text{-1} \end{cases} . \tag{3}$$

The corresponding primality test depends on the parameters P, Q, R. In Figure 2, we report the number of generalized Lucas pseudoprimes up to 10^5 for different values of the parameters randomly sampled. We can observe that the results strongly depend on the values of the parameters. For instance for $P = 5$, $Q = 5$, $R = -3$ we have no pseudoprimes up to 10^5 (the first pseudoprime is 218791 in this case), on the contrary for $P = 4$, $Q = 1$, $R = 3$ we found 79 pseudoprimes.

Finally, we discuss the strong and generalized Pell pseudoprimes. As we have shown in the previous section, they are connected to the double Lucas pseudoprimes. The strong Pell test with parameters D and a is equivalent to the double Lucas test with parameters $P = 2(a^2+D)/(a^2-D)$ and $Q = 1$. The generalized Pell test depends on the parameters D, $\tilde{x}$, $\tilde{y}$ and there is not an equivalent double Lucas test with fixed parameters P and Q. Thus, we only focus on some numerical experiments regarding this test. In Figure 3, we show the number of generalized Pell pseudoprimes up to 10^5 for $-3 \leq D \leq 3$ and $\tilde{x}$, $\tilde{y}$ randomly chosen between -9 and 9. Also in this case, the performances are heavily affected by the choice of the parameters

3.2 Tests with Selfridge method

In the previous section, we have seen that the performances of the studied primality tests are heavily affected by the choice of the parameters. The Selfridge method is a standard way for choosing the parameters of the Lucas test. Given the integer n to test, the parameters of the Lucas test are chosen by the Selfridge method in the following way

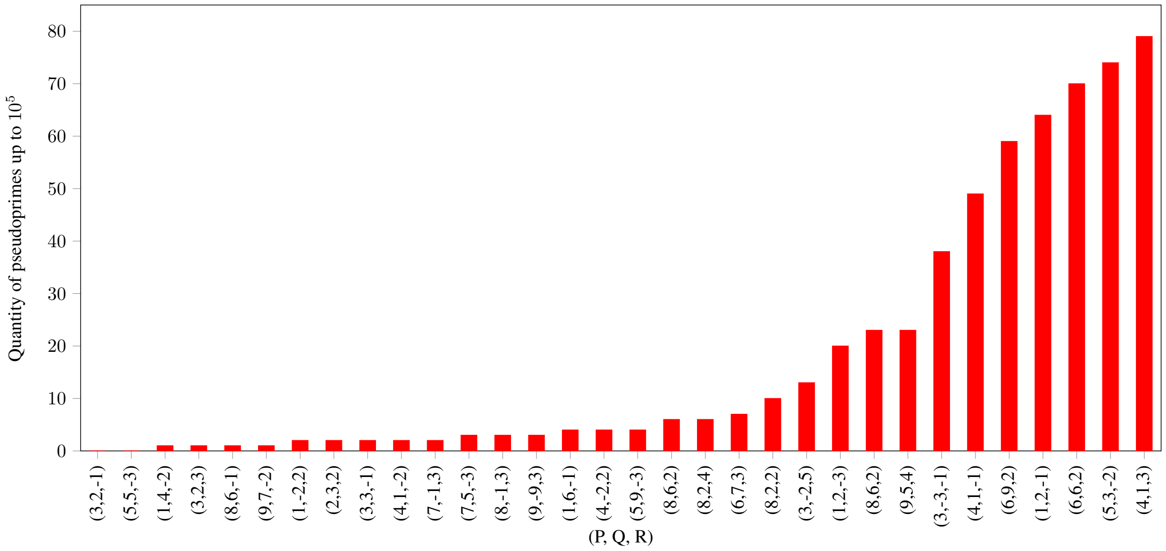

Figure 2: Number of generalized Lucas pseudoprimes up to 10^5 defined by (3) for different values of (P, Q, R).

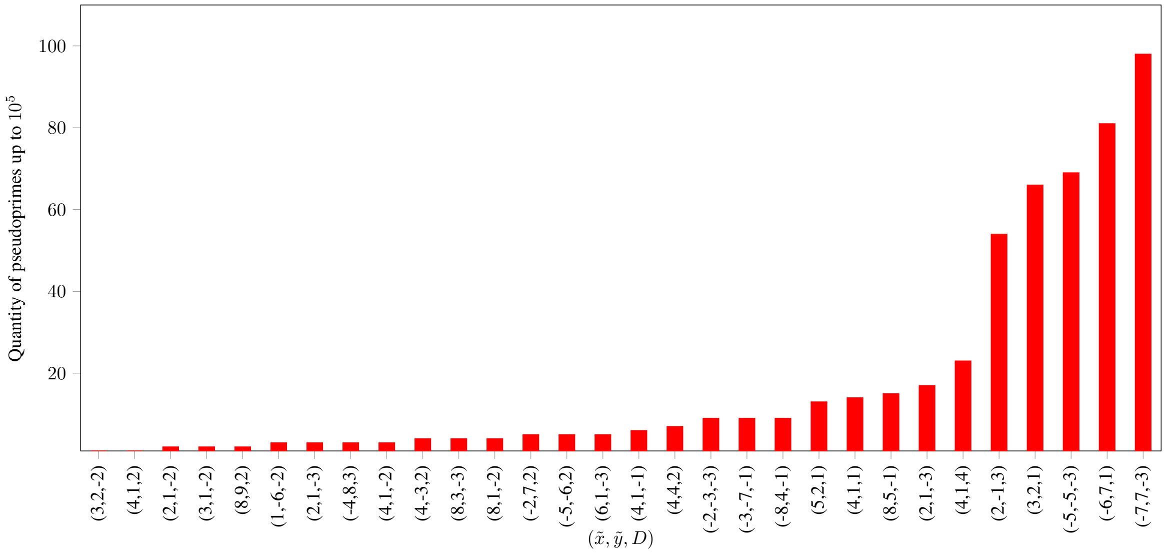

Figure 3: Number of generalized Pell pseudoprimes up to 10^5 for different values of $(\tilde{x}, \tilde{y}, D)$.

- Set $P = 1$.
- Set D as the first integer in the sequence $5, -7, 9, -11, \dots$ such that $\left(\frac{D}{n}\right) = -1$.
- Set $Q = \frac{1-D}{4}$.

The sequence of Lucas pseudoprimes, using the Selfridge method, is

$$323, 377, 1159, 1829, 3827, 5459, 5777, 9071, 9179, 10877, 11419, 11663, 13919, 14839, \dots$$

see A217120 in OEIS. If we apply the Selfridge method for the choice of the parameters to the double Lucas test, we find the following sequence of pseudoprimes

$$5777, 10877, 75077, 100127, 113573, 161027, 162133, 231703, \dots$$

which are the Frobenius pseudoprimes (A212423). Since the Selfridge method is a very standard and useful techniques for choosing the parameters in these primality tests, here we adapt the method to the new primality tests introduced previously. We will observe that the use of the Selfridge method with the generalized Lucas test (defined by (3)) and with the generalized Pell test (defined by (2)) gives very interesting and powerful results. In the following we describe the adaptation of the Selfridge method to these tests.

Given the integer n to test, for the generalized Lucas test, choose the parameters in the following way:

- Set $P = 1$ and $R = 2$.
- Set D as the first integer in the sequence $-7, 9, -15, 17, -23, 25, -31, 33 \dots$ such that $\left(\frac{D}{n}\right) = -1$.
- Set $Q = \frac{1-D}{8}$.

Using this method for the choice of the parameters, we did not find any pseudoprime up to 2^{38}. Note that if we set $R = \pm 1$, we find the Frobenius pseudoprimes, thus we used $R = 2$, which is the smallest value that produces a new primality test. This choice has been done for the sake of simplicity, as well as in the Selfridge method the parameters are taken in the simplest way that allows to have the Jacobi symbol equals to -1. Consequently, we modified the sequence where searching D in order to obtain an integer value for Q.

Given the integer n to test, for the generalized Pell test, choose the parameters in the following way:

- Set $\tilde{x} = 3$ and $\tilde{y} = 2$.
- Set D as the first integer in the sequence $5, -7, 9, -11, \dots$ such that $\left(\frac{D}{n}\right) = -1$.

Also with this method, we did not find any pseudoprime up to 2^{38}.

Moreover, we combined these two tests with the Fermat one. In particular, we found that the Fermat pseudoprimes to base 2 up to 2^{64} are declared composite by both previous tests.

Finally, we would like to highlight that the computation costs of these two tests are very similar to the cost of Lucas tests. Indeed, to the best of our knowledge, the most efficient way for evaluating the terms of the Lucas sequence is to perform powers of matrices with the square and multiply algorithm. In the case of our tests, we still have to perform powers of 2×2 matrices for checking conditions (2) and (3).

4 Conclusion

Considering the experimental results discussed in the previous section, we suggest the use of two new primality tests that we summarize here.

Generalized Lucas test with a Selfridge method. Given an odd positive integer n, do

- Set $P = 1$ and $R = 2$.
- Set D as the first integer in the sequence $-7, 9, -15, 17, -23, 25, -31, 33\dots$ such that $\left(\dfrac{D}{n}\right) = -1$.
- Set $Q = \dfrac{1-D}{8}$.
- Evaluate $\begin{pmatrix}\tilde{V}_{n+1}\\ \tilde{U}_{n+1}\end{pmatrix} := \begin{pmatrix}P & -Q\\ R & 0\end{pmatrix}^{n+1}\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}\tilde{V}_{n+2}\\ \tilde{U}_{n+2}\end{pmatrix} := \begin{pmatrix}P & -Q\\ R & 0\end{pmatrix}^{n+2}\begin{pmatrix}1\\0\end{pmatrix}$
- If $\tilde{U}_{n+1} \equiv 0 \pmod n$ and $\tilde{U}_{n+2} \equiv QR \pmod n$, then n is declared prime, otherwise n is composite.

Generalized Pell test with a Selfridge method. Given an odd positive integer n, do

- Set $\tilde{x} = 3$ and $\tilde{y} = 2$.
- Set D as the first integer in the sequence $5, -7, 9, -11, \dots$ such that $\left(\dfrac{D}{n}\right) = -1$.
- Evaluate $\begin{pmatrix}x_{n+1}\\ y_{n+1}\end{pmatrix} := \begin{pmatrix}\tilde{x} & D\tilde{y}\\ \tilde{y} & \tilde{x}\end{pmatrix}^{n+1}\begin{pmatrix}1\\0\end{pmatrix}$
- If $x_{n+1} \equiv \tilde{x}^2 - D\tilde{y}^2 \pmod n$ and $\tilde{y} \equiv 0 \pmod n$, then n is declared prime, otherwise n is composite.

These primality tests appear to be very promising in terms of finding good primality tests. Indeed, usually, in the Lucas test and similar ones, there are small pseudoprimes (the first Lucas pseudoprime is 323 and the first Frobenius pseudoprime is 5777), whereas for these two tests the first pseudoprime must be greater than 2^{38}. Moreover, both the above tests combined with the Fermat test to base 2 work without errors (i.e., no composite number is declared prime) up to 2^{64}.

In future works, it should be interesting to find the first pseudoprimes for these two tests, as well as investigating different choices for R and for $\tilde{x}$ and $\tilde{y}$. Furthermore, it could be very interesting to find some theoretical results about the distribution of these pseudoprimes.

Finally, the implementation of all the tests presented in this paper and used for the experiments described in Section 3 is available at https://github.com/duttos/primality_tests

Acknowledgment

A. J. Di Scala and N. Murru are members of GNSAGA of INdAM.
D. Bazzanella, A. J. Di Scala, S. Dutto are members of DISMA Dipartimento di Eccellenza MIUR 2018-2022.
All the authors are members of the groups ‘Cryptography and codes’ of UMI.
We would like to thank Dr. Tiziana Armano and Dr. Federico Tesser for the great help and support in the use of the workstations of the Department of Mathematics (University of Turin) and DISMA (Politecnico of Turin), respectively.
We would like to thank the anonymous referee for the valuable suggestions that helped to improve the paper.

References

[1] M. Agrawal, N. Kayal, N. Saxena, *Primes is in P*, Ann. Math. **160** (2004), 781–793.

[2] W. R. Alford, A. Granville, C. Pomerance, *There are Infinitely Many Carmichael Numbers*, Ann. Math. **139** (1994), 703–722.

[3] R. Baillie, S. S. Wagstaff, *Lucas pseudoprimes*, Math. Comp. **35** (1980), no. 152, 1391–1417.

[4] E. J. Barbeau, *Pell's equation*, New York-Berlin: Springer-Verlag, (2003).

[5] E. Bellini, N. Murru, *An efficient and secure RSA-like cryptosystem exploiting Rédei rational functions over conics*, Finite Fields Appl. **39** (2016), 179–194.

[6] Z. Chen, J. Greene, *Some comments on Baillie-PSW pseudoprimes*, Fibonacci Quart. **41** (2003), no. 4, 334–344.

[7] A. Di Porto, P. Filipponi, *A probabilistic primality test based on the properties of certain generalized Lucas numbers*, Advances in Cryptology — EUROCRYPT '88, Lecture Notes in Computer Science **330** (1988), 211–223.

[8] A. Di Scala, N. Murru, C. Sanna, *Lucas pseudoprimes and the Pell conic*, Preprint, Available at https://arxiv.org/abs/2001.00353, (2020).

[9] D. M. Gordon, C. Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), no. 196, 825–838.

[10] J. Grantham, *There are infinitely many Perrin peudoprimes*, J. Number Theory **130** (2010), 1117–1128.

[11] S. A. Hambleton, *Generalized Lucas-Lehmer tests using Pell conics*, Proc. Amer. Math. Soc. **140** (2012), no. 8, 2653–2661.

[12] F. Lemmermeyer, *Conics - a poor's man elliptic curves*, Preprint (2003), Available at https://arxiv.org/abs/math/0311306.

[13] F. Luca, I. E. Shparlinski, *Pseudoprimes in certain linear recurrences*, Albanian J. Math. **1** (2007), no. 3, 125–131.

[14] A. J. Menezes, S. A. Vanstone, *A note on cyclic groups, finite fields, and the discrete logarithm problem*, Appl. Algebra Engrg. Comm. Comput. **3** (1992), 67–74.

[15] C. Pomerance, *Are there counter-examples to the Baillie-PSW primality test?*, Preprint (1984), Available at http://www.pseudoprime.com/dopo.pdf.

[16] C. Pomerance, *Primality testing: variations on a theme of Lucas*, Congressus Numerantium **201** (2010), 301–312.

[17] C. Pomerance, J. L. Selfridge, S. S., Wagstaff, *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), no. 151, 1003–1026.

[18] M. O. Rabin, Probabilistic algorithm for testing primality, Journal of Number Theory **12** (1980), 128–138.

[19] N. J. A. Sloane, editor, The On-Line Encyclopedia of Integer Sequences, published electronically at https://oeis.org.

[20] L. Somer, *Lucas pseudoprimes of special types*, Fibonacci Quart. **47** (2009), no. 3, 198–206.

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

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