Irreducibility Criteria for Reciprocal Polynomials and Applications

Antonio Cafure and Eda Cesaratto

Abstract. We present criteria for determining irreducibility of reciprocal polynomials over the field of rational numbers. We also obtain some combinatorial results concerning the irreducibility of reciprocal polynomials. As a consequence of our approach, we are able to deal with other problems such as factorization properties of Chebyshev polynomials of the first and second kind and with the classical problems of computing minimal polynomials of algebraic values of trigonometric functions.

1. INTRODUCTION. The study of irreducibility of polynomials in $\mathbb{Q}[t]$ is a well established research area requiring different concepts and tools from many fields. In the opinion of these authors it is a very nice and instructive subject.

There are many criteria for studying irreducibility based on distinct characteristics of the polynomials—for instance, criteria based on the prime factors dividing the coefficients as in Eisenstein's criterion and, more generally, as in Newton's polygon. There are also criteria based on the size of the coefficients, whose proofs require tools of complex analysis, such as Perron's criterion and related results. In fact, there is an extensive literature about this subject. The notes written by Michael Filaseta [**5**] provide a very readable and interesting source of information about these facts.

In the classical book *Irrational Numbers* by Ivan Niven [**10**], we find another criterion for irreducibility over $\mathbb{Q}$, although it is not explicitly stated as such. It arises in a context where Niven proves (a result due to Derrick Lehmer) that the numbers $\cos(2\pi/n)$ and $\sin(2\pi/n)$ are algebraic over $\mathbb{Q}$. In fact, he first computes the minimal polynomials over $\mathbb{Q}$ of the numbers $2\cos(2\pi/n)$ by appealing to the fact that cyclotomic polynomials are reciprocal polynomials. By means of the change of variables $x = t + 1/t$, he shows that the cyclotomic polynomial Φ_n (which is irreducible over $\mathbb{Q}[t]$ and has $\cos(2\pi/n) + i\sin(2\pi/n)$ as a root) is transformed into an irreducible polynomial in $\mathbb{Q}[x]$ (whose degree is half the degree of Φ_n) having $2\cos(2\pi/n)$ as a root. To finish, Niven shows that the numbers $\sin(2\pi/n)$ are algebraic over $\mathbb{Q}$ by expressing $\sin(2\pi/n)$ in terms of $\cos(2\pi/m)$ for a certain integer m.

This paper intends to take advantage of Niven's approach to study problems related to factorization of reciprocal polynomials. We now define precisely all the needed notation. Our definition of reciprocal polynomial involves the more general notion of reversal polynomial.

Definition. Given a polynomial $f \in \mathbb{Q}[t]$, the *reversal polynomial* of f is defined as the following polynomial of $\mathbb{Q}[t]$:

$$f_{\mathsf{rev}}(t) = t^{\deg f} f(1/t). \tag{1}$$

Informally said, the reversal polynomial f_{rev} has the same coefficients as f but in reverse order. The interesting feature of (1) is that it is independent of the way f is expressed. As an easy example, if $f = t^2 - t + 2$ then its reversal polynomial is

http://dx.doi.org/10.4169/amer.math.monthly.124.1.37
MSC: Primary 12E05

$$f_{\mathsf{rev}} = t^2\Big(1/t^2 - 1/t + 2\Big) = 1 - t + 2t^2.$$

When f is a polynomial having 0 as a root, the degree of f_{rev} and f do not coincide. For instance, for any monomial $f = t^n$, its reversal polynomial is $f_{\mathsf{rev}} = 1$. In Section 2 many properties of f_{rev} are precisely stated.

Reversal polynomials are well known and arise in many instances. An interesting application of this notion to the division algorithm in $\mathbb{Q}[t]$ can be found in [**14**].

As stated before, reciprocal polynomials are the main object of this paper. They can be seen as "fixed points" of the reversal operation defined in (1).

Definition. A polynomial $f \in \mathbb{Q}[t]$ is a *reciprocal polynomial* if

$$f_{\mathsf{rev}}(t) = f(t). \tag{2}$$

One can find other names for referring to this type of polynomial: self-reciprocal, palindromic, etc. Our choice is a consequence of being introduced to this notion thanks to Edward Barbeau's wonderful book *Polynomials* [**1**]. An example of a reciprocal polynomial is $f = t^6 - 2t^5 + 5t^4 - t^3 + 5t^2 - 2t + 1$. We might say that cyclotomic polynomials Φ_n for $n > 1$ are the best known examples of reciprocal polynomials with rational coefficients.

The change of variables $x = t + 1/t$ is the key to the usual method for computing (or at least, simplifying the search for) the roots of a reciprocal polynomial. Given any reciprocal polynomial $f \in \mathbb{Q}[t]$ of degree $2n$, by making this change of variables, we obtain a polynomial in $\mathbb{Q}[x]$ of degree n. The roots of this polynomial are of the form $\alpha + 1/\alpha$ with α a root of f. Assuming that the n roots of the polynomial in x are able to be computed, we then recover the roots of f by solving n quadratic equations.

We will consider this change of variables as inducing a mapping which we call *reciprocal mapping* and which we define below.

Definition. The *reciprocal mapping* R assigns to each reciprocal polynomial $f \in \mathbb{Q}[t]$ of even degree the unique polynomial $p = \mathsf{R}(f) \in \mathbb{Q}[x]$ satisfying the equation

$$f(t) = t^{\deg p}\, p(t + 1/t).$$

Conversely, we observe that for every $p \in \mathbb{Q}[x]$ the polynomial $f = \mathsf{R}^{-1}(p)$, just defined, is reciprocal of even degree.

Example 1. Consider the reciprocal polynomial $\Phi_{11} = \sum_{i=0}^{10} t^i$, the eleventh cyclotomic polynomial. Writing

$$\Phi_{11} = t^5\left(1 + \sum_{k=1}^{5}\left(t^k + \frac{1}{t^k}\right)\right)$$

it is possible to express each term $t^k + 1/t^k$ as a linear combination of powers of $x = t + 1/t$ as follows:

$$\begin{aligned} t^2 + 1/t^2 &= (t + 1/t)^2 - 2, \\ t^3 + 1/t^3 &= (t + 1/t)^3 - 3(t + 1/t), \end{aligned}$$

$$t^4 + 1/t^4 = (t + 1/t)^4 - 4(t + 1/t)^2 + 2,$$
$$t^5 + 1/t^5 = (t + 1/t)^5 - 5(t + 1/t)^3 + 5(t + 1/t).$$

With these equalities, it turns out that

$$\Phi_{11} = t^5 p(t + 1/t) \quad \text{with} \quad p = \mathsf{R}(\Phi_{11}) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

Taking this known idea as a starting point, the main goal of our article is to provide an unified framework in which many different problems arising in the context of reciprocal polynomials may be considered.

Our reciprocal mapping has many interesting features which enable us to turn the usual change of variables into a systematic treatment. We will refer to the underlying method as the *reciprocal substitution method* and its details are explained in Section 3. The fact is that this method gives not only some information about the roots of a reciprocal polynomial, but it also provides information about its factorization. Thus, factorizations properties of reciprocal polynomials of even degree are translated into factorization properties of their images and vice versa.

By means of the reciprocal substitution method we are able to provide some criteria for determining the irreducibility of reciprocal polynomials in $\mathbb{Q}[t]$ (see Theorem 11).

Theorem. Let $f \in \mathbb{Z}[t]$ be a primitive reciprocal polynomial of even degree and assume that the image polynomial $p \in \mathbb{Q}[x]$ is irreducible.

1. If $|f(1)|$ or $|f(-1)|$ are not perfect squares, then f is irreducible in $\mathbb{Q}[t]$.
2. If $f(1)$ and the middle coefficient of f have different signs, then f is irreducible in $\mathbb{Q}[t]$.
3. If the middle coefficient of f is 0 or ± 1, then f is irreducible in $\mathbb{Q}[t]$.

We remark that many of the well-known criteria for determining irreducibility of integer polynomials cannot be used to determine irreducibility of reciprocal polynomials.

Our criterion permits us to show that the polynomials

$$g_{2p}(t) = \frac{(t+1)^{2p} - t^{2p} - 1}{t}$$

are irreducible over $\mathbb{Q}$ when p is an odd prime number (see Example 14). We learned about this family from Filaseta's notes [**5**]. The difference in our analysis from that of [**5**] is that we do not make use of the Newton polygon of g_{2p} with respect to p. We simply appeal to Eisenstein's criterion to show the irreducibility of the image of g_{2p}.

From a combinatorial point of view, it is interesting to estimate the "proportion" of reciprocal polynomials with a given factorization pattern. It is known that "almost all" polynomials with integer coefficients are irreducible over $\mathbb{Q}$ (see, e.g., [**5**]). By means of the reciprocal substitution method, combinatorial versions for reciprocal polynomials are deduced from their counterparts in $\mathbb{Q}[x]$. In fact, the following theorem holds (see Section 6).

Theorem. Almost all reciprocal polynomials with integer coefficients are irreducible over $\mathbb{Q}$.

To prove this result we take advantage of the properties of the reciprocal mapping. Mainly, this involves a matrix representation of R which enables us to obtain bounds on the coefficients of $\mathsf{R}(f)$ for any reciprocal f of degree $2n$.

Our approach also leads us to address problems related to the complete factorization over $\mathbb{Q}$ of the Chebyshev polynomials of first and second kind. Finally, we deal with the computation of the minimal polynomials of the numbers $\cos(2\pi/n)$ and $\sin(2\pi/n)$ and derived facts. There are many references dealing with this kind of problem beginning with the works of Lehmer, Niven, and others (see [**2**] and [**15**]).

2. FACTORIZATION PROPERTIES OF RECIPROCAL POLYNOMIALS.

We begin this section with a number of consequences which are derived from the definition of reversal polynomial given in (1).

- If α is a nonzero complex root of f, then $1/\alpha$ is a root of f_{rev}.
- Let k be the multiplicity of 0 as a root of f. Then the degree of f_{rev} is equal to $\deg f - k$. If $f(0) \neq 0$, then $(f_{\mathsf{rev}})_{\mathsf{rev}} = f$.
- $(fg)_{\mathsf{rev}} = f_{\mathsf{rev}}\, g_{\mathsf{rev}}$.
- If $f(0) \neq 0$, then f is irreducible in $\mathbb{Q}[t]$ if and only if f_{rev} is irreducible in $\mathbb{Q}[t]$.

Assume now that $f \in \mathbb{Q}[t]$ is a reciprocal polynomial of odd degree. From the properties of reversal polynomials, it is immediate that -1 is a root of f and that f factors as $(t+1)g$ with $g \in \mathbb{Q}[t]$ a reciprocal polynomial of even degree. Thus it makes sense to restrict our attention to the set of reciprocal polynomials with rational coefficients and even degree. Throughout the text we will use the following notation:

$$\mathcal{R} := \{f \in \mathbb{Q}[t] : \ f \text{ reciprocal and of even degree}\}.$$

Leaving aside $\Phi_1 = t - 1$ and $\Phi_2 = t + 1$, we see that any cyclotomic polynomial Φ_n belongs to $\mathcal{R}$ for $n \geq 3$.

The following proposition provides an equivalent definition of reciprocal polynomial.

Proposition 2. A polynomial $f \in \mathbb{Q}[t]$ is reciprocal if and only if it satisfies the following two properties.

1. If 1 is a root of f, then its multiplicity is even.
2. If α is a root of f of multiplicity r, then $1/\alpha$ is a root of multiplicity r.

In the sequel we will use indistinctly both characterizations.

We list now some useful properties concerning the factorization of reciprocal polynomials.

Lemma 3. The following assertions hold:

- The product of reciprocal polynomials is reciprocal.
- If $f = gh$ and f and g are reciprocal, then h is also reciprocal.

In spite of its simplicity our following lemma is crucial.

Lemma 4. Let $f \in \mathbb{Q}[t]$ be such that $f(0) \neq 0$. Then $ff_{\mathsf{rev}} \in \mathcal{R}$.

Proof. This is a consequence of the properties of $-_{\mathsf{rev}}$ listed at the beginning of this section. Since $f(0) \neq 0$, then ff_{rev} has degree equal to $2\deg f$ and $(ff_{\mathsf{rev}})_{\mathsf{rev}} = ff_{\mathsf{rev}}$. ■

Our next proposition will characterize the factorization pattern of a reciprocal polynomial in $\mathbb{Q}[t]$. We first observe that if f is any reciprocal polynomial in $\mathbb{Q}[t]$, Proposition 2 says that if 1 were a root of f, then it would have even multiplicity, say r. This would imply that $(t-1)^r$ is reciprocal and hence that f factors as $f = (t-1)^r g(t)$ with $g \in \mathbb{Q}[t]$ reciprocal. This reasoning permits us to leave aside the case in which $f(1) = 0$.

Proposition 5. Let $f \in \mathbb{Q}[t]$ be an arbitrary reciprocal polynomial with $f(1) \neq 0$ and let g be an irreducible factor in $\mathbb{Q}[t]$ of f. If g is nonreciprocal, then $f = g\, g_{\mathsf{rev}}\, h$ with $h \in \mathbb{Q}[t]$ reciprocal.

Proof. Let $g \in \mathbb{Q}[t]$ be an irreducible nonreciprocal factor of f. In particular, g is neither the polynomial $t-1$ nor the polynomial $t+1$. We have that g_{rev} is also irreducible in $\mathbb{Q}[t]$. For every root α of g we know that $1/\alpha$ is a root of g_{rev}. Since f is reciprocal, $1/\alpha$ is also a root of f. Hence it turns out that g_{rev} is also an irreducible factor of f (coprime with g) and thus gg_{rev} is a factor of f. Lemma 4 implies that gg_{rev} belongs to $\mathcal{R}$ and hence by Lemma 3 we obtain that f factors as $gg_{\mathsf{rev}}h$ with $h \in \mathbb{Q}[t]$ reciprocal. ■

The factor gg_{rev} in Proposition 5 is related to what is usually known as the nonreciprocal part of f. See for instance the paper [**6**].

We now introduce the notion of irreducibility in the set $\mathcal{R}$ which will be important in our setting.

Definition. We say that $f \in \mathcal{R}$ is *irreducible in* $\mathcal{R}$ if it does not factor as a product of two nonconstant polynomials in $\mathcal{R}$.

Under this definition, we see that $t^2 - 2t + 1$ is irreducible in $\mathcal{R}$ but not in $\mathbb{Q}[t]$. Hence irreducibility over $\mathcal{R}$ does not imply irreducibility over $\mathbb{Q}[t]$. On the contrary, it is clear that any polynomial $f \in \mathcal{R}$ that is irreducible in $\mathbb{Q}[t]$ is also irreducible in $\mathcal{R}$. For our combinatorial results it is useful to introduce the following notations:

$$\mathsf{Irred}(\mathcal{R}) = \{f \in \mathcal{R} : f \text{ is irreducible over } \mathcal{R}\},$$

$$\mathsf{Red}(\mathcal{R}) = \{f \in \mathcal{R} : f \text{ is reducible over } \mathcal{R}\}.$$

As a consequence of Proposition 5, we are able to characterize completely the factorization over $\mathbb{Q}$ of an irreducible element $f \in \mathcal{R}$.

Corollary 6. Let $f \in \mathsf{Irred}(\mathcal{R})$. Either f is irreducible in $\mathbb{Q}[t]$ or $f = agg_{\mathsf{rev}}$ with $g \in \mathbb{Q}[t]$ irreducible and $a \in \mathbb{Q}^*$.

Corollary 6 implies that $\mathsf{Irred}(\mathcal{R})$ splits as $\mathcal{R}_1 \cup \mathcal{R}_2$ where

$$\begin{aligned}\mathcal{R}_1 =& \{f \in \mathsf{Irred}(\mathcal{R}) : f \text{ is irreducible over } \mathbb{Q}\},\\ \mathcal{R}_2 =& \{f \in \mathsf{Irred}(\mathcal{R}) : f = agg_{\mathsf{rev}},\ a \in \mathbb{Q}^*, g \text{ irreducible over } \mathbb{Q}\}.\end{aligned}$$

We observe that if $f \in \mathsf{Irred}(\mathcal{R})$ and $f(1) = 0$, then $f = a(t-1)(-t+1)$ and thus f belongs to $\mathcal{R}_2$.

Remark. In case $f \in \mathcal{R}_2$ has integer coefficients, as a consequence of Gauss's lemma, we may assume that $f = agg_{\mathsf{rev}}$ with $a \in \mathbb{Z}$ and $g \in \mathbb{Z}[t]$. In particular, if f is primitive, then $f = \pm gg_{\mathsf{rev}}$ with g a primitive polynomial. This is important for studying irreducibility over $\mathbb{Q}$ as we may always assume that f is primitive.

3. THE RECIPROCAL SUBSTITUTION METHOD.

We now briefly recall the well-known method for computing the roots of a reciprocal polynomial. Given $f \in \mathcal{R}$ of degree $2n$, by means of the change of variables $x = t + 1/t$, we obtain a polynomial in $\mathbb{Q}[x]$ of degree n, whose roots are of the form $\alpha + 1/\alpha$, with α a root of f. Assuming that the n roots of the polynomial in x are able to be computed, we then recover the roots of f by solving n quadratic equations. This is the typical method for computing the roots of reciprocal polynomials.

In this section we explain the details of what we call the reciprocal substitution method. This sort of idea is already known in a finite field context (see [**9**]).

Let $f \in \mathcal{R}$ be a polynomial of degree $2n$. In dense form, f may be expressed as follows:

$$f(t) = a_0 t^n + \sum_{k=1}^{n} a_k (t^{n+k} + t^{n-k})$$

with $a_0, \ldots, a_n$ in $\mathbb{Q}$. By induction on k, it can be shown that $t^k + 1/t^k$ can be expressed in terms of x by a unique monic polynomial $f_k \in \mathbb{Z}[x]$ of degree k. These polynomials can be recursively computed by means of the following recurrence:

$$f_n(x) = x f_{n-1}(x) - f_{n-2}(x), \quad f_0(x) = 2,\ f_1(x) = x. \tag{3}$$

The first terms of recurrence (3) are the polynomials:

$$f_2(x) = x^2 - 2, \quad f_3(x) = x^3 - 3x, \quad f_4(x) = x^4 - 4x^2 + 2, \quad f_5(x) = x^5 - 5x^3 + 5x.$$

Therefore, since any $f \in \mathcal{R}$ is uniquely written as

$$f(t) = a_0 t^n + t^n \sum_{k=1}^{n} a_k f_k \left(t + \frac{1}{t} \right),$$

we deduce that

$$p = a_0 + \sum_{k=1}^{n} a_k f_k \in \mathbb{Q}[x]$$

is the only polynomial satisfying the functional equation

$$f(t) = t^{\deg f/2} p(x(t)) \quad \text{with} \quad x(t) = t + \frac{1}{t}. \tag{4}$$

This provides an effective way of computing the polynomial $p \in \mathbb{Q}[x]$ for every $f \in \mathcal{R}$. Thus we have a mapping R from $\mathcal{R}$ onto $\mathbb{Q}[x]$ defined as follows:

$$\begin{array}{rcccc} \mathsf{R} & : & \mathcal{R} & \to & \mathbb{Q}[x] \\ & & f & \mapsto & a_0 + a_1 f_1 + \cdots + a_n f_n. \end{array}$$

In particular, observe that for every $k \in \mathbb{N}$ we have that

$$\mathsf{R}(t^{2k} + 1) = f_k.$$

In [**1**], Barbeau introduces the terminology *reciprocal equation substitution* when referring to (4). Inspired by this terminology, we will say that the sequence $(f_n)_{n\in\mathbb{N}}$ is the *reciprocal substitution sequence* and that R is the *reciprocal mapping*.

The following properties of the reciprocal mapping R are immediately deduced from (4).

Proposition 7. R satisfies the following properties.

1. R is a bijective mapping.
2. $\mathsf{R}(fg) = \mathsf{R}(f)\mathsf{R}(g)$ for any $f, g \in \mathcal{R}$.

We finally show that there exists a matrix context in which we may understand the reciprocal mapping R. Although R is not a linear mapping since $\mathcal{R}$ is not a $\mathbb{Q}$-vector space, when restricted to the elements of $\mathcal{R}$ of degree $2n$ we are able to give a matrix representation for R. This is a nice characterization which will enable us to obtain information about the number of irreducible reciprocal polynomials.

We fix a natural number n. Every $f \in \mathcal{R}$ having degree $2n$ can be coded as a coefficient vector of $n + 1$ coordinates which we denote by $[f]$:

$$[f] = (a_n, a_{n-1}, \dots, a_0) \in \mathbb{Q}^{n+1}, \quad a_n \neq 0.$$

Consider the $(n + 1) \times (n + 1)$-matrix R_n whose entry a_{ij} is the coefficient of x^{n-i+1} in the polynomial f_{n-j+1}, except for the entry $a_{n+1,n+1}$ which is equal to 1 (instead of 2). Under this consideration we reach the conclusion that

$$[\mathsf{R}(f)]^t = \mathsf{R}_n[f]^t, \tag{5}$$

where $[\mathsf{R}(f)]$ is the coefficient vector of $\mathsf{R}(f)$ with respect to the monomial basis $\{x^n, \dots, x^2, x, 1\}$.

The matrix R_n is a lower triangular integer matrix. It is also a unimodular matrix and thus its inverse R_n^{-1} is also an integer matrix.

For instance if $n = 5$, the matrix R_5 turns out to be

$$\mathsf{R}_5 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ -5 & 0 & 1 & 0 & 0 & 0 \\ 0 & -4 & 0 & 1 & 0 & 0 \\ 5 & 0 & -3 & 0 & 1 & 0 \\ 0 & 2 & 0 & -2 & 0 & 1 \end{pmatrix}.$$

Recalling Example 1 from the Introduction, the coefficient vector of the cyclotomic polynomial Φ_{11} is $[\Phi_{11}] = (1, 1, 1, 1, 1, 1)$ and hence the coefficient vector of $\mathsf{R}(\Phi_{11})$ is obtained by computing the product

$$[\mathsf{R}(f)]^t = \mathsf{R}_5(1, 1, 1, 1, 1, 1)^t = (1, 1, -4, -3, 3, 1)^t,$$

which yields $\mathsf{R}(f) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$.

4. IRREDUCIBILITY CRITERIA OVER $\mathbb{Q}$. We begin this section by giving a refinement of the irreducibility criterion presented in Niven's book. As a matter of fact, our criterion is a criterion for irreducibility in $\mathcal{R}$ and thus we complete the characterization given in Corollary 6.

Proposition 8. Let $f \in \mathcal{R}$. Then f is irreducible in $\mathcal{R}$ if and only if $\mathsf{R}(f)$ is irreducible in $\mathbb{Q}[x]$.

Proof. Let $f = f_1 f_2$ be a factorization in $\mathcal{R}$ such that $2 \leq \deg f_i < \deg f$ for $i = 1, 2$. Then $\mathsf{R}(f) = \mathsf{R}(f_1)\mathsf{R}(f_2)$ is a factorization in $\mathbb{Q}[x]$ such that $1 \leq \deg \mathsf{R}(f_i) < \deg f/2$.

Reciprocally, if $\mathsf{R}(f)$ factors in $\mathbb{Q}[x]$, the properties of R imply that f factors in $\mathcal{R}$. ■

The statement of Proposition 8 establishes the relationship between irreducibility in $\mathcal{R}$ and in $\mathbb{Q}[x]$. We can reformulate this statement in terms of the reciprocal mapping. Denoting by $\mathsf{Irred}(\mathbb{Q})$ and by $\mathsf{Red}(\mathbb{Q})$ the set of irreducible and reducible elements of $\mathbb{Q}[x]$, respectively, we have that

$$\mathsf{R}(\mathsf{Irred}(\mathcal{R})) = \mathsf{Irred}(\mathbb{Q}) \quad \text{and} \quad \mathsf{R}(\mathsf{Red}(\mathcal{R})) = \mathsf{Red}(\mathbb{Q}). \tag{6}$$

Example 9. Let $f \in \mathbb{Z}[t]$ be a monic reciprocal polynomial of degree 4 such that $\mathsf{R}(f)$ has no rational roots. Following Proposition 8 and Corollary 6 we deduce its irreducibility over $\mathbb{Q}$ except when $f = t^4 - (b^2 + 2)t^2 + 1$, with $b \in \mathbb{Z}$. In this case we have the factorization $f = -gg_{\mathsf{rev}}$, where $g = t^2 + bt - 1$.

The next example shows that, in general, we cannot determine the irreducibility of f in $\mathbb{Q}[t]$ from that of $\mathsf{R}(f)$ in $\mathbb{Q}[x]$.

Example 10. If $f = t^6 - 3t^5 - 3t^4 + 11t^3 - 3t^2 - 3t + 1$, then $\mathsf{R}(f) = x^3 - 3x^2 - 6x + 17$. The irreducibility of $\mathsf{R}(f)$ over $\mathbb{Q}$ is readily seen and hence f is irreducible over $\mathcal{R}$. However, f is not irreducible over $\mathbb{Q}$ since it factors as $(t^3 - 3t + 1)(t^3 - 3t^2 + 1)$. As stated by Corollary 6, we see that $f = gg_{\mathsf{rev}}$ with $g = t^3 - 3t + 1$ an irreducible element of $\mathbb{Q}[t]$.

At this point we are ready to state our irreducibility criteria for reciprocal polynomials.

Theorem 11. *Let $f \in \mathcal{R}$ be a primitive polynomial and assume that $\mathsf{R}(f)$ is irreducible in $\mathbb{Q}[x]$.*

1. *If $|f(1)|$ or $|f(-1)|$ are not perfect squares, then f is irreducible in $\mathbb{Q}[t]$.*
2. *If $f(1)$ and the middle coefficient of f have different signs, then f is irreducible in $\mathbb{Q}[t]$.*
3. *If the middle coefficient of f is 0 or ± 1, then f is irreducible in $\mathbb{Q}[t]$.*

Proof. Since $\mathsf{R}(f)$ is irreducible, we have that f is irreducible in $\mathcal{R}$ by Proposition 8. Corollary 6 implies that either f is irreducible in $\mathbb{Q}$ or, considering that f is primitive, that it factors as $f = \pm gg_{\mathsf{rev}}$ with $g \in \mathbb{Z}[t]$ an irreducible polynomial over $\mathbb{Q}$. Assume that f is not irreducible over $\mathbb{Q}$. We will show that this assumption leads to a contradiction.

Since $g(1) = g_{\mathsf{rev}}(1)$, then $|f(1)| = |g(1)|^2$, contradicting the fact that $|f(1)|$ is not a perfect square. Similarly, from $g(-1) = \pm g_{\mathsf{rev}}(-1)$ we would have that $|f(-1)| = |g(-1)|^2$. This shows that 1. is satisfied.

In the case of 2., if $f(1) > 0$ it turns out that $f = g g_{\mathsf{rev}}$. Writing $g = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ we observe that the middle coefficient of f is equal to $a_0^2 + a_1^2 + \cdots + a_{n-1}^2 + a_n^2$. This is not possible as long as this coefficient takes negative values. A similar argument may be used if $f(1) < 0$.

Assertion 3 is a direct consequence of the expression for the middle coefficient given in the proof of 2. ■

In what follows we give many examples which exhibit the interest of our method.

Example 12. Consider the polynomial $f = t^8 + 6t^7 + 2t^6 + 22t^5 - 8t^4 + 22t^3 + 2t^2 + 6t + 1$. We have that $\mathsf{R}(f) = x^4 + 6x^3 - 2x^2 + 4x - 10$. By Eisenstein's criterion, $\mathsf{R}(f)$ is irreducible over $\mathbb{Q}[x]$. According to Theorem 11 we conclude that f is irreducible over $\mathbb{Q}$.

Example 13. Let $f \in \mathcal{R}$ with coefficients 0 and 1. If $\mathsf{R}(f)$ is irreducible in $\mathbb{Q}[x]$, then we immediately conclude that f is irreducible in $\mathbb{Q}[t]$.

Example 14. We consider the following sequence of polynomials in $\mathbb{Q}[t]$ for $n \geq 2$:

$$g_n(t) = \frac{(t+1)^n - t^n - 1}{t}.$$

First we make some general remarks about the polynomials g_n. Each g_n has degree $n - 2$. After expressing g_n in dense form

$$g_n(t) = \binom{n}{1} t^{n-2} + \binom{n}{2} t^{n-3} + \cdots + \binom{n}{n-2} t + \binom{n}{n-1},$$

and appealing to binomial identities, it is immediate that g_n is a reciprocal polynomial. When n is even, the polynomial g_n belongs to $\mathcal{R}$. Setting $m := (n-2)/2$, we have that

$$\mathsf{R}(g_n) = \binom{n}{1} f_m + \binom{n}{2} f_{m-1} + \cdots + \binom{n}{n/2 - 1} f_1 + \binom{n}{n/2},$$

where $f_1, \ldots, f_m$ are the first m polynomials of the reciprocal substitution sequence.

Let $n = 2p$ with p an odd prime number. Hence we have

$$\mathsf{R}(g_{2p}) = \binom{2p}{1} f_{p-1} + \binom{2p}{2} f_{p-2} + \cdots + \binom{2p}{p-1} f_1 + \binom{2p}{p}.$$

Using the fact that

$$\binom{2p}{j} \equiv 0 \pmod{p}, \; j = 1, \ldots, p-1, \qquad \binom{2p}{\text{mod } p} \not\equiv 0 \pmod{p},$$

by Eisenstein's criterion we see that $\mathsf{R}(g_{2p})_{\mathsf{rev}}$ is irreducible over $\mathbb{Q}$ and hence $\mathsf{R}(g_{2p})$ is irreducible over $\mathbb{Q}$. Since $g_{2p}(1) = 2^{2p} - 2$ is not a perfect square, our criterion shows that g_{2p} is irreducible over $\mathbb{Q}$.

Example 15. Proposition 8 together with Proposition 5 bring the following interesting fact. Let $f \in \mathbb{Q}[t]$ be any irreducible polynomial distinct from t. Then f_{rev} is also irreducible and thus the polynomial $f f_{\mathsf{rev}} \in \mathcal{R}$ (whose degree is twice the degree of f) is irreducible in $\mathcal{R}$. Then the polynomial $\mathsf{R}(f f_{\mathsf{rev}})$ is an irreducible polynomial in $\mathbb{Q}$ of degree equal to the degree of f. Continuing this process, we obtain a sequence of irreducible polynomials in $\mathbb{Q}[t]$ of degree equal to the degree of f and with coefficients arbitrarily large. This process gives a sort of *irreducible polynomial generator*.

5. NUMERICAL BEHAVIOR OF THE RECIPROCAL MAPPING. For our combinatorial results we need some insight on how the size of the coefficients of $\mathsf{R}(f)$ grows with respect to that of f. Similarly, we address the problem of relating the size of the coefficients of a given polynomial g and the product $g g_{\mathsf{rev}}$. In this way we will obtain some interesting results concerning the reciprocal substitution sequence $(f_n)_{n\in\mathbb{N}}$.

Two expressions for the size of f will play a role in our approach. Given $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Q}[x]$, the 1-norm $||f||_1$ and the max-norm $||f||_\infty$ of f are, respectively, the numbers

$$\begin{aligned} ||f||_1 &= \textstyle\sum_{i=0}^{n} |a_i|, \\ ||f||_\infty &= \max\{|a_i| : i = 0, 1, \ldots, n\}. \end{aligned}$$

For the reciprocal substitution sequence, we consider the associated integer sequence $(||f_n||_1)_{n\in\mathbb{N}}$ of 1-norms. The first terms of this sequence are

$$||f_0||_1 = 2,\ ||f_1||_1 = 1,\ ||f_2||_1 = 3,\ ||f_3||_1 = 4,\ ||f_4||_1 = 7,\ ||f_5||_1 = 11.$$

This shows a coincidence with the sequence of Lucas numbers. We recall that the sequence of Lucas numbers L_n is defined as follows:

$$L_n = L_{n-1} + L_{n-2} \quad \text{and} \quad L_0 = 2,\ L_1 = 1.$$

The recurrence (3) defining the reciprocal substitution sequence gives rise to the following recurrence for $||f_n||_1$:

$$||f_n||_1 = ||f_{n-1}||_1 + ||f_{n-2}||_1, \quad ||f_0||_1 = 2,\ ||f_1||_1 = 1, \tag{7}$$

therefore proving the equality between the sequences.

Proposition 16. The integer sequence $(||f_n||_1)_{n\in\mathbb{N}}$ is the sequence of Lucas numbers.

With the previous result at hand we next analyze the behavior of $||f||_\infty$ under the mapping R. To obtain an upper bound on $||\mathsf{R}(f)||_\infty$ for any $f \in \mathcal{R}$ of degree $2n$ and having max-norm $||f||_\infty \leq B$, it will be convenient to appeal to the matrix representation R_n of R defined in (5).

According to the usual setting for matrix norms, the max-norm of R_n as an operator is the number

$$||\mathsf{R}_n||_\infty = \max_{1\leq i\leq n+1} \sum_{j=1}^{n+1} |a_{ij}|.$$

Our matrix representation allows us to compute $\mathsf{R}(f)$ by computing the product $\mathsf{R}_n[f]^t$ and thus we have that

$$||\mathsf{R}(f)||_\infty \leq ||\mathsf{R}_n||_\infty ||f||_\infty.$$

We now obtain an upper bound on the max-norm of R_n taking into account Proposition 16. The following inequality holds for $n \in \mathbb{N}$:

$$||\mathsf{R}_n||_\infty = \max_{1\leq i\leq n+1} \sum_{j=1}^{n+1} |a_{ij}| \leq \sum_{j=1}^{n+1}\sum_{i=1}^{n+1} |a_{ij}| = 1 + \sum_{j=1}^{n} ||f_j||_1 = 1 + \sum_{j=1}^{n} L_j.$$

As a consequence of a classical identity involving Lucas numbers which asserts that $\sum_{j=0}^{n} L_j = L_{n+2} - 1$, we can conclude that

$$||\mathsf{R}(f)||_\infty \leq ||\mathsf{R}_n||_\infty ||f||_\infty \leq L_{n+2}B.$$

In this way we have shown the following result.

Proposition 17. Let $f \in \mathcal{R}$ have degree $2n$ and $||f||_\infty = B$. Then

$$||\mathsf{R}(f)||_\infty \leq L_{n+2}B.$$

We still have to state one result concerning the max-norm of the polynomial g given by Corollary 6. Our next proposition provides information in that direction. It can be seen as an effective version of this corollary.

Proposition 18. Let $f \in \mathcal{R}_2$ with integer coefficients have degree $2n$ and max-norm $||f||_\infty \leq B$. Then the irreducible polynomial $g \in \mathbb{Z}[t]$ of degree n such that $f = agg_{\mathsf{rev}}$ with $a \in \mathbb{Z}$ has max-norm $||g||_\infty$ at most $\sqrt{B}$.

Proof. Let $g = a_n t^n + \cdots + a_1 t + a_0$ (with $a_n \neq 0$) and suppose that $||g||_\infty = |a_i|$ for some $0 \leq i \leq n$. The middle coefficient of f is equal to $a(a_0^2 + a_1^2 + \cdots + a_n^2)$ and this implies that

$$||g||_\infty^2 = |a_i|^2 \leq \sum_{i=0}^{n} |a_i|^2 \leq ||f||_\infty \leq B.$$

■

6. THE NUMBER OF IRREDUCIBLE AND REDUCIBLE RECIPROCAL POLYNOMIALS.

In this section we obtain some upper bounds for the numbers of elements in $\mathsf{Red}(\mathcal{R})$ and $\mathsf{Irred}(\mathcal{R})$ in a sense to be clarified. The interesting feature of this treatment is that reciprocal polynomials may have nonreciprocal factors. However, we will show that the number of such polynomials is small.

We must remark that there is a well-established tradition of searching for results in this vein. Again, Filaseta's notes are a good reference for this item.

Let n be a fixed natural number. Every polynomial of degree n with integer coefficients may be represented as a point $(a_n, a_{n-1}, \ldots, a_1, a_0)$ of the $(n+1)$-dimensional lattice $\mathbb{Z}^{n+1}$. For a positive B we consider those lattice points lying in the $(n+1)$-cube $[-B, B]^{n+1}$:

$$S_n(B) := \Big\{ f \in \mathbb{Z}[t] : \deg f = n, \|f\|_\infty \le B \Big\}.$$

Thus $S_n(B)$ is the set of polynomials of degree n with integer coefficients in the interval $[-B, B]$. It is immediate that the number $|S_n(B)|$ is equal to $2B(2B+1)^n$ for an integer B.

There is a sort of classical result concerning the number of reducible polynomials in $S_n(B)$. In fact, it turns out that the following bound holds:

$$|\mathsf{Red}(\mathbb{Q}) \cap S_n(B)| \ll_n B^n \log^2 B, \tag{8}$$

where the notation $\ll_n$ means that there is a constant depending only on n involved in the upper bound. This bound apparently first appears in the classical book of George Pólya and Gabor Szegö [**11**] as Exercise 266 from Part VIII. We first learned about this result from Filaseta's notes [**5**, Theorem 5.1.1]. Subsequent improvements of (8) were successively obtained in the papers [**3**], [**8**], and [**4**]. For our needs it is enough to consider the upper bound stated in (8).

The upper bound given by (8) also provides an upper bound for the proportion:

$$\frac{\big|\mathsf{Red}(\mathbb{Q}) \cap S_n(B)\big|}{\big|S_n(B)\big|} \ll_n \frac{B^n \log^2 B}{2B(2B+1)^n} \quad (B \in \mathbb{N}). \tag{9}$$

This proportion tends to 0 as B tends to infinity. In Pólya–Szegö's words, "the probability that a polynomial with integral coefficients of given degree is reducible is equal to 0." This also usually leads to saying that *almost all polynomials in* $\mathbb{Z}$ *are irreducible over* $\mathbb{Q}$.

Our goal is to make use of this result in order to obtain some estimates about the number of reducible and irreducible reciprocal polynomials.

We consider the set $\mathsf{Red}(\mathcal{R}) \cap S_{2n}(B)$, that is to say, the set of reducible reciprocal integer polynomials of degree $2n$ and max-norm at most B. Our first result is an upper bound for the number $|\mathsf{Red}(\mathcal{R}) \cap S_{2n}(B)|$.

Theorem 19. *Let B a positive integer. Then*

$$|\mathsf{Red}(\mathcal{R}) \cap S_{2n}(B)| \ll_n B^n \log^2 B.$$

Proof. From (6) and from Proposition 17 we have that

$$\mathsf{R}\Big(\mathsf{Red}(\mathcal{R}) \cap S_{2n}(B)\Big) \subset \mathsf{Red}(\mathbb{Q}) \cap S_n(B'),$$

where $B' = L_{n+2}B$ and thus

$$|\mathsf{Red}(\mathcal{R}) \cap S_{2n}(B)| \le |\mathsf{Red}(\mathbb{Q}) \cap S_n(B')|.$$

Applying (8) to the right-hand side of the previous inequality, we deduce that

$$|\mathsf{Red}(\mathcal{R}) \cap S_{2n}(B)| \ll_n (L_{n+2}B)^n (\log(L_{n+2}B))^2.$$

This implies the statement of this proposition up to a multiplicative constant. ∎

Recalling that any $f \in \mathcal{R}$ of degree $2n$ is given by a coefficient vector $[f] = (a_n, a_{n-1}, \dots, a_1, a_0) \in \mathbb{Q}^{n+1}$, with $a_n \neq 0$, we have that

$$|\mathcal{R} \cap S_{2n}(B)| = 2B\big(2B+1\big)^n \quad \text{for } B \in \mathbb{N},$$

and then from Theorem 19 we obtain the proportion

$$\frac{|\mathsf{Red}(\mathcal{R}) \cap S_{2n}(B)|}{|\mathcal{R} \cap S_{2n}(B)|} \ll_n \frac{B^n(\log B)^2}{2B\big(2B+1\big)^n}, \tag{10}$$

which tends to 0 for B tending to infinity. Inspired by the usual terminology, we say that *almost all polynomials in $\mathcal{R}$ with integer coefficients are irreducible in $\mathcal{R}$.*

Remark. We may argue that the hidden constant bound provided by Theorem 19 is a rough one. Our approach consists of imbedding the $(n+1)$-dimensional cube $[-B, B]^{n+1}$ in the $(n+1)$-dimensional cube $[-L_{n+2}B, L_{n+2}B]$ and that encloses counting more reducible polynomials than necessary. However, in terms of proportions, what really matters is that it tends to 0 as B tends to infinity.

As a consequence of Corollary 6 we know that $\mathsf{Irred}(\mathcal{R}) = \mathcal{R}_1 \cup \mathcal{R}_2$. Our goal is to show that most of the irreducible polynomials in $\mathcal{R}$ are already irreducible in $\mathbb{Q}[t]$. In other words, we will show that $\mathcal{R}_2$ has very few elements.

Let f be a polynomial in $\mathcal{R}_2 \cap S_{2n}(B)$. First of all, we see that, appealing to our irreducibility criterion (Theorem 11), we can discard the case $B = 1$. In this case $\mathcal{R}_2 \cap S_{2n}(B)$ turns out to be empty. Thus we can assume that B is an integer greater than or equal to 2.

Theorem 20. *Let B be an integer greater than or equal to 2. Then*

$$\big|\mathcal{R}_2 \cap S_{2n}(B)\big| \leq 4B\sqrt{B}(2\sqrt{B}+1)^n.$$

Proof. By Proposition 18 we know that for $f \in \mathcal{R}_2 \cap S_{2n}(B)$ there exists an irreducible polynomial $g \in \mathbb{Z}[t]$ with max-norm $||g||_\infty \leq \sqrt{B}$ such that $f = agg_{\mathsf{rev}}$ for some nonzero integer $a \in [-B, B]$. By Lemma 4 we have that

$$\big|\mathcal{R}_2 \cap S_{2n}(B)\big| \leq 2B\big|\{gg_{\mathsf{rev}} : g \in \mathsf{Irred}(\mathbb{Q})\} \cap S_n(\sqrt{B})\big|.$$

Since the following bound holds:

$$\big|\{gg_{\mathsf{rev}} : g \in \mathsf{Irred}(\mathbb{Q})\} \cap S_n(\sqrt{B})\big| \leq 2\sqrt{B}(2\sqrt{B}+1)^n$$

the statement of our theorem easily follows. ∎

As an immediate consequence of Theorem 20, we deduce the following proportion:

$$\frac{\big|\mathcal{R}_2 \cap S_{2n}(B)\big|}{\big|\mathcal{R} \cap S_{2n}(B)\big|} \leq 2\sqrt{B}\left(\frac{2\sqrt{B}+1}{2B+1}\right)^n \leq \frac{2\sqrt{B}}{(\sqrt{B}-1/2)^n}. \tag{11}$$

This shows that the number of irreducible polynomials in $\mathcal{R}$ belonging to $\mathcal{R}_2$ is almost irrelevant with respect to the number of reciprocal polynomials for $n \geq 2$. (Recall that $\mathcal{R}_2$ is empty for $B = 1$.) Gathering proportions (10) and (11), we come to the conclusion that most of the polynomials in $\mathcal{R} \cap S_{2n}(B)$ are irreducible over $\mathbb{Q}$ when B tends to infinity.

Theorem 21. *Almost all polynomials $f \in \mathcal{R}$ with integer coefficients are irreducible over $\mathbb{Q}$.*

In summary, when we consider a polynomial in $\mathcal{R}$ we must expect that it is an irreducible polynomial over $\mathbb{Q}$. Thus it is important to have at our disposal criteria for determining its irreducibility.

7. APPLICATIONS.

In this section we apply the reciprocal substitution method and our irreducibility criteria to study classical examples.

Factorization patterns of Chebyshev polynomials. As a consequence of our approach, we can easily deal with many facts concerning factorization properties over $\mathbb{Q}$ of Chebyshev polynomials T_n and U_n of the first and second kind, respectively.

The reciprocal substitution sequence is related to the sequences T_n and U_n. As a matter of fact, they are related by the following identity:

$$T_n(x) = \frac{1}{2} f_n(2x), \quad \text{and} \quad U_{n-1}(x) = \frac{1}{n} f_n'(2x) \quad n \in \mathbb{N}.$$

In this way, any property concerning the factorization of T_n and U_n over the rationals may be deduced from that of f_n and f_n'.

As we have already pointed out, the definition of the reciprocal mapping R implies that $f_n = \mathsf{R}(t^{2n} + 1)$. Moreover, by induction on n it follows that

$$f_n' = \begin{cases} n\,(f_1 + f_3 + \cdots + f_{n-1}) & n \text{ even} \\ n\,(1 + f_2 + \cdots + f_{n-1}) & n \text{ odd} \end{cases}$$

and hence we deduce that

$$f_n' = n\,\mathsf{R}\left(t^{2(n-1)} + t^{2(n-2)} + \cdots + t^2 + 1\right).$$

The factorization of the polynomials $t^{2n} + 1$ and $t^{2(n-1)} + t^{2(n-2)} + \cdots + t^2 + 1$ in $\mathbb{Q}[t]$ is well known. They factor as a product of cyclotomic polynomials of even degree:

$$t^{2n} + 1 = \prod_{\substack{d \mid 4n \\ d \nmid 2n}} \Phi_d \qquad t^{2(n-1)} + t^{2(n-2)} + \cdots + t^2 + 1 = \prod_{\substack{d \mid 2n \\ d \neq 1,2}} \Phi_d.$$

In particular, they factor as a product of irreducible elements in $\mathcal{R}$. Thus, it is immediate that

$$f_n = \prod_{\substack{d \mid 4n \\ d \nmid 2n}} R(\Phi_d) \quad \text{and} \quad \frac{1}{n} f_n' = \prod_{\substack{d \mid 2n \\ d \neq 1,2}} \mathsf{R}(\Phi_d) \tag{12}$$

are the irreducible factorizations of f_n and f_n' over $\mathbb{Q}$, respectively. From this fact many well-known properties of the factorization of f_n and f_n' can be derived.

Example 22. Since $t^m + 1$ is irreducible over $\mathbb{Q}$ if and only if m is a power of 2, it follows that f_n is irreducible over $\mathbb{Q}$ if and only if $n = 2^k$ for $k \in \mathbb{N}$. Therefore, this provides another proof that the Chebyshev polynomial T_n is irreducible over $\mathbb{Q}$ if and only if $n = 2^k$.

In the same vein, we conclude that the Chebyshev polynomial of the second kind U_{n-1} is never irreducible over $\mathbb{Q}$ for $n \geq 3$, since f_n' is never irreducible over $\mathbb{Q}$ for $n \geq 3$.

In summary, taking into account (12) our method solves completely problems like the following.

- Factoring completely over $\mathbb{Q}$ the Chebyshev polynomials of first and second kind.
- Proving divisibility relations between different T_n and U_m.
- Computing greatest common divisors such as (T_n, T_m), (U_n, U_m), and (T_n, U_m).

Some of these results, were previously considered in [**7**], [**12**], and [**13**], although by using other approaches. Our interest is to stress that our approach simplifies the search for a solution to these problems. Instead of dealing with T_n and U_{n-1}, it is easier to deal with f_n and f_n' as images by R of products of cyclotomic polynomials.

The minimal polynomials of cos$(2\pi/n)$ and sin$(2\pi/n)$. In this section C_n and S_n will denote the minimal polynomials over $\mathbb{Q}$ of $2\cos(2\pi/n)$ and $2\sin(2\pi/n)$, respectively.

Let $\xi := \cos(2\pi/n) + i\sin(2\pi/n)$ be a primitive nth root of unity and let Φ_n be its minimal polynomial over $\mathbb{Q}$, i.e., the cyclotomic polynomial of order n. By Proposition 8, it turns out that

$$C_n = \mathsf{R}(\Phi_n) \in \mathbb{Q}[x] \tag{13}$$

is the minimal polynomial over $\mathbb{Q}$ of $2\cos(2\pi/n)$ when $n \geq 3$. From this it follows easily that the minimal polynomial (up to a nonzero rational) of $\cos(2\pi/n)$ is equal to $C_n(2x)$. This is the proof one can find in Niven's book [**10**, p. 38]. In the same proof it is shown that the numbers $\sin(2\pi/n)$ are algebraic over $\mathbb{Q}$ by using trigonometric identities and then the degrees of their minimal polynomials are computed.

In our context, to compute S_n we use the same idea for computing C_n. We simply have to find an irreducible reciprocal polynomial having $\sin(2\pi/n) + i\cos(2\pi/n)$ as a root. Hence, S_n will be the image under R of this sought polynomial.

We consider the complex number

$$i\bar{\xi} = \sin(2\pi/n) + i\cos(2\pi/n).$$

Since $i\bar{\xi}$ is a primitive root of unity for a suitable m, its minimal polynomial over $\mathbb{Q}$ will be a certain cyclotomic polynomial. We denote by Ψ_n the minimal polynomial over $\mathbb{Q}$ of $i\bar{\xi}$. To compute Ψ_n it is necessary to determine the order of $i\bar{\xi}$ as a primitive root.

Proposition 23. Let n be a natural number. The minimal polynomial Ψ_n of $i\bar{\xi}$ is computed as follows.

1. If n is odd, then $\Psi_n = \Phi_{4n}$.
2. If $n = 2m$ with odd m, then $\Psi_n = \Phi_{2n}$.
3. If $n = 4m$ with odd $m \neq 1$, then $\Psi_n = \Phi_{\frac{n}{2}}$ and for $n = 4$, $\Psi_4 = \Phi_1$.
4. If $n = 8m$ with odd m, then $\Psi_n = \Phi_n$.

As a consequence of Proposition 23 we can assure that $S_n = \mathsf{R}(\Psi_n)$ is the minimal polynomial over $\mathbb{Q}$ of $2\sin(2\pi/n)$.

Proposition 24. Let n be a natural number. Then the minimal polynomial S_n of $2\sin(2\pi/n)$ is computed as follows.

1. If n is odd, then $S_n = \mathsf{R}(\Phi_{4n})$.
2. If $n = 2m$ with odd m, then $S_n = \mathsf{R}(\Phi_{2n})$.
3. If $n = 4m$ with odd $m \neq 1$, then $S_n = \mathsf{R}(\Phi_{\frac{n}{2}})$ and for $n = 4$, $S_4 = \mathsf{R}(\Phi_1)$.
4. If $n = 8m$ with odd m, then $S_n = \mathsf{R}(\Phi_n)$.

This approach exploits the ideas of Niven [**10**] providing a complementary treatment to the many existing references. For instance, compare with [**2**], where S_n is computed for primes values of n.

8. CONCLUSIONS AND OPEN PROBLEMS. In this article we have intended to show how the reciprocal substitution method might constitute a systematic way of studying problems involving factorization of reciprocal polynomials over the rationals. In this sense we have obtained two irreducibility criteria, combinatorial results on the number of reducible and irreducible reciprocal polynomials, and have also shown how to deal with some classical families of polynomials.

Observe that our approach could be used to design algorithms for factoring reciprocal polynomials. To the best of our knowledge, the "time-cost" of factoring primitive polynomials $f \in \mathbb{Z}[t]$ of degree n with an efficient algorithm is of order $C(f) = n^u + n^v \log_2 ||f||_\infty$, with $u \geq v + 1 \geq 3$ (see, e.g., [**14**]). However, when the input is a reciprocal polynomial, these algorithms do not take advantage of this fact. Next we outline an algorithm for factoring primitive reciprocal polynomials in $\mathcal{R}$.

1. Compute $\mathsf{R}(f)$ as a matrix-vector product.
2. Factor the primitive polynomial $\mathsf{R}(f)$ of degree n and $||\mathsf{R}(f)||_\infty \leq L_{n+2}B$ using a standard algorithm.
3. Recover the irreducible integer factors in $\mathcal{R}$ by multiplying by R_n^{-1}.

Roughly speaking, the outlined algorithm computes the irreducible factors in $\mathcal{R}$ with time-cost of order $n^u + n^v(\log_2 L_{n+2} + \log_2 B)$. This procedure runs asymptotically 2^u times faster than directly factoring f with a standard algorithm. Observe that thanks to the reciprocal mapping we factor polynomials of degree n instead of degree $2n$.

This procedure gives at first the irreducible factorization of f in $\mathcal{R}$. Thus it remains to determine if the irreducible reciprocal factors of f belong to $\mathcal{R}_1$ or $\mathcal{R}_2$. Our counting results show that the case is that they must belong to $\mathcal{R}_1$. Therefore, for most polynomials the factorizations in $\mathcal{R}$ and $\mathbb{Z}[t]$ coincide.

For instance, in [**6**, Lemma 2] it is proved that a 0, 1-reciprocal polynomial has no nonreciprocal factors. Hence, our algorithm provides the factorization in $\mathbb{Z}[t]$ of any 0, 1-reciprocal polynomial.

It remains open the detailed analysis of this algorithm from the points of view of worst-case and average-case complexity.

ACKNOWLEDGMENT. The authors wish to thank two anonymous reviewers for their comments which greatly contributed to improving this article. Also, the authors specially thank Diego Rial for many helpful conversations.

This work has been supported by project UNGS 30/3222 *Irreducibilidad de polinomios y formación de profesores* and by project Stic AmSud *Alea En Am Sud*.

REFERENCES

1. E. J. Barbeau, *Polynomials*. Problem Books in Mathematics, Springer-Verlag, New York, 1989.
2. S. Beslin, V. de Angelis, The minimal polynomials of $\sin(\frac{2\pi}{p})$ and $\cos(\frac{2\pi}{p})$, *Math. Mag.* **77** (2004) 146–149.
3. K. Dörge, Abschätzung der anzahl der reduziblen polynome, *Math. Ann.* **160** (1965) 59–63.
4. A. Dubickas, On the number of reducible polynomials of bounded naive height, *Manuscripta Math.* **144** (2014) 439–456.
5. M. Filaseta, Course notes on The Theory of Irreducible Polynomials. University of South Carolina, 2013.
6. M. Filaseta, D. Meade, Irreducibility testing of lacunary 0, 1-polynomials, *J. Algorithms* **55** (2005) 21–28.
7. H. J. Hsiao, On factorization of Chebyshev's polynomials of the first kind, *Bull. Inst. Math. Acad. Sin.* **12** (1984) 89–94.
8. G. Kuba, On the distribution of reducible polynomials, *Math. Slovaca* **59** (2009) 349–356.
9. G. Mullen, D. Panario, Eds. *Handbook of Finite Fields*. CRC Press, Boca Raton, FL, 2013.
10. I. Niven, *Irrational Numbers*. The Carus Mathematical Monographs, No. 11, Mathematical Association of America, Washington, DC, 1956.
11. G. Pólya, G. Szegö, *Problems and Theorems in Analysis II*. Reprint of the 1976 Edition. English trans. by C. E. Billigheimer. Springer-Verlag, Berlin, 1998.
12. T. Rivlin, *The Chebyshev Polynomials*. John Wiley & Sons, New York, 1974.
13. M. Rayes, V. Trevisan, P. Wang, Factorization properties of Chebyshev polynomials, *Comput. Math. Appl.* **50** (2005) 1231–1240.
14. J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*. Second ed. Cambridge Univ. Press, Cambridge, 2003.
15. W. Watkins, J. Zeitlin, The minimal polynomial of $\cos(2\pi/n)$, *Amer. Math. Monthly* **100** (1993) 471–474.

ANTONIO CAFURE received his Ph.D. in mathematics from Universidad de Buenos Aires in 2006.
Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (1613) Los Polvorines, Buenos Aires, Argentina.
Ciclo Básico Común, Universidad de Buenos Aires, Ciudad Universitaria, Pabellón III (1428) Buenos Aires, Argentina.
National Council of Science and Technology (CONICET), Argentina.
acafure@ungs.edu.ar

EDA CESARATTO received his Ph.D. in mathematics from Universidad de Buenos Aires in 2005.
Instituto del Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150 (1613) Los Polvorines, Buenos Aires, Argentina.
National Council of Science and Technology (CONICET), Argentina.
ecesarat@ungs.edu.ar