The American Mathematical Monthly

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uamm20

Reciprocity via Reciprocants

Matthew Baker

To cite this article: Matthew Baker (2025) Reciprocity via Reciprocants, The American Mathematical Monthly, 132:4, 303-315, DOI: 10.1080/00029890.2024.2439819

To link to this article: https://doi.org/10.1080/00029890.2024.2439819

Reciprocity via Reciprocants

Matthew Baker

Abstract. The resultant of two reciprocal polynomials of even degree has a canonical square root given by their *reciprocant*. Computing the reciprocant of two cyclotomic polynomials yields a short and elegant proof of the Law of Quadratic Reciprocity.

1. INTRODUCTION. Let p be a prime number and let a be an integer not divisible by p. The *Legendre symbol* $(\frac{a}{p})$ is defined by $(\frac{a}{p}) = 1$ if a is a square modulo p and $(\frac{a}{p}) = -1$ otherwise.

According to *Euler's criterion* (see Appendix C), $a^{(p-1)/2} \equiv 1 \pmod{p}$ if $(\frac{a}{p}) = 1$ and $a^{(p-1)/2} \equiv -1 \pmod{p}$ if $(\frac{a}{p}) = -1$.

The Law of Quadratic Reciprocity, first proved by Gauss in [1], asserts that there is an unexpected relationship between $(\frac{p}{q})$ and $(\frac{q}{p})$ when p, q are distinct odd primes, and a supplement to the law asserts that $(\frac{2}{p})$ depends only on p modulo 8.

Theorem 1 (Law of Quadratic Reciprocity).

(a) *If p and q are distinct odd primes then* $(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. *In other words,* $(\frac{p}{q}) = (\frac{q}{p})$ *unless* $p \equiv q \equiv 3 \pmod 4$, *in which case* $(\frac{p}{q}) = -(\frac{q}{p})$.

(b) *If p is an odd prime then* $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ *and* $(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$. *In other words,* $(\frac{-1}{p}) = 1$ *if* $p \equiv 1 \pmod 4$ *and* $(\frac{-1}{p}) = -1$ *if* $p \equiv 3 \pmod 4$, *and* $(\frac{2}{p}) = 1$ *if* $p \equiv 1, 7 \pmod 8$ *and* $(\frac{2}{p}) = -1$ *if* $p \equiv 3, 5 \pmod 8$.

Note that the supplementary law for $(\frac{-1}{p})$ is an immediate consequence of Euler's criterion.

There are currently more than 300 known proofs of the Law of Quadratic Reciprocity [2]. In this paper we will present an elegant proof that deserves to be better known. The basic approach, via the identity

$$\mathrm{Res}(g, f) = (-1)^{\deg(f)\cdot\deg(g)}\mathrm{Res}(f, g) \tag{1}$$

for resultants, appears to have been independently discovered on at least two occasions [3, 4], see Section 5 for a discussion of related work.

Our exposition is somewhat novel, in that a central role is played by an expression that we dub the *reciprocant*.[1] The resultant of two reciprocal[2] polynomials f and g of even degree is always a square, and the reciprocant of f and g furnishes a canonical square root. If p and q are distinct primes, the resultant of the cyclotomic polynomials $\Phi_p(x)$ and $\Phi_q(x)$ is always equal to 1, but their reciprocant $\mathrm{Rec}(\Phi_p(x), \Phi_q(x))$ turns

doi.org/10.1080/00029890.2024.2439819
MSC: 11A15

[1] This is not a standard term; we chose the name both because it involves reciprocal polynomials and because of its relation to quadratic reciprocity.

[2] Reciprocal means that the coefficients read the same backwards and forwards; see Section 2 for more details.

out to be the Legendre symbol $(\frac{q}{p})$. By symmetry, we have $\mathrm{Rec}(\Phi_q(x), \Phi_p(x)) = (\frac{p}{q})$, and part (a) of the Law of Quadratic Reciprocity is then a consequence of (1).

We also provide a proof via reciprocants of the supplementary law (Theorem 1(b)) for $(\frac{2}{p})$.

Our proof of the resultant identity $\mathrm{Res}(\Phi_p(x), \Phi_q(x)) = 1$ is original, to the best of our knowledge. It is in some ways more elementary than the other proofs we have seen of this formula.

Throughout the article, we strive to keep the exposition as elementary as possible, with the goal of making the paper understandable by a reader who has taken basic undergraduate courses in number theory, abstract algebra, and linear algebra. In order to make the paper as self-contained as possible, we provide three appendices, one on resultants, one on the trace polynomial (which is used to define the reciprocant), and one on Euler's criterion.

2. RESULTANTS AND RECIPROCANTS. All rings in this paper will be commutative rings with identity.

We denote by $\mathrm{LC}(f)$ the leading coefficient of a polynomial f.

Resultants. The resultant of two non-zero polynomials $f, g \in R[x]$ over an integral domain R is an element of R which is typically defined as the determinant of a certain matrix, the so-called *Sylvester matrix* associated to f and g (see [5]).

For our purposes, all we will need to know about the resultant is that it satisfies the following properties:

(RES1) If $f(x) = \mathrm{LC}(f)(x - \alpha_1) \cdots (x - \alpha_m)$ with all α_i in R, then

$$\mathrm{Res}(f, g) = \mathrm{LC}(f)^{\deg(g)} \prod_i g(\alpha_i).$$

(RES2) $\mathrm{Res}(g, f) = (-1)^{\deg(f)\cdot\deg(g)}\mathrm{Res}(f, g)$.

(RES3) Suppose $\phi : R \to R'$ is a ring homomorphism and that neither $\mathrm{LC}(f)$ nor $\mathrm{LC}(g)$ belongs to $\ker(\phi)$. Then[3]

$$\phi(\mathrm{Res}(f, g)) = \mathrm{Res}(\phi(f), \phi(g)).$$

(RES4) If $g(x) = f(x) \cdot q(x) + r(x)$ with $f, g, q, r \in R[x]$ non-zero and $\deg(r) \leq \deg(g)$, then

$$\mathrm{Res}(f, g) = \mathrm{LC}(f)^{\deg(g)-\deg(r)}\mathrm{Res}(f, r).$$

Note that (RES1) implies that $\mathrm{Res}(f, g) = 0$ if and only if f and g have a common root over some field containing R.

In Appendix A, we will (following S. Barnett [6]) define $\mathrm{Res}(f, g)$ as the determinant of a different matrix, and we will give self-contained proofs of the identities (RES1)-(RES4). Note that property (RES1) completely characterizes $\mathrm{Res}(f, g)$ over an integral domain R, so *a posteriori* our definition of the resultant agrees with the more common one based on Sylvester matrices.

[3]Here $\phi(f) \in R'[x]$ denotes the image of $f \in R[x]$ under the homomorphism $R[x] \to R'[x]$ induced by ϕ, and similarly for $\phi(g)$.

Reciprocal polynomials and their traces. A polynomial $g(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ with coefficients in a ring R is called *reciprocal* if $a_n \neq 0$ and $a_k = a_{n-k}$ for all $k = 0, 1, \ldots, n$. Equivalently, g is reciprocal if and only if $g(x) = x^n g(\frac{1}{x})$.

If $g \in R[x]$ is reciprocal of even degree $2m$, then by Proposition 9 in Appendix B there is a unique polynomial $g^{\#}(x) \in R[x]$ of degree m such that

$$g(x) = x^m g^{\#}(x + \frac{1}{x}). \tag{2}$$

We call $g^{\#}(x)$ the *trace polynomial* of g. Note that if $g(x)$ is monic, then $g^{\#}(x)$ is monic as well.

The following result will also be proved in Appendix B:

Proposition 2. *Let R be ring and let K be a field.*

(a) *If $g(x) \in R[x]$ and $g(x) = \prod_{i=1}^{m}(x - \alpha_i)(x - \alpha_i^{-1})$ for some units $\alpha_1, \ldots, \alpha_m \in R^{\times}$, then g is reciprocal of degree $2m$ and*

$$g^{\#}(x) = \prod_{i=1}^{m} \left(x - (\alpha_i + \alpha_i^{-1})\right). \tag{3}$$

(b) *Conversely, if $g \in K[x]$ is monic and reciprocal of even degree $2m$, and L is a splitting field for g over K, then there exist $\alpha_1, \ldots, \alpha_m \in L^{\times}$ such that $g(x) = \prod_{i=1}^{m}(x - \alpha_i)(x - \alpha_i^{-1})$.*

Reciprocants. The determinant of a skew-symmetric matrix has a canonical square root given by the Pfaffian [7, XV, Section 9]. Similarly, the resultant of two monic reciprocal polynomials of even degree over an integral domain R has a canonical square root given by their *reciprocant*, defined as $\mathrm{Rec}(f, g) := \mathrm{Res}(f^{\#}, g^{\#}) \in R$.

Proposition 3. *If R is an integral domain and $f, g \in R[x]$ are monic reciprocal polynomials of even degree, then*

$$\mathrm{Res}(f, g) = \mathrm{Rec}(f, g)^2.$$

Proof. Let K be the fraction field of R and let L be a splitting field for f over K. By Proposition 2(b), we can write $f(x) = \prod_{i=1}^{m}(x - \alpha_i)(x - \alpha_i^{-1})$ with $\alpha_i \in L$ for all i. In what follows, will apply (RES3) to the natural injective map $\phi : R \to L$.

Let $a_i = \alpha_i + \alpha_i^{-1}$ for $i = 1, \ldots, m$. We have:

$$\begin{aligned}
\mathrm{Res}(f^{\#}, g^{\#})^2 &= \prod_i g^{\#}(a_i) \cdot \prod_i g^{\#}(a_i) \qquad \text{(by (RES1), (RES3), and (3))} \\
&= \prod_i \alpha_i^{-m} g(\alpha_i) \cdot \prod_i \alpha_i^{m} g(\alpha_i^{-1}) \qquad \text{(by (2))} \\
&= \prod_i g(\alpha_i) \cdot \prod_i g(\alpha_i^{-1}) \\
&= \mathrm{Res}(f, g) \qquad \text{(by (RES1))}.
\end{aligned}$$

■

We will also need the following property of reciprocants, which is a simple consequence of (RES3):

Proposition 4. *If $g_1, g_2, h \in \mathbb{Z}[x]$ are monic and reciprocal polynomials of even degree and n is a positive integer such that $g_1 \equiv g_2 \pmod{n}$, then*

$$\mathrm{Rec}(g_1, h) \equiv \mathrm{Rec}(g_2, h) \pmod{n}$$

and

$$\mathrm{Rec}(h, g_1) \equiv \mathrm{Rec}(h, g_2) \pmod{n}.$$

Proof. It suffices, by (RES2), to prove the following statement: if $g_1, g_2, h \in \mathbb{Z}[x]$ are monic and reciprocal of even degree and n is a positive integer such that $g_1 \equiv g_2 \pmod{n}$, then $\mathrm{Rec}(g_1, h) \equiv \mathrm{Rec}(g_2, h) \pmod{n}$. By (2), we have $g_1^{\#}(x) \equiv g_2^{\#}(x) \pmod{n}$. Applying (RES3) to the natural ring homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ shows that $\mathrm{Res}(g_1^{\#}, h^{\#}) \equiv \mathrm{Res}(g_2^{\#}, h^{\#}) \pmod{n}$ as desired. ∎

3. PROOF OF THE LAW OF QUADRATIC RECIPROCITY. For $n \geq 1$, define

$$g_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1 \in \mathbb{Z}[x]. \tag{4}$$

If p is prime, then since $x^p - 1 \equiv (x-1)^p \pmod{p}$ we have

$$g_p(x) \equiv (x-1)^{p-1} \pmod{p}. \tag{5}$$

Proposition 5. *If m, n are relatively prime positive integers,* $\mathrm{Res}(g_m, g_n) = 1$.

Proof. If $m = n = 1$ then $\mathrm{Res}(g_m, g_n) = \mathrm{Res}(1, 1) = 1$. We may therefore suppose without loss of generality that $n > m$. Note that since $\gcd(m, n) = 1$, at least one of m and n is odd.

By the division algorithm, we can write $n = mq + r$ with q, r integers such that $q \geq 1$ and $0 \leq r < q$. Since at least one of m and n is odd, the same is true for m and r.

Working in the quotient ring $\mathbb{Z}[x]/(x^m - 1)$, we have

$$\begin{aligned} x^n - 1 &\equiv (x^m)^q \cdot x^r - 1 \\ &\equiv 1^q \cdot x^r - 1 \\ &\equiv x^r - 1 \pmod{x^m - 1}. \end{aligned}$$

In other words, there is a polynomial $h(x) \in \mathbb{Z}[x]$ such that

$$x^n - 1 = (x^m - 1)h(x) + x^r - 1.$$

Dividing both sides by $x - 1$ gives

$$g_n(x) = g_m(x)h(x) + g_r(x).$$

By (RES4) and (RES2), we have

$$\mathrm{Res}(g_m, g_n) = \mathrm{Res}(g_m, g_r) = \mathrm{Res}(g_r, g_m). \tag{6}$$

Since $\gcd(m, n) = 1$, it follows from (6) and the Euclidean algorithm that there is an integer $k \geq 1$ such that

$$\mathrm{Res}(g_m, g_n) = \mathrm{Res}(g_k, g_1) = \mathrm{Res}(g_k, 1) = 1.$$

■

Remark. Conversely, if $\gcd(m, n) = d > 1$ then (RES1) and (RES3) (applied to the natural injection $\phi : \mathbb{Z} \hookrightarrow \mathbb{C}$) imply that $\mathrm{Res}(g_m, g_n) = 0$, since a primitive d^{th} root of unity in $\mathbb{C}$ is a common root of g_m and g_n.

Remark. Here is an alternate proof of Proposition 5 which is arguably more conceptual, but somewhat less elementary. First, observe that if K is any field and $\alpha \in K$ satisfies both $\alpha^m = 1$ and $\alpha^n = 1$, with $\gcd(m, n) = 1$, then necessarily $\alpha = 1$. Let p be a prime number, let $\mathbb{F}_p$ be the finite field of order p, and let $\phi : \mathbb{Z} \to \mathbb{F}_p$ be the natural homomorphism. Applying (RES3) to ϕ implies, together with (RES1) and the above observation with $K = \mathbb{F}_p$, that $\mathrm{Res}(g_m, g_n) \not\equiv 0 \pmod{p}$. Since this holds for all prime numbers p, we must have $\mathrm{Res}(g_m, g_n) = \pm 1$. By Proposition 3, we must in fact have $\mathrm{Res}(g_m, g_n) = 1$.

Assume from now on that n is odd. Since g_n is a reciprocal polynomial of even degree, it follows from (2) that

$$g_n^{\#}(2) = g_n(1) = n. \tag{7}$$

Furthermore, for any ring R, if $g(x) = (x-1)^{2m} \in R[x]$ then, by Proposition 2,

$$g^{\#}(x) = (x-2)^m. \tag{8}$$

Remark. By (14), we have $g_1^{\#}(x) = 1$ and $g_3^{\#}(x) = x + 1$, and

$$g_n^{\#}(x) = x g_{n-2}^{\#}(x) - g_{n-4}^{\#}(x) \tag{9}$$

for all odd integers $n \geq 5$. This implies that the polynomials $g_n^{\#}$ are related to the classical *Lucas polynomials* $L_n(x)$, defined for $n \geq 0$ by $L_0(x) = 2$, $L_1(x) = x$, and $L_n(x) = x L_{n-1}(x) + L_{n-2}(x)$, as follows. For $n \geq 1$ odd, define $H_n(x)$ by $L_n(x) = x H_n(x^2)$. Then $g_n^{\#}(x) = H_n(x-2)$.

Proof of the Law of Quadratic Reciprocity. Let p, q be distinct odd primes.

Since $\mathrm{Res}(g_p, g_q) = 1$ by Proposition 5, it follows from Proposition 3 that $\mathrm{Rec}(g_p, g_q) \in \{\pm 1\}$. We compute the following congruences modulo p:

$$\begin{aligned}
\mathrm{Rec}(g_p, g_q) &\equiv \mathrm{Rec}((x-1)^{p-1}, g_q) && \text{(by (5) and Proposition 4)} \\
&\equiv \mathrm{Res}((x-2)^{\frac{p-1}{2}}, g_q^{\#}) && \text{(by (8) and the definition of the reciprocant)} \\
&= g_q^{\#}(2)^{\frac{p-1}{2}} && \text{(by (RES1))} \\
&= q^{\frac{p-1}{2}} && \text{(by (7))} \\
&\equiv \left(\frac{q}{p}\right) && \text{(by Euler's criterion).}
\end{aligned}$$

Since $\mathrm{Rec}(g_p, g_q)$ and $(\frac{q}{p})$ both belong to $\{\pm 1\}$, it follows that

$$\mathrm{Rec}(g_p, g_q) = \left(\frac{q}{p}\right). \tag{10}$$

By symmetry, we also have

$$\mathrm{Rec}(g_q, g_p) = \left(\frac{p}{q}\right). \tag{11}$$

The Law of Quadratic Reciprocity now follows from (10), (11), and (RES2). ∎

4. THE SUPPLEMENTARY LAW. We can use a similar argument to prove the supplementary law characterizing $(\frac{2}{p})$ when p is an odd prime. Actually, it turns out to be more straightforward to establish a formula for $(\frac{-2}{p})$.

By Euler's criterion, we have

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{2}{p}\right),$$

so the supplementary law is equivalent to:

Theorem 6. *If p is an odd prime then $(\frac{-2}{p}) = 1$ if $p \equiv 1$ or $3 \pmod 8$ and $(\frac{-2}{p}) = -1$ if $p \equiv 5$ or $7 \pmod 8$.*

Instead of the polynomial $g_2(x) = x + 1$, we will use the cyclotomic polynomial $\Phi_4(x) = x^2 + 1$. Note that Φ_4 is a reciprocal polynomial of even degree, with $\Phi_4^{\#}(x) = x$.

Proposition 7. *If n is an odd positive integer, then $\mathrm{Rec}(\Phi_4, g_n)$ is equal to 1 if n is 1 or 3 (mod 8) and -1 if n is 5 or 7 (mod 8).*

Proof. We have

$$\mathrm{Rec}(\Phi_4, g_n) = \mathrm{Res}(x, g_n^{\#}) = g_n^{\#}(0),$$

so it suffices to evaluate $g_n^{\#}(0)$.

This is a straightforward calculation given (2), which implies that

$$g_n^{\#}(0) = g_n(i) i^{-\frac{n-1}{2}} = \frac{i^n - 1}{i - 1} i^{-\frac{n-1}{2}},$$

where $i^2 = -1 \in \mathbb{C}$.

Alternatively, recall from (9) that for $n \geq 5$ odd we have

$$g_n^{\#}(x) = x g_{n-2}^{\#}(x) - g_{n-4}^{\#}(x).$$

From this, a simple inductive argument shows that $g_n^{\#}(0) = 1$ if n is 1 or 3 (mod 8) and -1 if n is 5 or 7 (mod 8). ∎

Proof of Theorem 6. Let p be an odd prime. We compute:

$$\begin{aligned}
\mathrm{Rec}(\Phi_4, g_p) &\equiv \mathrm{Rec}(\Phi_4, (x-1)^{p-1}) && \text{(by (5) and Proposition 4)} \\
&\equiv \mathrm{Res}(x, (x-2)^{\frac{p-1}{2}}) && \text{(by (8) and the definition of the reciprocant)}
\end{aligned}$$

$$= (-2)^{\frac{p-1}{2}} \qquad \text{(by (RES1))}$$

$$\equiv \left(\frac{-2}{p}\right) \pmod{p} \qquad \text{(by Euler's criterion).}$$

Since $\mathrm{Rec}(\Phi_4, g_p)$ and $(\frac{-2}{p})$ both belong to $\{\pm 1\}$, we have $\mathrm{Rec}(\Phi_4, g_p) = (\frac{-2}{p})$, which implies the desired result via Proposition 7. ∎

5. RELATED WORK. The proof of Quadratic Reciprocity given here is closely related to several existing arguments. The earliest reference we are aware of for a proof of quadratic reciprocity based on resultants of cyclotomic polynomials is J.-Y. Mérindol's paper [**3**], which was published in a French higher education journal called *L'Ouvert*. A similar proof appears to have been independently discovered by S. Hambleton and V. Scharaschkin in [**4**]. We learned of the basic argument behind these papers from A. Chambert-Loir's blog post [**8**].

The main new ingredient in the present paper is a systematic use of Proposition 3 and the quantity we have dubbed the reciprocant. As far as we know, our arguments proving the supplementary law (Theorem 6) are also new.

Our treatment of resultants was inspired by a paper of S. Barnett [**6**]. Our proof of Proposition 5 makes use of the Euclidean algorithm and property (RES4) of resultants; this approach is also used, for example, in [**9**].

Although we have not seen Proposition 3 explicitly stated in a published paper, it is mentioned without proof in a Math Overflow post by D. Serre [**10**]. The main ingredients in the proof of Proposition 3 are also contained in the proof of [**11**, Theorem 3.4].

The first published work we are aware of that computes the resultant of two cyclotomic polynomials is F. E. Diederichsen's paper [**12**]. Diederichsen's results were extended, and his proofs simplified, in T. Apostol's paper [**13**]. Some other papers computing resultants of Fibonacci–Lucas type polynomials include [**3**, **4**, **9**, **11**].

As noted in [**4**, Section 3], the key step underlying our proof of Quadratic Reciprocity, which is identifying the Legendre symbol with a resultant, is closely related to one of G. Eisenstein's classical proofs [**14**, Chapter 8.1]. There are also close connections to the more recent proof of R. Swan [**15**].

A resultant-based approach to quadratic reciprocity in the function field case is given in [**16**]. See Section 3.4 of *loc. cit.* for remarks about other proofs of the Law of Quadratic Reciprocity which ultimately boil down (either explicitly or in disguise) to property (RES2) of resultants.

A. RESULTANTS. Let R be a ring and let $f, g \in R[x]$ be nonzero polynomials. As above, we denote by $\mathrm{LC}(f)$ the leading coefficient of f.

If $f = c$ is a constant polynomial, we define the *resultant* of f and g to be

$$\mathrm{Res}(f, g) := c^{\deg(g)}.$$

Otherwise, we set

$$\mathrm{Res}(f, g) := \mathrm{LC}(f)^{\deg(g)} \det\left(g(C_f)\right) \in R,$$

where C_f is the *companion matrix* of $f(x)/\mathrm{LC}(f) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1} + x^m$:

$$C_f := \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -a_{m-1} \end{pmatrix}.$$

We assume for the rest of this section that R is an integral domain with fraction field K. We will use the following two well-known facts from linear algebra:

(LA1) The characteristic polynomial of C_f over K is f (cf. [17, Lemma 8.4]).

(LA2) If an $m \times m$ matrix A over K has characteristic polynomial f, and if f factors over some extension field L of K as $f(x) = (x - \lambda_1) \cdots (x - \lambda_m)$, then the characteristic polynomial of $g(A)$ is $(x - g(\lambda_1)) \cdots (x - g(\lambda_m))$. (**Proof:** The characteristic polynomial of A over K is equal to its characteristic polynomial over L. By [17, Theorem 14.17], A is similar over L to an upper triangular matrix B with $\lambda_1, \ldots, \lambda_m$ on the diagonal. Therefore $g(A)$ is similar over L to $g(B)$. The diagonal entries of $g(B)$ are $g(\lambda_1), \ldots, g(\lambda_m)$, and similar matrices have the same characteristic polynomial, cf. [17, Theorem 8.12].)

Our goal is now to prove the properties (RES1)–(RES4) from Section 2. We formulate this as a theorem:

Theorem 8. *Let R be a ring and let $f, g \in R[x]$ be nonzero polynomials. Then:*

(RES1) *If $f(x) = \mathrm{LC}(f)(x - \alpha_1) \cdots (x - \alpha_m)$ with all α_i in R, then*

$$\mathrm{Res}(f, g) = \mathrm{LC}(f)^{\deg(g)} \prod_i g(\alpha_i).$$

(RES2) $\mathrm{Res}(g, f) = (-1)^{\deg(f)\cdot\deg(g)}\mathrm{Res}(f, g)$.

(RES3) *Suppose $\phi : R \to R'$ is a ring homomorphism and that neither* $\mathrm{LC}(f)$ *nor* $\mathrm{LC}(g)$ *belongs to* $\ker(\phi)$. *Then*

$$\phi(\mathrm{Res}(f, g)) = \mathrm{Res}(\phi(f), \phi(g)).$$

(RES4) *If $g(x) = f(x) \cdot q(x) + r(x)$ with $f, g, q, r \in R[x]$ nonzero and* $\deg(r) \leq \deg(g)$, *then*

$$\mathrm{Res}(f, g) = \mathrm{LC}(f)^{\deg(g)-\deg(r)}\mathrm{Res}(f, r).$$

Proof. Assume f splits into linear factors over R as

$$f(x) = LC(f)(x - \alpha_1) \cdots (x - \alpha_m).$$

Then by (LA1) and (LA2), the characteristic polynomial of $g(C_f)$ over K is

$$(x - g(\alpha_1)) \cdots (x - g(\alpha_m)).$$

It follows that the determinant of $g(C_f)$ is $\prod_{i=1}^{m} g(\alpha_i)$, which proves (RES1). Moreover, if $g(x) = LC(g)(x - \beta_1)\cdots(x - \beta_n)$ with all $\beta_j \in R$, then (RES1) may be stated as

$$\operatorname{Res}(f, g) = \operatorname{LC}(f)^{\deg(g)}\operatorname{LC}(g)^{\deg(f)} \prod_{i,j}(\alpha_i - \beta_j) \in R. \tag{12}$$

If f and g are monic and we view their coefficients as indeterminates, the expression $\det\left(g(C_f)\right)$ is a polynomial of degree $m + n$ with integer coefficients in these variables. In other words, there is a multivariate polynomial

$$S_{m,n} \in \mathbb{Z}[x_0, x_1, \ldots, x_{m-1}, y_0, y_1, \ldots, y_{n-1}]$$

such that for every ring R and every pair of monic polynomials $f(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1} + x^m$ and $g(x) = b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + x^n$ in $R[x]$,

$$\operatorname{Res}(f, g) = S_{m,n}(a_0, a_1, \ldots, a_{m-1}, b_0, b_1, \ldots, b_{n-1}).$$

The "functoriality" relation (RES3) follows easily from this observation.

By (RES3) and the fact that R is an integral domain, we may replace R by a splitting field L for fg over the fraction field K of R. The identity (RES2) then follows immediately from (12).

Using (RES1), we compute:

$$\begin{aligned}
\operatorname{LC}(f)^{\deg(g)-\deg(r)}\operatorname{Res}(f(x), r(x)) &= \operatorname{LC}(f)^{\deg(g)} \prod_{i=1}^{m} r(\alpha_i) \\
&= \operatorname{LC}(f)^{\deg(g)} \prod_{i=1}^{m} (g(\alpha_i) - f(\alpha_i)q(\alpha_i)) \\
&= \operatorname{LC}(f)^{\deg(g)} \prod_{i=1}^{m} g(\alpha_i) \\
&= \operatorname{Res}(f(x), g(x)),
\end{aligned}$$

which proves (RES4). ∎

B. THE TRACE POLYNOMIAL. Our first goal in this Appendix is to prove:

Proposition 9. *Suppose R is a ring and $g \in R[x]$ is a reciprocal polynomial of even degree $2m$. Then there is a unique polynomial $h(x) \in R[x]$ of degree m such that $g(x) = x^m h(x + \frac{1}{x})$.*

The following proof was suggested by Darij Grinberg.

Proof. We first prove the existence of $h(x)$. This will be done by induction on m. The base case $m = 0$ is clear. For the induction step, let $g(x) = a_0 + a_1 x + \cdots + a_{2m}x^{2m}$ be a reciprocal polynomial of degree $2m$; in particular, $a_{2m} = a_0$. Thus $\tilde{g}(x) := \left(g(x) - a_0(1 + x^2)^m\right)/x$ is a reciprocal polynomial of degree $2(m - 1)$. By the inductive hypothesis, $\tilde{g}(x) = x^{m-1}\tilde{h}(x + 1/x)$ for some polynomial $\tilde{h}(x)$ of degree $m - 1$. Setting $h(x) = a_0 x^m + \tilde{h}(x)$ yields $g(x) = x^m h(x + 1/x)$, as desired. This establishes the existence of h.

The uniqueness of h follows by reversing the existence argument. More formally, we again proceed by induction on m. The base case $m = 0$ is obvious. For the induction step, note that the equation $g(x) = x^m h(x + 1/x)$ implies that the x^m-coefficient of $h(x)$ must be a_0. Let $\tilde{h}(x) = h(x) - a_0 x^m$, which has degree $m - 1$, and let $\tilde{g}(x) = \left(g(x) - a_0(1 + x^2)^m\right)/x$, which is reciprocal of degree $2(m - 1)$. Then $\tilde{g}(x) = x^{m-1}\tilde{h}(x + 1/x)$, and by the inductive hypothesis $\tilde{h}(x)$ is uniquely determined by $\tilde{g}(x)$. It follows that h is uniquely determined by g. ∎

Following the terminology of [**18**, Section 2.1], we define the *trace polynomial* $g^{\#}$ of g to be the polynomial h appearing in Proposition 9.

Remark. The following alternative proof of the existence portion of Proposition 9 was suggested by Franz Lemmermeyer, and provides an explicit recursion which will be useful in the next remark.

Write $g(x) = a_0 + a_1 x + \cdots + a_{2m} x^{2m}$ with $a_i = a_{2m-i}$ for all $0 \le i \le m$ and $h(x) = b_0 + b_1 x + \cdots + b_m x^m$. We wish to prove that we can uniquely solve for the coefficients of h in terms of the coefficients of g.

In the Laurent polynomial ring $R[x, \frac{1}{x}]$, we have the identity

$$x^{-m} g(x) = a_0(x^m + x^{-m}) + a_1(x^{m-1} + x^{-(m-1)}) + \cdots + a_{m-1}(x + x^{-1}) + a_m,$$

so it suffices to prove the result for the special Laurent polynomials $f_n(x) := x^n + x^{-n}$ for all $n \ge 0$. In other words, we want to prove that for each $n \ge 0$, there is a polynomial $h_n(x) \in R[x]$ of degree n such that $f_n(x) = h_n(x + x^{-1})$.

We prove existence of the polynomials $h_n(x)$ by induction on n. The result is trivial for $n = 0, 1$, so we may assume that $n \ge 2$ and that the result is true for polynomials of degree at most $n - 1$. A simple calculation gives

$$f_n(x) = (x + x^{-1}) f_{n-1}(x) - f_{n-2}.$$

Therefore, if we set $h_0(x) = 2$, $h_1(x) = x$, and

$$h_n(x) = x h_{n-1}(x) - h_{n-2}(x), \tag{13}$$

we will have the desired identity $f_n(x) = h_n(x + x^{-1})$.

Remark. For $n \ge 0$, define $g_{2n+1}(x) = \sum_{k=0}^{2n} x^k$ as in (4).

Then with $f_k(x)$ and $h_k(x)$ as in the previous remark, for $n \ge 1$ we have $x^{-n} g_{2n+1} = 1 + \sum_{k=1}^{n} f_k(x)$, and thus $g^{\#}_{2n+1}(x) = 1 + \sum_{k=1}^{n} h_k(x)$.

Since $g_1(x) = 1$ and $g_3(x) = 1 + x + x^2$, we have $g^{\#}_1(x) = 1$ and $g^{\#}_3(x) = x + 1$. Moreover, since $h_k(x) = x h_{k-1}(x) - h_{k-2}(x)$ for $k \ge 2$, it follows from (13) that for $n \ge 2$,

$$\begin{aligned} x g^{\#}_{2n-1}(x) - g^{\#}_{2n-3}(x) &= x + \sum_{k=1}^{n-1} (x h_k(x) - h_{k-1}(x)) - 1 + h_0 \\ &= 1 + x + \sum_{k=2}^{n} h_k(x) \\ &= g^{\#}_{2n+1}. \end{aligned}$$

In other words, for all odd integers $n \geq 5$ we have

$$g_n^{\#}(x) = x g_{n-2}^{\#}(x) - g_{n-4}^{\#}(x). \tag{14}$$

We now provide a proof of Proposition 2 from Section 2.

Proof of Proposition 2. We begin with the proof of part (a). To see that $g(x) = \prod_{i=1}^{m}(x-\alpha_i)(x-\alpha_i^{-1})$ is reciprocal, we compute:

$$\begin{aligned} x^{2m} g(\frac{1}{x}) &= x^{2m} \prod (\frac{1}{x} - \alpha_i)(\frac{1}{x} - \frac{1}{\alpha_i}) \\ &= \prod (1 - \alpha_i x)(1 - \frac{1}{\alpha_i} x) \\ &= (-1)^m \prod \alpha_i (x - \frac{1}{\alpha_i}) \cdot (-1)^m \prod \frac{1}{\alpha_i}(x - \alpha_i) \\ &= \prod (x - \frac{1}{\alpha_i})(x - \alpha_i) \\ &= g(x). \end{aligned}$$

To prove (3), the case $m = 1$ can be handled by a simple computation: setting $\alpha = \alpha_1$ and $a = \alpha + \alpha^{-1}$, we have $g(x) = (x-\alpha)(x-\alpha^{-1}) = x^2 - ax + 1 = x(x + \frac{1}{x} - a)$, and thus $g^{\#}(x) = x - a$. The general case follows immediately from the special case $m = 1$: if $a_j = \alpha_j + \alpha_j^{-1}$ then $g^{\#}(x) = \prod_{j=1}^{m}(x - a_j)$.

For part (b), since $g(x)$ is reciprocal we have $g(x) = x^n g(\frac{1}{x})$, where $n = 2m$. Therefore $\alpha \in L^{\times}$ is a root of $g(x)$ if and only if α^{-1} is. Since an element $\alpha \in L$ satisfies $\alpha^2 = 1$ iff $\alpha = \pm 1$, we can write $g(x) = (x-1)^k (x+1)^{\ell} \prod_{i=1}^{t}(x-\alpha_i)(x-\alpha_i^{-1})$ with $\alpha_i \in L^{\times} \backslash \{1, -1\}$. It therefore suffices to prove that each of 1 and -1 has even multiplicity as a root of $g(x)$.

If K has characteristic 2 then $1 = -1$ in K and so $g(x) = (x-1)^s \prod_{i=1}^{t}(x - \alpha_i)(x - \alpha_i^{-1})$, where $s = k + \ell$ is the multiplicity of 1 as a root of $g(x)$. Since $g(x)$ has even degree, it follows that s is even. So we may assume that K does not have characteristic 2.

Since $(x-\alpha)^2 = x^2(\frac{1}{x} - \alpha)^2$ for $\alpha \in \{1, -1\}$, it follows that if $g(x)$ is monic reciprocal of even degree and $(x-\alpha)^2$ divides $g(x)$ with $\alpha \in \{1, -1\}$, then $\frac{g(x)}{(x-\alpha)^2}$ is monic reciprocal of even degree as well. By induction, it therefore suffices to prove that if either 1 or -1 is a root of $g(x)$ then it must be a double root.

To see this, note that the chain rule applied to the right-hand side of the identity $g(x) = x^n g(\frac{1}{x})$ yields

$$g'(x) = n x^{n-1} g(\frac{1}{x}) - x^{n-2} g'(\frac{1}{x}). \tag{15}$$

Assuming that $g(\alpha) = 0$ with $\alpha \in \{1, -1\}$, evaluating (15) at $x = \alpha$ gives $g'(\alpha) = -g'(\alpha)$. Since K does not have characteristic 2, it follows that $g'(\alpha) = 0$ as claimed. ∎

C. EULER'S CRITERION. In this Appendix, we present a proof of Euler's criterion which is more elementary than the typical proofs one finds based on primitive

roots or Lagrange's theorem on the number of roots of a polynomial modulo p. The argument—which deserves to be better known—is adapted from [19]. We begin with:

Lemma 10. *If p is prime then the only solutions to $x^2 \equiv b^2 \pmod{p}$ are $x \equiv \pm b$.*

Proof. We have $x^2 \equiv b^2 \pmod{p}$ if and only if $p \mid x^2 - b^2$ if and only if $p \mid (x - b)(x + b)$. Since p is prime, the latter occurs if and only if $p \mid x - b$ or $p \mid x + b$. ■

As a warm-up, before tackling Euler's criterion we first prove a result known as "Wilson's theorem":

Lemma 11 (Wilson's theorem). *If p is prime then $(p-1)! \equiv -1 \pmod{p}$.*

Proof. If $p = 2$ the result is clear, so we may assume that p is odd. Since p is prime, Lemma 10 shows that the only solutions to $x^2 \equiv 1 \pmod{p}$ are $x \equiv \pm 1$. Therefore the $p - 1$ nonzero residues mod p can be partitioned into $\frac{p-3}{2}$ pairs $\{x, y\}$ of distinct elements such that $xy \equiv 1 \pmod{p}$, together with the two elements $\{1, -1\}$. Multiplying these elements together and noting that $1 \cdot (-1) \equiv -1 \pmod{p}$ gives

$$(p-1)! \equiv 1^{\frac{p-3}{2}} \cdot 1 \cdot (-1) \equiv -1 \pmod{p}. \tag{16}$$

■

Theorem 12 (Euler's criterion). *If p is an odd prime and a is an integer with $p \nmid a$ then $a^{(p-1)/2} \equiv 1 \pmod{p}$ if $(\frac{a}{p}) = 1$ and $a^{(p-1)/2} \equiv -1 \pmod{p}$ if $(\frac{a}{p}) = -1$.*

Proof. If $(\frac{a}{p}) = -1$, the $p - 1$ nonzero residues mod p can be partitioned into $\frac{p-1}{2}$ pairs $\{x, y\}$ of distinct elements such that $xy \equiv a \pmod{p}$. Multiplying these elements together and applying Wilson's theorem gives

$$a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}.$$

On the other hand, if $(\frac{a}{p}) = 1$, so that $a \equiv b^2 \pmod{p}$ for some b, then by Lemma 10, the only solutions to $x^2 \equiv a \pmod{p}$ are $x \equiv \pm b$. Therefore the $p - 1$ nonzero residues mod p can be partitioned into $\frac{p-3}{2}$ pairs $\{x, y\}$ of distinct elements such that $xy \equiv a \pmod{p}$, together with the two elements $\{b, -b\}$. Multiplying these elements together and noting that $b \cdot (-b) \equiv -a \pmod{p}$ gives

$$-a^{\frac{p-1}{2}} \equiv a^{\frac{p-3}{2}} \cdot b \cdot (-b) \equiv (p-1)! \pmod{p},$$

and thus, by Wilson's theorem,

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

■

ACKNOWLEDGMENT. We thank Antoine Chambert-Loir for pointing us to J.-Y. Mérindol's paper [3]. Thanks also to Darij Grinberg, Franz Lemmermeyer, Evan O'Dorney, and the anonymous referees for helpful feedback on an earlier version of this paper.

DISCLOSURE STATEMENT. No potential conflict of interest was reported by the author.

ORCID
Matthew Baker http://orcid.org/0000-0001-5951-8814

[1] Gauss CF. Disquisitiones arithmeticae; 1801.
[2] Lemmermeyer F. Proofs of the quadratic reciprocity law. Available from: https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html
[3] Mérindol J-Y. Résultant et symbol de Legendre. *L'Ouvert*;1995;80.
[4] Hambleton S, Scharaschkin V. Quadratic reciprocity via resultants. Int J Number Theory. 2010;6(6):1413–1417.
[5] Sylvester JJ. A method of determining by mere inspection the derivatives from two equations of any degree. Philos Magazine. 1840;16:132–135.
[6] Barnett S. A note on the Bézoutian matrix. SIAM J Appl Math. 1972;22:84–86.
[7] Lang S. Algebra. Revised 3rd ed. Springer graduate texts in mathematics. Berlin: Springer-Verlag; 2002.
[8] Chambert-Loir A. Some proofs of the quadratic reciprocity law; 2020. Available from: https://freedommathdance.blogspot.com/2020/04/some-proofs-of-quadratic-reciprocity-law.html
[9] Flórez R, Higuita R, Ramírez A. The resultant, the discriminant, and the derivative of generalized Fibonacci polynomials. J Integer Seq. 2019;22(4):Art. 19.4.4, 28.
[10] Serre D. Splitting the resultant. Available from: https://mathoverflow.net/questions/282069/splitting-the-resultant-as-when-the-determinant-becomes-the-square-of-the-pfaff.
[11] Loper KA, Werner NJ. Resultants of minimal polynomials of maximal real cyclotomic extensions. J Number Theory. 2016;158:298–315.
[12] Diederichsen F-E. Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz. Abh Math Sem Hansischen Univ. 1940;13:357–412.
[13] Apostol TM. Resultants of cyclotomic polynomials. Proc Amer Math Soc. 1970;24:457–462.
[14] Lemmermeyer F. Reciprocity laws. Springer monographs in mathematics. Berlin: Springer-Verlag; 2000.
[15] Swan RG. Another proof of the quadratic reciprocity theorem? Amer Math Monthly. 1990;97(2):138–139.
[16] Clark PL, Pollack P. Reciprocity by resultant in $k[t]$. Enseign Math. 2019;65(1–2):101–116.
[17] Liesen J, Mehrmann V. Linear algebra. Springer undergraduate mathematics series. Cham: Springer; 2015.
[18] Gross BH, McMullen CT. Automorphisms of even unimodular lattices and unramified Salem numbers. J Algebra. 2002;257(2):265–290.
[19] Hardy GH, Wright EM. An introduction to number theory. 5th ed. Oxford: Oxford University Press; 1979.