Primary Elements in Cyclotomic Fields with Applications to Power Residue Symbols, and More

Éric Brier\textsuperscript{1}, Rémi Géraud-Stewart\textsuperscript{2}, Marc Joye\textsuperscript{3}, David Naccache\textsuperscript{4}

\textsuperscript{1}Malissard, France
\textsuperscript{2}Qualcomm, San Diego, CA, USA
\textsuperscript{3}Zama, Paris, France
\textsuperscript{4}École normale supérieure, Paris, France

Abstract Higher-order power residues have enabled the construction of numerous public-key encryption schemes, authentication schemes, and digital signatures. Their explicit characterization is however challenging; an algorithm of Caranay and Scheidler computes $p^{th}$ power residue symbols, with $p \leq 13$ an odd prime, provided that primary elements in the corresponding cyclotomic field can be efficiently found. In this paper, we describe a new, generic algorithm to compute primary elements in cyclotomic fields; which we apply for $p = 3, 5, 7, 11, 13$. A key insight is a careful selection of fundamental units as put forward by Dénes. This solves an essential step in the Caranay–Scheidler algorithm. We give a unified view of the problem. Finally, we provide the first efficient deterministic algorithm for the computation of the 9\textsuperscript{th} and 16\textsuperscript{th} power residue symbols.

1 MOTIVATION

Quadratic residues played a central role in building the first provably secure public-key cryptosystems [10]. A number is a quadratic residue modulo $n$ when it can be expressed as the square of an integer modulo $n$, although that integer may be hard to find. This notion, along with generalizations to higher powers (called higher-order power residues), have enabled the construction of numerous public-key encryption schemes, authentication schemes, and digital signatures [26, 21, 22, 1, 2, 18].

The computation of $p^{th}$ power residue symbols, when $p$ is an odd prime $\leq 13$, can be performed by a generic algorithm of Caranay and Scheidler [4, § 7], although the concrete implementation for a given $p$ remains challenging (see, e.g., [12] for the 11\textsuperscript{th} power residue symbol and [3] for the 13\textsuperscript{th} power residue symbol). The computation of the 4\textsuperscript{th} power residue symbol [25, 7] and of the 8\textsuperscript{th} power residue symbol [15, Chap. 9] (see also [11]) was solved independently. Finally, a generic algorithm was proposed by de Boer and Pagano [8], but it is inherently a probabilistic method which makes it unusable in most cryptographic settings. This leaves open the question to deterministically compute 9\textsuperscript{th} residue symbols, and all power residue symbols above the 13\textsuperscript{th}.

In this paper, we provide a unified and simplified approach to compute primary elements in cyclotomic fields, encompassing all previously-known results. This makes the Caranay–Scheidler algorithm practical, as it fundamentally relies on the (hitherto specialized) determination of primary elements. We also describe efficient deterministic algorithms for computing the 9\textsuperscript{th} and 16\textsuperscript{th} power residue symbols, which were open problems.

2 DEFINITIONS AND NOTATION

Throughout this paper, unless otherwise specified, $p \leq 13$ denotes an odd rational prime.

Let $\zeta = \zeta_p = e^{2\pi i/p}$ be a primitive $p^{th}$ of unity and let $\omega = 1 - \zeta$. The ring of integers in the cyclotomic field $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$. It is known to be norm-Euclidean [16, 14]; in particular, $\mathbb{Z}[\zeta]$ is a unique factorization domain. Two elements $\alpha$ and $\beta$ of $\mathbb{Z}[\zeta]$ are called associates if they differ only by a unit factor. We write $\alpha \sim \beta$ if $\exists u \in \mathbb{Z}[\zeta]^\times$ such that $\alpha = u\beta$. The element $\omega$ is a prime in $\mathbb{Z}[\zeta]$ above $p$; we have $\omega^{p-1} \sim p$.

Since $\zeta$ is a root of the $p^{th}$ cyclotomic polynomial, $\Phi_p(z) = z^{p-1} + \cdots + z + 1$, any algebraic integer $\alpha \in \mathbb{Z}[\zeta]$ can be expressed as

$$\alpha = \sum_{j=0}^{p-2} a_j \zeta^j \quad \text{with } a_j \in \mathbb{Z}.$$
The powers $\omega^k$ with $0 \leq k \leq p - 2$ also form an integral basis of $\mathbb{Q}(\zeta)$. Given $\alpha = \sum_{j=0}^{p-2} a_j \zeta^j$, an application of the binomial theorem leads to

$$
\alpha = \sum_{j=0}^{p-2} a_j \zeta^j = \sum_{j=0}^{p-2} a_j (1 - \omega)^j = \sum_{j=0}^{p-2} a_j \sum_{k=0}^{j} \binom{j}{k} (-\omega)^k = \sum_{k=0}^{p-2} \sum_{j=k}^{p-2} a_j \binom{j}{k} (-\omega)^k
$$

$$
:= \sum_{k=0}^{p-2} C_k(\alpha) \omega^k
$$

where $C_k(\alpha) = (-1)^k \sum_{j=k}^{p-2} a_j \binom{j}{k}$. (1)

Namely, an algebraic integer $\alpha \in \mathbb{Z}[\zeta]$ can be equally written as $\alpha = \sum_{j=0}^{p-2} c_j \omega^j$ with $c_j = C_j(\alpha) \in \mathbb{Z}$. Note also that writing $\alpha = \sum_{j=0}^{p-2} a_j \zeta^j$, we have $C_0(\alpha) = \sum_{j=0}^{p-2} a_j$ and $C_1(\alpha) = -\sum_{j=1}^{p-2} a_j j$.

The norm and trace of $\alpha \in \mathbb{Z}[\zeta]$ are the rational integers respectively given by $N(\alpha) = \prod_{k=1}^{p-1} \sigma_k(\alpha)$ and $T(\alpha) = \sum_{k=1}^{p-1} \sigma_k(\alpha)$, where $\sigma_k : \zeta \mapsto \zeta^k$. Note that $T(\alpha) \equiv -C_0(\alpha) \pmod{p}$. The complex conjugate of $\alpha$ is $\sigma_{-1}(\alpha)$ and is denoted by $\overline{\alpha}$. If $\overline{\alpha} = \alpha$ then $\alpha$ is said to be real.

3 PRIMARY ELEMENTS

We start with the definition as given by Kummer [13, p. 158]. We use the notations of the previous section.

Definition 1. An element $\alpha \in \mathbb{Z}[\zeta]$ is said to be primary whenever it satisfies

$$
\alpha \equiv 0 \pmod{\omega}, \quad \alpha \equiv B \pmod{\omega^2}, \quad \alpha \overline{\alpha} \equiv B^2 \pmod{p}
$$

for some $B \in \mathbb{Z}$.

Remark 1. If only the two first conditions are met, $\alpha$ is said to be semi-primary.

The next two propositions establish simple criteria for semi-primary and primary elements.

Proposition 1. Let $\alpha \in \mathbb{Z}[\zeta]$. Then $\alpha$ is semi-primary if $C_0(\alpha) \equiv 0 \pmod{p}$ and $C_1(\alpha) \equiv 0 \pmod{p}$.

Proof. From Eq. (1), we get $\alpha \equiv C_0(\alpha) + C_1(\alpha) \omega \pmod{\omega^2}$. Hence, letting $B = C_0(\alpha) \in \mathbb{Z}$, we have (i) $\alpha \equiv 0 \pmod{\omega}$ if and only if $C_0(\alpha) \equiv 0 \pmod{p}$ and (ii) $\alpha \equiv B \pmod{\omega^2}$ if and only if $C_1(\alpha) \equiv 0 \pmod{p}$. As rational integers are congruent modulo $\omega$ if and only if they are congruent modulo $p$, we obtain the equivalent conditions (i) $C_0(\alpha) \equiv 0 \pmod{p}$ and (ii) $C_1(\alpha) \equiv 0 \pmod{p}$.

Lemma 1. If $\alpha \in \mathbb{Z}[\zeta]$, $\alpha \not\equiv C_0(\alpha) \pmod{p}$, is real then $\alpha \equiv B + C \omega^{2k} \pmod{\omega^{2k+1}}$ for some $B, C \in \mathbb{Z}, C \equiv 0 \pmod{p}$, and $1 \leq k \leq \frac{p-3}{2}$. Moreover, $k$ is uniquely determined by $\alpha$.

Proof. Given $\alpha \in \mathbb{Z}[\zeta]$, we can uniquely express $\alpha$ as $\alpha = C_0(\alpha) + C_1(\alpha) \omega + \cdots + C_{p-2}(\alpha) \omega^{p-2}$. Now, since $\alpha \not\equiv C_0(\alpha) \pmod{p}$, there exists an index $1 \leq j \leq p - 2$ with $C_j(\alpha) \not\equiv 0 \pmod{p}$—recall that $p \sim \omega^{p-1}$. If we set $m = \text{arg min}_{j \leq p-2} |C_j(\alpha)| \pmod{p}$), we can write $\alpha \equiv B + C \omega^m \pmod{p}$ with $B = C_0(\alpha)$ and $C = C_m(\alpha)$. Its complex conjugate verifies $\overline{\alpha} \equiv B + C \omega^m \equiv B + C (-\sum_{j=1}^{m} \omega^j)^m \equiv B + C (\omega)^m \pmod{\omega^m}$. The condition $\alpha$ being real (i.e., $\alpha = \overline{\alpha}$) implies that $m$ is even; say, $m = 2k \in \{1, \ldots, p-2\}$ i.e. $1 \leq k \leq \frac{p-3}{2}$.

Proposition 2. Let $\alpha \in \mathbb{Z}[\zeta]$, $\alpha$ semi-primary. Then $\alpha$ is primary if $C_{2j}(\alpha \overline{\alpha}) \equiv 0 \pmod{p}$ for all $1 \leq j \leq \frac{p-3}{2}$.

Proof. Define $B = C_0(\alpha)$ and $\beta = \alpha \overline{\alpha}$. From $\beta \equiv C_0(\beta) + C_1(\beta) \omega + \cdots + C_{p-2}(\beta) \omega^{p-2} \pmod{p}$ and since $\omega \sim \omega^{p-1}$, we have $C_0(\beta) \equiv C_0(\alpha)^2 \equiv B^2 \pmod{p}$ and $C_1(\beta) \equiv C_1(\alpha)^2 \equiv B^2 \pmod{p}$. Consequently, the third condition in Definition 1 becomes $C_1(\beta) \equiv 0 \pmod{p}$ if and only if $C_{2j}(\alpha \overline{\alpha}) \equiv 0 \pmod{p}$, for all $1 \leq j \leq p - 2$.

If $\beta \equiv C_0(\beta) \pmod{p}$ then $\beta \equiv B^2 \pmod{p}$ and thus $\alpha$ is primary. We henceforth assume that $\beta \not\equiv C_0(\beta) \pmod{p})$. Noticing that $\beta = \alpha \overline{\alpha}$ is real, we can apply Lemma 1. We obtain $\beta \equiv B^2 + C \omega^{2k} \pmod{p}$ for some $1 \leq k \leq \frac{p-3}{2}$ and where $C \equiv C_{2k}(\beta) \pmod{p}$. In particular, this implies $C_1(\beta) \equiv 0 \pmod{p}$. Furthermore, by assumption, $C_{2j}(\beta) \equiv 0 \pmod{p}$ for all $1 \leq j \leq \frac{p-3}{2}$. It remains to show that $C_{2j+1}(\beta) \equiv 0 \pmod{p}$ for all $1 \leq j \leq \frac{p-3}{2}$. This follows by successive applications of Lemma 1: $C_{1}(\beta) \equiv 0 \pmod{p}$ and $C_2(\beta) \equiv 0 \pmod{p}$ imply $C_3(\beta) \equiv 0 \pmod{p}$; in turn, together with $C_4(\beta) \equiv 0 \pmod{p}$ imply $C_5(\beta) \equiv 0 \pmod{p}$; and so on... until $C_{p-2}(\beta) \equiv 0 \pmod{p}$.

2
4 OBTAINING PRIMARY ASSOCIATES

As a consequence of Dirichlet’s unit theorem, the group of units of \( \mathbb{Z}[\zeta] \) is the direct product of \( (\pm \zeta^i) \) and a free abelian group \( E \) of rank \( r = \frac{p-3}{2} \). The generators of \( E \) are called fundamental units and will be denoted by \( \eta_1, \ldots, \eta_r \).

The next proposition states that among the associates of an algebraic integer, we may distinguish one (up to the sign) which is primary. Clearly, from Definition 1, if \( \alpha^* \) is primary then \( -\alpha^* \) is also primary.

**Proposition 3.** Every element \( \alpha \in \mathbb{Z}[\zeta] \) with \( \alpha \neq 0 \) (mod \( \omega \)) has a primary associate \( \alpha^* \) of the form

\[
\alpha^* = \pm \zeta^{e_0} \eta_1^{e_1} \cdots \eta_r^{e_r} \alpha \quad \text{where } 0 \leq e_0, e_1, \ldots, e_r \leq p - 1.
\]

Moreover, \( \alpha^* \) is unique up to its sign.

**Proof.** See [4, Lemma 2.6]. \( \square \)

The following lemma is useful.

**Lemma 2.** If \( \alpha, \alpha^* \in \mathbb{Z}[\zeta] \) are semi-primary then so is \( \alpha^\prime \).  

**Proof.** Let \( \alpha, \alpha^* \in \mathbb{Z}[\zeta] \) with \( C_0(\alpha), C_0(\alpha^*) \neq 0 \) (mod \( p \)) and \( C_1(\alpha) \equiv C_1(\alpha^*) \equiv 0 \) (mod \( p \)). Write \( \alpha = \sum \alpha_{j} \zeta^j \). It is worth seeing that \( \alpha = \sum \alpha_{j} \zeta^j \). Moreover, from \( \alpha \equiv \sum \alpha_{j} \zeta^j \equiv 0 \) (mod \( p \)) and \( \alpha \equiv \sum \alpha_{j} \zeta^j \equiv 0 \) (mod \( p \)), we obtain \( C_0(\alpha^*) \equiv C_0(\alpha) \equiv 0 \) (mod \( p \)). Letting \( \alpha^* = \sum \alpha_{j} \zeta^j \) with \( c_j = C_j(\alpha^*) \), we get \( C_j(\alpha^*) = C_j(\alpha) \equiv 0 \) (mod \( p \)) for all \( 0 \leq c_j \leq p - 2 \). In particular, we have \( C_0(\alpha^*) \equiv 0 \) (mod \( p \)). Letting \( \alpha^* = \sum \alpha_{j} \zeta^j \) with \( c_j = C_j(\alpha^*) \), we get \( C_j(\alpha^*) = C_j(\alpha) \equiv 0 \) (mod \( p \)) for all \( 0 \leq c_j \leq p - 2 \). Hence, we obtain \( C_0(\alpha^*) \equiv C_0(\alpha) \equiv 0 \) (mod \( p \)).

As a result, from \( C_0(\alpha^*) \equiv 0 \) (mod \( p \)) and \( C_1(\alpha^*) \equiv C_1(\alpha) \equiv 0 \) (mod \( p \)), we get \( C_0(\alpha^*) \equiv 0 \) (mod \( p \)) and \( C_1(\alpha^*) \equiv 0 \) (mod \( p \)). This is semi-primary. \( \square \)

**Theorem 1.** Let \( \alpha \in \mathbb{Z}[\zeta] \) with \( \alpha \neq 0 \) (mod \( \omega \)). Then \( \alpha^* \) with \( s = \frac{C_1(\alpha)}{C_0(\alpha)} \) (mod \( \omega \)) is semi-primary.

**Proof.** Note that the condition \( \alpha \equiv 0 \) (mod \( \omega \)) is equivalent to \( C_0(\alpha) \equiv 0 \) (mod \( p \)). Let \( \alpha^{(1)} = \alpha \) with \( s = \frac{C_1(\alpha)}{C_0(\alpha)} \) (mod \( p \)). We need to check the conditions of Proposition 1. In the proof of Lemma 2, we showed that, for every \( \alpha, \alpha^* \in \mathbb{Z}[\zeta] \), \( C_0(\alpha^*) \equiv C_0(\alpha) \) (mod \( p \)) and \( C_1(\alpha^*) \equiv C_1(\alpha) \) (mod \( p \)). By induction, we therefore get \( C_0(\alpha^*) \equiv C_0(\alpha) \equiv 1 \) (mod \( p \)) and \( C_1(\alpha^*) \equiv s \) (mod \( p \)). So, we have \( C_0(\alpha^{(1)}) \equiv C_0(\alpha) \equiv 1 \) (mod \( p \)) and \( C_1(\alpha^{(1)}) \equiv C_1(\alpha) \equiv 1 \) (mod \( p \)). We also have \( C_0(\alpha^{(1)}) \equiv C_0(\alpha) \equiv 1 \) (mod \( p \)) and \( C_1(\alpha^{(1)}) \equiv C_1(\alpha) \equiv 1 \) (mod \( p \)). This is semi-primary. \( \square \)

Theorem 1 provides an efficient way to produce a semi-primary associate. Now, suppose we are given two semi-primary integers \( \alpha, \varepsilon \in \mathbb{Z}[\zeta] \). Lemma 2 teaches that \( \varepsilon \) is also semi-primary. The same holds true by induction for \( \alpha^* \equiv \alpha \varepsilon_k \alpha^* \), for any exponent \( \varepsilon_k \geq 1 \).

Suppose further that the resulting \( \alpha \) satisfies

\[
C_2(\alpha \bar{\alpha}) \equiv 0 \quad \text{mod } p \quad \text{for all } 1 \leq j \leq k.
\]

As will become apparent (cf. Theorem 2), by Proposition 2, iterating this process for \( k = 1, \ldots, \frac{p-3}{2} \) eventually yields a primary element. Moreover, if all involved \( \varepsilon \) are units then the so-obtained primary element is also an associate. In order to make the above process work, the updating step (i.e., \( \alpha^* \equiv \varepsilon_k \alpha^* \)) should be such that Equation (2) remains fulfilled for the new \( \alpha \) when \( k \) is incremented. This can be achieved by selecting real units \( \varepsilon_k \) of the form

\[
\varepsilon_k \equiv E_k + F_k \omega^{2k} \quad \text{mod } \omega^{2k+1} \quad \text{with } E_k, F_k \in \mathbb{Z} \text{ and } E_k, F_k \equiv 0 \quad \text{mod } p,
\]

for \( 1 \leq k \leq \frac{p-3}{2} \); cf. Lemma 1. Note that as defined by Eq. (3), units \( \varepsilon_k \) are semi-primary.

**Theorem 2.** Given some integer \( k \geq 1 \), let \( \alpha \in \mathbb{Z}[\zeta] \), a semi-primary, such that \( C_2(\alpha \bar{\alpha}) \equiv 0 \) (mod \( p \)) for all \( 1 \leq j < k-1 \) and a real unit \( \varepsilon \in \mathbb{Z}[\zeta] \) such that \( e \equiv C_0(\varepsilon) + C_{2k}(\varepsilon) \omega^{2k} \) (mod \( \omega^{2k+1} \)) with \( C_0(\varepsilon), C_{2k}(\varepsilon) \equiv 0 \) (mod \( p \)). Then \( \alpha^* \equiv \alpha \varepsilon \) with \( t = C_2(\alpha \bar{\alpha}) C_0(\varepsilon) \times C_{2k}(\varepsilon) \omega^{2k} \) (mod \( p \)), \( \alpha^* \equiv \alpha \varepsilon \equiv 0 \) (mod \( p \)) for all \( 1 \leq j \leq k \).
Proof. Since $\varepsilon$ is semi-primary, $\alpha' = \alpha \varepsilon^t$ is semi-primary for any $t$ by Lemma 2. Further, since $\varepsilon$ is real (i.e., $\varepsilon = \overline{\varepsilon}$), it follows that $\alpha' \overline{\alpha'} = \alpha \overline{\alpha} \overline{\varepsilon}^{2t}$. From Lemma 1, $\alpha \overline{\alpha}$ is real and since $C_{2j}(\alpha \overline{\alpha}) \equiv 0 \pmod{p}$ for all $1 \leq j \leq k - 1$, we deduce that $\alpha \overline{\alpha} \equiv C_0(\alpha \overline{\alpha}) + C_{2k}(\alpha \overline{\alpha}) \omega^{2k} \pmod{\omega^{2k+1}}$. Hence, we get $\alpha' \overline{\alpha'} \equiv (C_0(\alpha \overline{\alpha}) + C_{2k}(\alpha \overline{\alpha}) \omega^{2k}) \equiv C_0(\alpha \overline{\alpha}) + C_{2k}(\alpha \overline{\alpha}) \omega^{2k} \equiv 2C_0(\alpha \overline{\alpha}) \omega^{2k} \pmod{\omega^{2k+1}}$ and thus $C_{2k}(\alpha' \overline{\alpha'}) \equiv 2C_0(\alpha \overline{\alpha}) \omega^{2k} \equiv C_{2k}(\alpha' \overline{\alpha'}) \pmod{\omega^{2k+1}}$. Consequently, since $C_0(\varepsilon) \equiv 0 \pmod{p}$, we have $C_{2k}(\alpha' \overline{\alpha'}) \equiv 0 \pmod{p} \iff 2C_0(\varepsilon) \equiv 0 \pmod{p} \iff \varepsilon \equiv 0 \pmod{p}$, and thus $C_0(\alpha' \overline{\alpha'}) \equiv 0 \pmod{p}$ since $C_0(\alpha \overline{\alpha}) \equiv 0 \pmod{p}$ ($\alpha \overline{\alpha}$ being semi-primary from Lemma 2) and $C_{2k}(\varepsilon) \equiv 0 \pmod{p}$ by assumption.

The existence of a set of fundamental real units $\{e_1, \ldots, e_r\}$ with $r = \frac{p-3}{2}$ of the form (3) is a result of Dénes [9]; see also [20, pp. 192–193] and [23, Theorem 2]. Let $e^+ = (\zeta \overline{\zeta}/2 - \zeta \overline{\zeta}/2) / (\zeta - \overline{\zeta}/2)$ where $g$ is an odd primitive root modulo $p$. Then the units $e_k, 1 \leq k \leq r,$ given by

$$e_k = (e^+)^{\sum_{j=0}^{k-1} \sigma_r \cdot \zeta^{j} \cdot \zeta^k \mod p} \quad \text{where } \sigma_r : \zeta \mapsto \zeta^r$$

are real and satisfy Equation (3) with $E_k \equiv C_0(e_k) \pmod{p}$ and $F_k \equiv C_{2k}(e_k) \pmod{p}$.

We now have all the ingredients to obtain a primary element $\alpha^*$ as per Proposition 3. Starting with $\alpha^{[0]} \leftarrow \alpha$ and iterating as

$$\begin{align*}
\alpha^{[1]} &\leftarrow \alpha^{[0]} \cdot e_0 \equiv \frac{C_1(\alpha^{[0]})}{C_0(\alpha^{[0]})} \pmod{p} \quad \text{(Theorem 1)} \\
\alpha^{[k+1]} &\leftarrow \alpha^{[k]} \cdot e_k \equiv \frac{C_{2k}(\alpha^{[k]})}{2C_0(\alpha^{[k]}) \cdot C_{2k}(\varepsilon)} \pmod{p} \quad \text{(Theorem 2), \quad for } 1 \leq k \leq r
\end{align*}$$

where $\beta^{[k]} = \alpha^{[k]} \overline{\alpha^{[k]}}$ and $r = \frac{p-3}{2},$ we obtain $\alpha^{[r+1]} \leftarrow \alpha^{[0]} \cdot e_0 \cdot e_1 \cdot \ldots \cdot e_r,$ which is primary. Knowing that two primary associates only differ by a $p^{th}$-power unit, exponents $e_j$ (0 \leq j \leq r) can be reduced modulo $p$. Finally, if the resulting primary associate to be expressed with respect to a given set of fundamental units $\{\eta_1, \ldots, \eta_r\},$ from the decompositions $e_j = \zeta \overline{\zeta}/2 \prod_{k=1}^{j} \eta_k$ with $f_{j,k} \in \mathbb{Z},$ we write $\alpha^{[r+1]} \leftarrow \alpha^{[0]} \cdot e_0 \cdot \prod_{j=1}^{r} e_j^{f_j} = \alpha^{[0]} \cdot e_0 \cdot \prod_{j=1}^{r} \eta_j \zeta \overline{\zeta} e_j^{f_j}$ where $e_j = e_0 + \sum_{j=1}^{r} f_{j,k} e_j$ and $e'_k = \sum_{j=1}^{r} f_{j,k} e_j$, for $1 \leq k \leq r$, or using matrix notation,

$$(e'_0, \ldots, e'_r) = T(e_0, \ldots, e_r) \quad \text{with } T(e_0, \ldots, e_r) = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ f_1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_r \end{bmatrix}.$$ 

We define

$$\alpha^* = \alpha^{[0]} \cdot e_0 \cdot e_1 \cdot \ldots \cdot e_r \pmod{p}.$$ 

Putting it all together, this yields a generic algorithm for finding primary associates along with their representation; see Algorithm 1. On input $\alpha \in \mathbb{Z}[\zeta]$ with $T(\alpha) \not\equiv 0 \pmod{p},$ the algorithm outputs the primary associate $\alpha^*$ with respect to basis $\{\eta_1, \ldots, \eta_r\}$ and the representation vector $(e_0, e_1, \ldots, e_r),$ such that $\alpha^* = \zeta^{e_0} \eta_1^{e_1} \cdots \eta_r^{e_r} \alpha.$ We write primary($\alpha$) $\leftarrow \alpha^*$ and repr($\alpha$) $\leftarrow (e_0, e_1, \ldots, e_r).$ The algorithm internally makes use of the set of real units $\{e_1, \ldots, e_r\}$ as defined in Eq. (4) and corresponding conversion transform $T.$

5 COMPUTING SYMBOLS

If $\mathbb{Z}[\zeta]$ is norm-Euclidean, there exists for all pairs $\alpha, \beta \in \mathbb{Z}[\zeta]$ with $\beta \neq 0$ an element $p \in \mathbb{Z}[\zeta]$ such that $\alpha \equiv p \pmod{\beta}$ and $N(p) < N(\beta).$ Explicit algorithms for finding $p$ are known; see [16] for $p \leq 11$ and [17] for $p = 13.$ We refer to such an algorithm as euclid_div(). The Caranay–Scheidler algorithm [3] (initially given in the context of $p = 7$) can then be extended to compute higher-order power residue symbols. Recall that $\omega = 1 - \zeta.$ For $\alpha, \pi \in \mathbb{Z}[\zeta]$ with $\pi$ a prime such that $\pi + \omega$ and $\pi \not\equiv \alpha \pmod{p}$, the $p^{th}$ power residue symbol $\left( \frac{\zeta}{\pi} \right)_p$ is defined to be the $p^{th}$ root of unity $\zeta^i$ such that

$$\alpha^{(N(p)-1)/p} \equiv \zeta^i \pmod{p}$$

and the integer $i$ is called the index of $\alpha$ with respect to $\pi,$ henceforth denoted ind$_\pi(\alpha).$ In a way similar to the Legendre symbol, the definition generalizes: If $\lambda \in \mathbb{Z}[\zeta]$ is non-unit and gcd($\lambda, \omega) \sim 1$ then, writing $\lambda = \prod_j \pi_j^{f_j}$
Algorithm 1: Computing $\alpha^* \sim \alpha$ and its representation

**Input:** $\alpha \in \mathbb{Z}[\zeta]$ with $T(\alpha) \equiv 0 \pmod{p}$

**Output:** $\alpha^* \leftarrow \text{primary}(\alpha)$ and $(e_0, e_1, \ldots, e_r) \leftarrow \text{repr}(\alpha)$ with $\alpha^* = \zeta^{\epsilon_0} \eta^{e_0} \cdots \eta^{e_r} \alpha$ and $r = \frac{p-3}{2}$

$e_0 \leftarrow C_1(\alpha)/C_0(\alpha) \pmod{p}$
$\alpha \leftarrow \zeta^{e_0} \alpha; \beta \leftarrow \alpha \overline{\alpha}$

for $k = 1$ to $\frac{p-3}{2}$ do
$e_k \leftarrow -\frac{C_{2k}(\beta) C_0(e_k)}{2C_0(\beta) C_{2k}(e_k)} \pmod{p}$
$\beta \leftarrow \beta e_k^{2^{2k}}$
end

$(e_0, e_1, \ldots, e_r) \leftarrow \tau(e_0, e_1, \ldots, e_r) \pmod{p}$
$\alpha^* \leftarrow \zeta^{e_0} \eta^{e_0} \cdots \eta^{e_r} \alpha$
return $(\alpha^*, (e_0, e_1, \ldots, e_r))$

for primes $\pi_j$ in $\mathbb{Z}[\zeta]$, the (generalized) $p^\text{th}$ power residue symbol $\left\lfloor \frac{\alpha}{\pi_j} \right\rfloor_p$ is defined as $\left\lfloor \frac{\alpha}{\pi_j} \right\rfloor_p = \prod_j \left\lfloor \frac{\alpha}{\pi_j} \right\rfloor_p^{e_j}$. Provided that $p$ is a regular prime (which is verified for all odd primes $p \leq 13$), Kummer’s reciprocity law [13] states that for any two primary elements $\alpha, \lambda \in \mathbb{Z}[\zeta]$, $\left\lfloor \frac{\alpha}{\lambda} \right\rfloor_p = \left\lfloor \frac{\lambda}{\alpha} \right\rfloor_p$.

This leads to Algorithm 2 given below (where for compactness we have set $\eta_0 = \zeta$).

Algorithm 2: Computing the $p^\text{th}$ power residue symbol

**Input:** $\alpha, \lambda \in \mathbb{Z}[\zeta]$ with $\gcd(\alpha, \lambda) = 1$ and $T(\lambda) \equiv 0 \pmod{p}$

**Output:** $\left\lfloor \frac{\alpha}{\lambda} \right\rfloor_p$

$\lambda^* \leftarrow \text{primary}(\lambda)$
$j \leftarrow 0$
while $N(\lambda^*) > 1$ do
$\rho \leftarrow \text{euclid\_div}(\alpha, \lambda^*)$
$s \leftarrow 0$
while $T(\rho) \equiv 0 \pmod{p}$ do
$s \leftarrow s + 1$
$\rho \leftarrow \rho + \omega$
end
$(\rho^*, (e_0, e_1, \ldots, e_r)) \leftarrow \text{primary}(\rho), \text{repr}(\rho)$
$j \leftarrow j + s \cdot \text{ind}_P(\omega)$
for $i = 0$ to $r$ do
$j \leftarrow j - e_i \cdot \text{ind}_P(\eta_i)$
end
$\alpha \leftarrow \lambda^*; \lambda^* \leftarrow \rho^*$
end
return $\zeta^j$

6 NINTH- AND SIXTEENTH-POWER RESIDUE SYMBOLS

In this section, we study the $9^\text{th}$- and the $16^\text{th}$ power residue symbols.

$9^\text{th}$ power residue symbol For $p = 9$, the ring $\mathbb{Z}[\zeta_9]$ is known to be norm-Euclidean [5]; see [6, § 3] for a division algorithm. The previous framework does not readily apply to this case; we nevertheless still obtain a reciprocity law and complementary laws through decomposition. Let $\zeta := \zeta_9$ and $\omega = 1 - \zeta$. For $\alpha, \beta \in \mathbb{Z}[\zeta]$ co-prime with $\omega$,
we can write
\[ \alpha = \prod_{i=1}^{15} \left( 1 + \omega^i \right)^{e_i} \mod \omega^{15}, \quad \beta = \prod_{i=1}^{15} \left( 1 + \omega^i \right)^{f_i} \mod \omega^{15} \]
with integer exponents \( e_i, f_i \) and \( e_1, f_1 \in \{0, 1\} \). There are \( 4 \times 15 \) integer constants \( U_{j,i} \) so that
\[ k_j = \sum_{i=1}^{15} U_{j,i} e_i \]
makes the following “complementary laws” hold:
\[ \left[ \frac{\zeta}{\alpha} \right]_j = \zeta^{k_1}, \quad \left[ 1 + \frac{\zeta + \zeta^2}{\alpha} \right]_j = \zeta^{k_2}, \quad \left[ 1 + \frac{\zeta^2 + \zeta^3}{\alpha} \right]_j = \zeta^{k_3}, \quad \left[ \frac{\omega}{\alpha} \right]_j = \zeta^{k_4}. \]
Importantly, the constants \( U_{j,i} \) do not depend on \( \alpha \). Similarly there is a fixed \( 15 \times 15 \) matrix \( (T_{i,j}) \) with integer coefficients so that we have this ninth reciprocity law:
\[ \left[ \frac{\alpha}{\beta} \right]_j = \left[ \frac{\beta}{\alpha} \right]_j \cdot \zeta^k \quad \text{where} \quad k = \sum_{i,j} T_{i,j} e_i f_j. \]
The matrices are given below:
\[
T = \begin{pmatrix}
0 & 5 & 3 & 7 & 1 & 8 & 7 & 5 & 3 & 6 & 3 & 6 & 3 & 0 \\
4 & 0 & 4 & 3 & 2 & 3 & 1 & 6 & 6 & 3 & 0 & 6 & 0 & 0 \\
6 & 5 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 6 & 3 & 0 & 5 & 6 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\
8 & 7 & 0 & 4 & 0 & 0 & 3 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\
1 & 6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
2 & 8 & 0 & 3 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 \\
4 & 3 & 0 & 3 & 3 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\]
\[ U = \begin{pmatrix}
8 & 6 & 1 & 0 \\
4 & 6 & 7 & 0 \\
8 & 6 & 1 & 0 \\
5 & 4 & 3 & 0 \\
1 & 7 & 7 & 0 \\
7 & 8 & 7 & 6 \\
7 & 4 & 6 & 0 \\
1 & 2 & 7 & 0 \\
0 & 3 & 3 & 8 \\
0 & 6 & 3 & 0 \\
0 & 3 & 0 & 0 \\
6 & 3 & 6 & 6 \\
6 & 6 & 0 & 0 \\
6 & 3 & 6 & 0 \\
0 & 0 & 0 & 3
\end{pmatrix}
\]
A complete algorithm for computing the 9th power residue symbol using these matrices is given in Appendix A.

16th power residue symbol The same can be done very similarly in the norm-Euclidean ring \( \mathbb{Z}[\zeta_{16}] \) (see [19] for a proof of the division property and [6, §5] for a division algorithm) with \( \zeta := \zeta_{16} \) a 16th root of unity and \( \omega = 1 - \zeta \). Then, for \( \alpha, \beta \in \mathbb{Z}[\zeta] \) co-prime with 2, we can write:
\[ \alpha = \prod_{i=1}^{40} \left( 1 + \omega^i \right)^{e_i} \mod \omega^{41}, \quad \beta = \prod_{i=1}^{40} \left( 1 + \omega^i \right)^{f_i} \mod \omega^{41} \]
with integer exponents \( e_i, f_i \) and \( e_1, f_1 \in \{0, 1\} \). There are \( 5 \times 40 \) integer constants \( U_{j,i} \) so that
\[ k_j = \sum_{i=1}^{40} U_{j,i} e_i \]
makes the following equalities hold:
\[ \left[ \frac{\zeta}{\alpha} \right]_{16} = \zeta^{k_1}, \quad \left[ 1 + \frac{\zeta + \zeta^2}{\alpha} \right]_{16} = \zeta^{k_2}, \quad \left[ 1 + \frac{\zeta^2 + \zeta^3}{\alpha} \right]_{16} = \zeta^{k_3}, \quad \left[ \frac{\omega}{\alpha} \right]_{16} = \zeta^{k_4}, \quad \left[ \frac{\beta}{\alpha} \right]_{16} = \zeta^{k_5}. \]
Again, the constants \( U_{j,i} \) do not depend on \( \alpha \). Similarly there is a fixed \( 40 \times 40 \) matrix \( (T_{i,j}) \) with integer coefficients so that we have this sixteenth reciprocity law:
\[ \left[ \frac{\alpha}{\beta} \right]_{16} = \left[ \frac{\beta}{\alpha} \right]_{16} \cdot \zeta^k \quad \text{where} \quad k = \sum_{i,j} T_{i,j} e_i f_j. \]
The matrices \( T \) and \( U \) are given below:
7 CONCLUSION AND FURTHER RESEARCH

The methods described in this paper enable the computation of \( p^{th} \) power residue symbols up to and including \( p = 13 \) when \( p \) is prime. Whether for \( p = 17 \) and \( p = 19 \) there is an Euclidean division seems (to the best of our understanding) currently unknown and perhaps an alternative strategy must be found. The problem gets harder beyond \( p = 23 \), as the ideal class group is no longer trivial, and in particular is difficult for \( p = 37 \) which is not a regular prime (and therefore Kummer’s theory does not apply).

We also provide algorithms for the \( 9^{th} \) and \( 16^{th} \) power residue symbols, which may be extended albeit may require a more compact formulation.

REFERENCES


A COMPUTING NINTH RESIDUE SYMBOLS

A.1 COMMENTED CODE

We use in this section the following conventions: $\perp$ denotes failure, $[x]$ consists in rounding $x$ arithmetically, and if $P(\zeta)$ be a polynomial in the variable $\zeta$ we denote:

- by $P_\chi$ the reduction of $P$ modulo the polynomial $\chi(\zeta) = 1 + \zeta^3 + \zeta^6$;
- by $P[\zeta]$ the polynomial $P$ in which $\zeta$ was replaced by $\ell$. $\ell$ may be a polynomial in $\zeta$ or any other expression;
- by $f_c$ and $f_n$ the following functions:

$$f_c[P] = (P[\zeta^2] \cdot P[\zeta^4] \cdot P[\zeta^5] \cdot P[\zeta^7] \cdot P[\zeta^8])_\chi$$

$$f_n[P] = (P \cdot f_c[P])_\chi.$$

The function $\text{Random}_L$ generates a random integer comprised between $-10^L$ and $10^L$. In the code we set $L = 27$ for the sake of the example to generate numbers $\in [-10^{27}, 10^{27}]$. The function $\text{CoefficientList}$ returns all the coefficients of $\zeta^i$ up to the indicated index $\ell \leq u$, i.e.:

$$\text{CoefficientList}_\ell \left[ \sum_{i=0}^{W} \epsilon_i \zeta^i \right] = \{\epsilon_0, \ldots, \epsilon_\ell\}.$$

This section will make use of matrices $T$ and $U$ defined in Section 6.

We implement both the algorithm and test functions for experimentation with it. The following auxiliary function generates a random prime in the cyclotomic field which is $1$ mod $\omega$.

```
Function FieldRandomPrime[]
  p = 1
  While[p is composite,  
    $\alpha \leftarrow 1 + (1 - \zeta) \sum_{i=0}^{5} \zeta^i \cdot \text{Random}_L$
    $p \leftarrow f_n[\alpha]$
  ]
  Return[\alphaΧ]
```

The following function computes $9^{th}$ power residues for prime elements $\beta$ and checks the result to validate the algorithm.

```
Function Resid[α,β]
  n ← f_n[β]
  $γ \leftarrow f_c[β]$
  $q \leftarrow (α^{(n\ell-1)/9})_\chi \mod n$
  If $\exists 0 < \epsilon < 8$ s.t. $((q - \zeta^\epsilon)γ)_\chi \mod n = 0$ then
  Return[\epsilon]
  Else
    Return[\perp]
```

Euclidean division is computed by the following function:

```
Function Euclid[α,β]
  $s \leftarrow \{-\zeta^8, \ldots, -\zeta, -1, 0, 1, \zeta, \ldots, \zeta^8\}$
  $q \leftarrow (\bar{\alpha}\bar{β})_\chi$
  $\{c_0, \ldots, c_5\} \leftarrow \text{CoefficientList}_5[\zeta^8 + q]$
  $r \leftarrow \sum_{j=0}^{5} c_j \zeta^j$
  construct the list $z \leftarrow \{f_n(q - r \cdot s_j)\}_{1 \leq j \leq 19}$
  $w \leftarrow \arg \min r[z[i]]$
  $r \longleftarrow r - s_w$
  Return[(α - β)\chi]
```

As its name indicates, $\text{OmegaExp}$ computes the $\omega$ expansion of $\alpha$ up to $\omega^{15}$:

```
Function OmegaExp[α]
  $v \leftarrow \{0\}^{16}$
  $η \leftarrow α$
  For[ℓ = 1, ℓ ≤ 15, ℓ++,
    While[f_n[η - 1] mod 3^{ℓ+1} > 0,
      $η \leftarrow (η(1 + (1 - ζ^\ell)))_\chi$
      $vr++$
    ]
  ]
  Return[v]
```
The rest of the code tests the algorithm. In the (* Additional laws *) section we generate a random prime \( \alpha \) (renamed \( A \) for the sake of easier reference) and print it. We then print:

\[
\text{Resid}[\zeta, \alpha], \text{Resid}[1 + \zeta, \alpha], \text{Resid}[1 + \zeta^2, \alpha], \text{Resid}[1 - \zeta, \alpha]
\]

compute \( v = \OmegaExp[\alpha] \) and display the value of:

\[
- \sum_{i=1}^{15} v_i \pi_i \mod 9
\]

to visually check that results agree.

In the (* Reciprocity with prime elements *) section we generate and print two random primes \( \alpha, \beta \) (again, denoted \( A, B \) in the code for easier reference). Here we check visually that primality and coupling results agree, namely that:

\[
(\text{Resid}[\alpha, \beta] - \text{Resid}[\beta, \alpha]) \mod 9 \equiv \OmegaExp[\alpha].T.\OmegaExp[\beta]
\]

In the (* Reciprocity with composite elements *) section we generate five random primes \( \alpha_1, \alpha_2, \alpha_3 \) and \( \beta_1, \beta_2 \). We let \( \alpha = (\alpha_1 \alpha_2 \alpha_3)^x \) and \( \beta = (\beta_1 \beta_2)^x \). The test here consists in visually testing the equality:

\[
\sum_{x=1}^{3} \sum_{y=1}^{2} (\text{Resid}[\alpha_x, \beta_y] - \text{Resid}[\beta_y, \alpha_x]) \mod 9 \equiv \OmegaExp[\alpha].T.\OmegaExp[\beta]
\]

The code then randomly refreshes \( \alpha_1, \alpha_2, \alpha_3 \) and \( \beta_1, \beta_2 \). We let again: \( \alpha = (\alpha_1 \alpha_2 \alpha_3)^x \) and \( \beta = (\beta_1 \beta_2)^x \). The program prints for visual inspection the value:

\[
\sum_{x=1}^{3} \sum_{y=1}^{2} \text{Resid}[\alpha_x, \beta_y] \mod 9
\]

Let \( w = 0 \) and \( \gamma = \alpha \). We instruct the computer to dynamically update on the screen the value of \( f_0(\gamma) \) and perform the following operations:

```plaintext
While[f0[\gamma] > 1,
  w' = w + OmegaExp[\alpha].T.\OmegaExp[\beta]
  \{\alpha, \beta\} \leftarrow \{\beta, \alpha\}
  \gamma \leftarrow \text{Euclid}[\alpha, \beta]
  While[f0[\gamma] \mod 3 \equiv 0,
    \gamma \leftarrow 2(\text{\gamma \mod 3})
    w' \leftarrow w - \pi_2.\OmegaExp[\beta] \mod 9
  ]
  If[\gamma \mod 3 \equiv 2, \gamma \leftarrow -\gamma]
  \alpha \leftarrow \gamma
]
```

Finally, we print the value of the symbol, \( \OmegaExp[\alpha].T.\OmegaExp[\beta] \mod 9 \).

### A.2 SOURCE CODE

1 (* Defining cyclotomic field and norm function *)

2 \text{PR}[\alpha_\text{mod} \Omega] := \text{PolynomialRemainder}[\alpha, \Omega, \text{Modulus} \rightarrow \Omega] \Rightarrow \Omega;

3 \text{fc}[\alpha] := \text{PR}[\{\alpha/\zeta \rightarrow \zeta^2, \zeta^4 \rightarrow \zeta^8\}];

4 \OmegaExp[\alpha] := \text{PR}[\alpha/\text{fc}[\alpha]];

5 (* Generates a random prime in the cyclotomic field, which is 1 mod \( \omega \) *)

6 \text{FieldRandomPrime}[] := \text{Module}[\{\alpha, \text{p}, \text{l}\},
  \{\text{p}, \text{l}\} \leftarrow \{1, 2\};
  \text{While}[\text{PrimeQ}[\alpha],
    \alpha \leftarrow 1+\{1-\zeta\} \text{Sum}[\text{RandomInteger}[\{-100, 100\}] \zeta^i, \{i, 0, 5\}]\text{\rightarrow p};
  \text{Return}[\text{PR}[\alpha]];
];

7 (* Computing ninth power residue in the case where \( \beta \) is a prime element *)

8 \text{PolyExp} := \text{If}[\#2 == 0, 1, \text{PR}[\theta[0 \text{PR}[\theta^2 = 2, \theta^3], \text{Floor}[\#2/2, \theta^3] \#1 \text{\times Mod}[\#2, \theta^3]] \Rightarrow \theta[1, \#2, \theta^3] \& \theta[1, \#2, \theta^3] \&];
Primary Elements in Cyclotomic Fields with Applications to Power Residue Symbols, and More

\[ \text{Resid}[\alpha_{-}\beta_{-}] := \text{Module}[\{(n,y,q,e), \{n,y\}=\{\text{FN}[\beta],\text{FC}[\beta]\}; q=\text{PolyExp}[\alpha,(n-1)/9,n]; \text{For}\left[e=0, e<8, e++, \right. \]
\[ \left. \text{If}[\text{PR}[q-Z^e]n==0, \text{Return}[e]]; \right\}; \text{Return}["This should not happen!"]]; \]

\[ (\text{Euclidean division - Not proven}) \]
\[ s = \text{Union}[\{q=\text{Table}[Z_i, \{i,0,8\}],-q,\{0\}\}]; \]

\[ \text{Euclid}[U,V] := \text{Module}[\{q,r,z,w\}, q = \text{PR}[U]/\text{FNC}[V]; r = \text{Round}[\text{Delete}[\text{CoefficientList}[Z^6+q,-1]].\text{Table}[Z_i, \{i,0,5\}]; z = fN/(q-r+s); w = \text{Position}[z, \text{Min}[z]]\{1,1\}; r = r-s[w]; \text{Return}[\text{PR}[U-rV]]; ]; \]

\[ \text{(\text{Additional laws})} \]
\[ \text{Print["Using primality: ", \text{Resid}[\#A]/\text{Mod}[1+Z,-1]], \text{Resid}[\#B], 9]; \]
\[ \text{Print["Using structure: ", \text{Mod}[\text{Sum}[v[[i]] U[[i]], \{i,1,15\}],9]]; \]

\[ \text{(* Reciprocity with prime elements *)} \]
\[ \text{Print["Using coupling : ", \text{Mod}[\text{OmegaExp}[A].T.OmegaExp[B],9]]; \]

\[ (\text{Reciprocity with composite elements}) \]
\[ \{a[1],a[2],a[3],\beta[1],\beta[2]\}=\text{Array}[\text{FieldRandomPrime}[\#&],[5]]; \]
\[ \text{Print["Using factors : ", \text{Mod}[\text{Sum}[\text{Resid}[a[x],\beta[y]]-\text{Resid}[\beta[y],a[x]], \{x,1,3\},\{y,1,2\}],9]]; \]

\[ \text{Print["Using coupling : ", \text{Mod}[\text{OmegaExp}[A].T.OmegaExp[B],9]]; \]

\[ \text{\(\text{T} = \begin{bmatrix} 0 & 5 & 3 & 7 & 1 & 8 & 7 & 5 & 3 & 6 & 3 & 6 & 3 & 6 & 3 & 0 \\ 4 & 0 & 4 & 3 & 2 & 3 & 1 & 6 & 6 & 3 & 3 & 0 & 6 & 0 & 9 \\ 6 & 5 & 0 & 6 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 6 & 3 & 0 & 5 & 0 & 6 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 8 & 7 & 0 & 4 & 0 & 0 & 3 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 1 & 6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 0 & 3 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 0 & 3 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \]
\[ \text{U} = \begin{bmatrix} 8 & 6 & 1 & 0 \\ 4 & 6 & 7 & 0 \\ 8 & 6 & 1 & 0 \\ 5 & 4 & 3 & 0 \\ 1 & 7 & 7 & 0 \\ 7 & 8 & 7 & 6 \\ 7 & 4 & 6 & 0 \\ 1 & 2 & 7 & 0 \\ 0 & 3 & 3 & 8 \\ 0 & 6 & 3 & 0 \\ 0 & 3 & 0 & 0 \\ 6 & 3 & 6 & 6 \\ 6 & 6 & 0 & 0 \\ 6 & 3 & 6 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \]

\[ \text{\(\text{T} = \begin{bmatrix} 0 & 5 & 3 & 7 & 1 & 8 & 7 & 5 & 3 & 6 & 3 & 6 & 3 & 6 & 3 & 0 \\ 4 & 0 & 4 & 3 & 2 & 3 & 1 & 6 & 6 & 3 & 3 & 0 & 6 & 0 & 9 \\ 6 & 5 & 0 & 6 & 0 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 6 & 3 & 0 & 5 & 0 & 6 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 8 & 7 & 0 & 4 & 0 & 0 & 3 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 1 & 6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 8 & 0 & 3 & 6 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 4 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \]
\[ \text{U} = \begin{bmatrix} 8 & 6 & 1 & 0 \\ 4 & 6 & 7 & 0 \\ 8 & 6 & 1 & 0 \\ 5 & 4 & 3 & 0 \\ 1 & 7 & 7 & 0 \\ 7 & 8 & 7 & 6 \\ 7 & 4 & 6 & 0 \\ 1 & 2 & 7 & 0 \\ 0 & 3 & 3 & 8 \\ 0 & 6 & 3 & 0 \\ 0 & 3 & 0 & 0 \\ 6 & 3 & 6 & 6 \\ 6 & 6 & 0 & 0 \\ 6 & 3 & 6 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \]
{w,y}={θ,A};
Print["Norm : ", Dynamic[fN[y]]];

While[fN[A]>1,
  (* Invert α and β *)
  w = Mod[w+ΩExp[A].T.ΩExp[B],9];
  {A,B} = {B,A};
  (* Reduce α mod β *)
  y = Euclid[A,B];
  While[Mod[fN[y],3]==0,
    y = PR[y, fc[1-ζ]/3];
    w = Mod[w-(#[[4]]&/@ U).ΩExp[B],9];
  ];
  If[Mod[(y/.ζ→1),3]==2,y = -y];
  A = y;
];
Print["Algorithm : ", Mod[ΩExp[A].T.ΩExp[B],9]];

{w,y}={θ,A};
Print["Norm : ", Dynamic[fN[y]]];

While[fN[A]>1,
  (* Invert α and β *)
  w = Mod[w+ΩExp[A].T.ΩExp[B],9];
  {A,B} = {B,A};
  (* Reduce α mod β *)
  y = Euclid[A,B];
  While[Mod[fN[y],3]==0,
    y = PR[y, fc[1-ζ]/3];
    w = Mod[w-(#[[4]]&/@ U).ΩExp[B],9];
  ];
  If[Mod[(y/.ζ→1),3]==2,y = -y];
  A = y;
];
Print["Algorithm : ", Mod[ΩExp[A].T.ΩExp[B],9]];

12